



# **ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**

## **IMPLEMENTACIÓN DE UN PROTOTIPO COMO SISTEMA DETECTOR DE INTRUSOS PARA DETECTAR ATAQUES DIRIGIDOS AL PROTOCOLO IPv6 DESARROLLADO CON HERRAMIENTAS OPEN SOURCE**

**DIEGO GUSTAVO CAIZA MÉNDEZ**

**Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,  
presentado ante el Instituto de Posgrado y Educación Continua de la  
ESPOCH, como requisito parcial para la obtención del grado de Magíster  
en Seguridad Telemática**

**RIOBAMBA - ECUADOR**

**Diciembre 2016**



## ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

### CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado “IMPLEMENTACIÓN DE UN PROTOTIPO COMO SISTEMA DETECTOR DE INTRUSOS PARA DETECTAR ATAQUES DIRIGIDOS AL PROTOCOLO IPv6 DESARROLLADO CON HERRAMIENTAS OPEN SOURCE”, de responsabilidad del Ing. Diego Gustavo Caiza Méndez ha sido prolijamente revisado y se autoriza su presentación.

#### Tribunal:

Ing. Fredy Proaño Ortiz; PhD.

\_\_\_\_\_  
**PRESIDENTE**

\_\_\_\_\_  
**FIRMA**

Ing. Andrés Cisneros Barahona; M.Sc.

\_\_\_\_\_  
**DIRECTOR**

\_\_\_\_\_  
**FIRMA**

Ing. Edwin Altamirano Santillán; M.Sc.

\_\_\_\_\_  
**MIEMBRO**

\_\_\_\_\_  
**FIRMA**

Ing. Cristhy Jiménez Granizo; M.Sc.

\_\_\_\_\_  
**MIEMBRO**

\_\_\_\_\_  
**FIRMA**

Riobamba, Diciembre 2016

## **DERECHOS INTELECTUALES**

Yo, Diego Gustavo Caiza Méndez declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

---

0603595059

## DECLARACIÓN DE AUTENTICIDAD

Yo, Diego Gustavo Caiza Méndez declaro que el presente Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, Diciembre 2016

---

Diego Gustavo Caiza Méndez  
0603595059



## **DEDICATORIA**

De manera especial quiero dedicar este trabajo a mi abuelita Mercedes quien es la luz en mi camino y guía mis pasos desde el cielo; nada igualará la nobleza de su alma, la grandeza de su espíritu y la bondad de su corazón. Gracias por confiar en mí, por tus sacrificios y por creer que siempre llegaría lejos, sin tu apoyo nunca hubiese alcanzado mis metas.

A mi abuelito Manuel quien ha sido un ejemplo de sencillez, disciplina y rectitud.

A mi mamá Ani quien ha estado siempre presente gracias por tu abnegación, esfuerzo, dedicación y paciencia.

A mi familia quienes han sido la fuente de apoyo constante e incondicional durante este proceso y a las personas especiales en mi vida, este nuevo logro es gracias a ustedes.

**Diego**

## **AGRADECIMIENTO**

Quiero agradecer a Dios quien día a día me protege y me fortalece para seguir adelante.

Mi gratitud muy especial a la Escuela Superior Politécnica de Chimborazo, por haberme permitido adquirir sabios conocimientos para mi formación académica.

Al Ing. Víctor Méndez quien gracias a su apoyo hizo posible iniciar y concluir este ciclo de estudios.

Al Ing. Pablo Méndez por toda su ayuda quien durante todo el desarrollo de este trabajo fue un gran guía.

Al Ing. Santiago Cisneros, al Ing. Edwin Altamirano y a la Ing. Cristhy Jiménez por todo el apoyo incondicional y la asesoría brindada en la realización de esta tesis.

Un sincero agradecimiento a cada una de las personas que han estado involucradas de una u otra manera desde el inicio de esta etapa de manera muy especial a Myriam; todos ustedes saben lo que me ha costado culminar este trabajo de investigación, gracias porque siempre supieron brindarme palabras de aliento y motivación.

**Diego**

## ÍNDICE DE CONTENIDO

<b>DERECHOS INTELECTUALES</b> -----	iii
<b>DECLARACIÓN DE AUTENTICIDAD</b> -----	iv
<b>DEDICATORIA</b> -----	v
<b>AGRADECIMIENTO</b> -----	vi
<b>ÍNDICE DE CONTENIDO</b> -----	vii
<b>ÍNDICE DE TABLAS</b> -----	xi
<b>ÍNDICE DE FIGURAS</b> -----	xiii
<b>ÍNDICE DE GRÁFICOS</b> -----	xix
<b>ÍNDICE DE ANEXOS</b> -----	xx
<b>RESUMEN</b> -----	xxi
<b>ABSTRACT</b> -----	xxii

### CAPITULO I

#### INTRODUCCIÓN

1.1.	<b>Antecedentes</b> -----	1
1.2.	<b>Problematización</b> -----	3
1.2.1.	<b>Formulación del problema</b> -----	3
1.2.2.	<b>Sistematización del problema</b> -----	3
1.3.	<b>Justificación</b> -----	3
1.3.1.	<b>Justificación Teórica</b> -----	3
1.3.2.	<b>Justificación Práctica</b> -----	4
1.4.	<b>Objetivos</b> -----	4
1.4.1.	<b>Objetivo General</b> -----	4
1.4.2.	<b>Objetivos Específicos</b> -----	4
1.5.	<b>Hipótesis</b> -----	5

### CAPITULO II

#### MARCO DE REFERENCIA

2.1.	<b>Protocolo IPv6</b> -----	6
2.1.1.	<b>Introducción</b> -----	6
2.1.2.	<b>Formato de la cabecera IPv6</b> -----	6
2.1.3.	<b>Direccionamiento</b> -----	7
2.1.4.	<b>Características de IPv6</b> -----	8

2.1.5.	<b>Conceptos básicos de IPv6</b>	9
2.1.5.1.	<i>Dirección de vínculo o enlace local</i>	11
2.1.5.2.	<i>Direcciones IPv6 comunes</i>	12
2.1.6.	<b>Mecanismos de autoconfiguración de IPv6</b>	14
2.1.6.1.	<i>Proceso de autoconfiguración con el protocolo Neighbor Discovery</i>	14
2.1.7.	<b>Problemas de seguridad de IPv6</b>	18
2.1.7.1.	<i>Ataques de reconocimiento</i>	18
2.1.7.2.	<i>Ataques contra el protocolo Neighbor Discovery</i>	19
2.1.8.	<i>ICMPv6 (Protocolo de Mensajes de Control de Internet Versión 6)</i>	22
2.2.	<b>Sistemas detectores de intrusos</b>	24
2.2.1.	<b>Descripción del soporte IPv6 en Snort</b>	24
2.2.2.	<b>Descripción del soporte IPv6 en Suricata</b>	26
2.2.3.	<b>Descripción del soporte IPv6 en BRO</b>	26
2.2.4.	<b>Comparación global de los IDS analizados</b>	27
2.3.	<b>Herramientas relacionadas con la seguridad de IPv6</b>	29
2.3.1.	<b>Evil Foca</b>	29
2.3.2.	<b>SI6 Networks' IPv6 Toolkit</b>	29
2.3.3.	<b>THC-IPv6 Toolkit</b>	30

### CAPITULO III

#### DISEÑO DE INVESTIGACIÓN

3.1.	<b>Tipo de investigación</b>	32
3.2.	<b>Diseño de la investigación</b>	32
3.3.	<b>Métodos y técnicas</b>	32
3.3.1.	<b>Métodos</b>	32
3.3.2.	<b>Técnicas</b>	33
3.3.3.	<b>Fuentes</b>	33
3.4.	<b>Instrumentos</b>	34
3.5.	<b>Validación de instrumentos</b>	34
3.6.	<b>Sistema Detector De Intrusos IPv6</b>	36
3.6.1.	<b>Introducción</b>	36
3.6.2.	<b>Reglas para los patrones de tráfico malicioso</b>	37
3.6.2.1.	<i>Patrón de tráfico IPv6 para ataque de reconocimiento con alive6</i>	39
3.6.2.2.	<i>Patrón de tráfico IPv6 para ataque Mitm con parasite6</i>	40
3.6.2.3.	<i>Patrón de tráfico IPv6 para ataque Mitm con fake-router6</i>	41

3.6.2.4.	<i>Patrón de tráfico IPv6 para ataque de denegación de servicio con flood_advertise6</i>	42
3.6.2.5.	<i>Patrón de tráfico IPv6 para ataque de denegación de servicio con flood_solicitate6</i>	43
3.6.2.6.	<i>Patrón de tráfico IPv6 para ataque de denegación de servicio con flood_router6</i>	44
3.6.2.7.	<i>Patrón de tráfico IPv6 para ataque de denegación de servicio con flood_rs645</i>	
3.6.2.8.	<i>Patrón de tráfico IPv6 para ataque de denegación de servicio con flood_redir6</i>	46
3.6.3.	<b>Infraestructura para la implementación del sistema</b>	47
3.6.4.	<b>Requerimientos software y hardware para la implementación del sistema</b>	48
3.6.5.	<b>Instalación, configuración y acoplamiento del sistema</b>	49
3.6.5.1.	<i>Security Onion</i>	49
3.6.5.2.	<i>Snort</i>	56
3.6.5.3.	<i>Servidor Graylog</i>	57
3.6.5.4.	<i>Instalación del colector de Graylog en Security Onion</i>	60
3.6.5.5.	<i>Inicialización del sistema</i>	65
3.7.	<b>Definición de los escenarios de pruebas</b>	66
3.7.1.	<b>Prototipos de prueba</b>	66
3.7.1.1.	<i>Prototipo I</i>	66
3.7.1.2.	<i>Prototipo II</i>	67
3.7.2.	<b>Experimento 1</b>	67
3.7.3.	<b>Experimento 2</b>	69
3.7.4.	<b>Experimento 3</b>	69
3.7.5.	<b>Experimento 4</b>	70
3.7.6.	<b>Experimento 5</b>	70
3.7.7.	<b>Experimento 6</b>	70
3.8.	<b>Hipótesis</b>	70
3.8.1.	<b>Determinación de variables</b>	70
3.8.2.	<b>Operacionalización conceptual</b>	71
3.8.3.	<b>Operacionalización metodológica</b>	71

## CAPITULO IV

### RESULTADOS Y DISCUSIÓN

4.1.	<b>Desarrollo de las pruebas</b>	72
------	----------------------------------	----

4.1.1.	<b>Prototipo I</b>	72
4.1.1.1.	No. Alertas positivas verdaderas (ataques detectados)	72
4.1.1.2.	No. Alertas falsas positivas	87
4.1.1.3.	Gestión de logs IPv6	91
4.1.1.4.	Replicación de logs IPv6	96
4.1.2.	<b>Prototipo II</b>	98
4.1.2.1.	No. Alertas positivas verdaderas (ataques detectados)	98
4.1.2.2.	No. Alertas falsas positivas	112
4.1.2.3.	Gestión de logs IPv6	116
4.1.2.4.	Replicación de logs IPv6	117
4.2.	<b>Análisis y comparación de resultados</b>	118
4.2.1.	<b>No. Alertas positivas verdaderas (ataques detectados)</b>	118
4.2.2.	<b>No. Alertas falsas positivas</b>	120
4.2.3.	<b>Gestión de logs IPv6</b>	121
4.2.4.	<b>Replicación de logs IPv6</b>	122
4.3.	<b>Prueba de hipótesis</b>	123
4.3.1.	<b>Ambiente de pruebas</b>	123
4.3.2.	<b>Escala de calificación</b>	123
4.3.2.1.	Indicador 1: No. Alertas positivas verdaderas	124
4.3.2.2.	Indicador 2: No. Alertas falsas positivas	124
4.3.2.3.	Indicador 3: Gestión de logs IPv6	124
4.3.2.4.	Indicador 4: Replicación de logs IPv6	125
4.3.3.	<b>Ponderación de los indicadores</b>	125
4.3.3.1.	Indicador 1: No. Alertas positivas verdaderas	125
4.3.3.2.	Indicador 2: No. Alertas falsas positivas	126
4.3.3.3.	Indicador 3: Gestión de logs IPv6	127
4.3.3.4.	Indicador 4: Replicación de logs IPv6	128
4.3.4.	<b>Comprobación de la hipótesis</b>	129
4.3.4.1.	Estadística descriptiva	129
4.3.4.2.	Estadística inferencial	131
	<b>CONCLUSIONES</b>	136
	<b>RECOMENDACIONES</b>	138
	<b>BIBLIOGRAFÍA</b>	
	<b>ANEXOS</b>	

## ÍNDICE DE TABLAS

<b>Tabla 1-2:</b>	Mensajes de error e informativos ICMPv6 .....	23
<b>Tabla 2-2:</b>	Mensajes de detección de vecino ICMPv6.....	24
<b>Tabla 3-2:</b>	Tipos de firmas IPv6 del conjunto de reglas VRT + ET .....	25
<b>Tabla 4-2:</b>	Comparación de los IDS analizados .....	28
<b>Tabla 1-3:</b>	Requerimientos hardware del sistema .....	48
<b>Tabla 2-3:</b>	Requerimientos software del sistema.....	49
<b>Tabla 3-3:</b>	Requerimientos hardware de la máquina atacante .....	49
<b>Tabla 4-3:</b>	Requerimientos software de la máquina atacante.....	49
<b>Tabla 5-3:</b>	Nombre del ataque ejecutado y categorización.....	68
<b>Tabla 6-3:</b>	Intervalos de tiempo experimento 3 .....	69
<b>Tabla 7-3:</b>	Operacionalización conceptual de las variables de la investigación.....	71
<b>Tabla 8-3:</b>	Operacionalización metodológica de las variables de la investigación....	71
<b>Tabla 1-4:</b>	Resultados del indicador No. Alertas Positivas del Prototipo I.....	86
<b>Tabla 2-4:</b>	Resumen de resultados del indicador No. Alertas Positivas del Prototipo I .....	87
<b>Tabla 3-4:</b>	Resumen de resultados del indicador No. Alertas Falsas Positivas del...91	
<b>Tabla 4-4:</b>	Resultados finales del indicador No. Alertas Falsas Positivas del .....	91
<b>Tabla 5-4:</b>	Resumen de resultados del indicador Gestión de logs IPv6 del Prototipo I .....	96
<b>Tabla 6-4:</b>	Resumen de resultados del indicador Replicación de logs IPv6.....	98
<b>Tabla 7-4:</b>	Resultados del indicador No. Alertas Positivas del Prototipo II .....	111
<b>Tabla 8-4:</b>	Resumen de resultados del indicador No. Alertas Positivas del Prototipo II .....	112
<b>Tabla 9-4:</b>	Resumen de resultados del indicador No. Alertas Falsas Positivas del	115
<b>Tabla 10-4:</b>	Resultados finales del indicador No. Alertas Falsas Positivas del.....	116
<b>Tabla 11-4:</b>	Resumen de resultados indicador Gestión de logs IPv6 del Prototipo II .....	117
<b>Tabla 12-4:</b>	Resumen de resultados del indicador Replicación de logs IPv6.....	118
<b>Tabla 13-4:</b>	Resultados del indicador No. Alertas Positivas .....	118
<b>Tabla 14-4:</b>	Resultados del indicador No. Alertas Positivas del Prototipo I y II.....	119
<b>Tabla 15-4:</b>	Resultados del indicador No. Falsos Positivos.....	120

<b>Tabla 16-4:</b> Resultados del indicador No. Alertas Falsas Positivas del Prototipo I y II .....	121
<b>Tabla 17-4:</b> Resultados del indicador Gestión de logs IPv6 del Prototipo I y II.....	121
<b>Tabla 18-4:</b> Resultados del indicador Replicación de logs IPv6 del Prototipo I y II..	122
<b>Tabla 19-4:</b> Tabla de escalas para el Indicador 1: No. Alertas positivas .....	124
<b>Tabla 20-4:</b> Tabla de escalas para el Indicador 2: No. Alertas Falsas Positivas .....	124
<b>Tabla 21-4:</b> Tabla de escalas para el Indicador 3: Gestión de logs IPv6 .....	124
<b>Tabla 22-4:</b> Tabla de escalas para el Indicador 4: Replicación de logs IPv6 .....	125
<b>Tabla 23-4:</b> Códigos del Indicador 1: No. Alertas positivas .....	125
<b>Tabla 24-4:</b> Códigos del Indicador 2: No. Alertas Falsas Positivas .....	126
<b>Tabla 25-4:</b> Códigos del Indicador 3: Gestión de logs IPv6.....	127
<b>Tabla 26-4:</b> Códigos del Indicador 4: Replicación de logs IPv6.....	128
<b>Tabla 27-4:</b> Resultados de indicadores.....	129
<b>Tabla 28-4:</b> Tabla de contingencia de frecuencias observadas.....	132
<b>Tabla 29-4:</b> Tabla de contingencia de frecuencias esperadas.....	132
<b>Tabla 30-4:</b> Calculo de $X^2$ .....	133
<b>Tabla 31-4:</b> Tabla de distribución de $X^2$ .....	135



## ÍNDICE DE FIGURAS

<b>Figura 1-2:</b>	Formato de la Cabecera IPv6.....	7
<b>Figura 2-2:</b>	Direccionamiento IPv6 por defecto en Windows 7.....	9
<b>Figura 3-2:</b>	Ejemplo de configuración de IPv6 en Windows .....	10
<b>Figura 4-2:</b>	Configuración de la NIC por defecto en Windows 7.....	11
<b>Figura 5-2:</b>	Configuración de la NIC por defecto en Mac OS X.....	12
<b>Figura 6-2:</b>	Resolución de direcciones IPv6.....	17
<b>Figura 7-2:</b>	Detección de direcciones duplicadas con colisión .....	18
<b>Figura 8-2:</b>	Paquete NA enviado spoofeando la IPv6 fe80::f47c:d2ae:b534:40b2 ...	20
<b>Figura 9-2:</b>	Paquete NA enviado spoofeando la IPv6 fe80:f95c:b7c5:ea34:d3ff .....	21
<b>Figura 10-2:</b>	Formato general de ICMPv6 .....	22
<b>Figura 11-2:</b>	Firmas IPv6 del conjunto de reglas VRT + ET .....	25
<b>Figura 12-2:</b>	Alertas de tráfico IPv6 obtenidas con Snort.....	25
<b>Figura 13-2:</b>	Alertas de tráfico IPv6 obtenidas con Suricata .....	26
<b>Figura 14-2:</b>	Alertas de tráfico IPv6 obtenidas con Bro.....	27
<b>Figura 1-3:</b>	Logo de Security Onion.....	34
<b>Figura 2-3:</b>	Logo de Snort.....	35
<b>Figura 3-3:</b>	Logo de Graylog.....	35
<b>Figura 4-3:</b>	Módulos del sistema desarrollado .....	36
<b>Figura 5-3:</b>	Estructura de una regla en Snort.....	38
<b>Figura 6-3:</b>	Primer patrón de tráfico IPv6 generado por alive6.....	39
<b>Figura 7-3:</b>	Segundo patrón de tráfico IPv6 generado por alive6 .....	40
<b>Figura 8-3:</b>	Patrón de tráfico IPv6 generado por parasite6 .....	41
<b>Figura 9-3:</b>	Patrón de tráfico IPv6 generado por fake-router6.....	42
<b>Figura 10-3:</b>	Patrón de tráfico IPv6 generado por flood_advertise6 .....	43
<b>Figura 11-3:</b>	Patrón de tráfico IPv6 generado por flood_advertise6 .....	44
<b>Figura 12-3:</b>	Patrón de tráfico IPv6 generado por flood_advertise6 .....	45
<b>Figura 13-3:</b>	Patrón de tráfico IPv6 generado por flood_advertise6 .....	46
<b>Figura 14-3:</b>	Patrón de tráfico IPv6 generado por flood_advertise6 .....	47
<b>Figura 15-3:</b>	Estructura general del sistema detector de intrusos IPv6 propuesto.....	48
<b>Figura 16-3:</b>	Asistente de configuración en Security Onion .....	50
<b>Figura 17-3:</b>	Inicio de configuración de las interfaces de red .....	51
<b>Figura 18-3:</b>	Selección de la interfaz eth2 como administrador.....	51

<b>Figura 19-3:</b>	Selección dinámica o estática de la dirección IP .....	51
<b>Figura 20-3:</b>	Configuración de la interfaz de red en modo monitor .....	52
<b>Figura 21-3:</b>	Selección de la interfaz de red eth3 como monitor .....	52
<b>Figura 22-3:</b>	Cambios guardados de la configuración de interfaces .....	52
<b>Figura 23-3:</b>	Reinicio de Security Onion .....	52
<b>Figura 24-3:</b>	Inicio de configuración del motor detector de intrusos .....	53
<b>Figura 25-3:</b>	Inicio de la configuración avanzada del IDS .....	53
<b>Figura 26-3:</b>	Selección del modo de trabajo del detector de intrusos.....	54
<b>Figura 27-3:</b>	Selección de Snorby como gestor de incidencias.....	54
<b>Figura 28-3:</b>	Selección del motor detector de intrusos .....	54
<b>Figura 29-3:</b>	Selección de las reglas por defecto de Snort.....	55
<b>Figura 30-3:</b>	Habilitación de ingeniería IDS .....	55
<b>Figura 31-3:</b>	Desactivación del IDS Bro.....	55
<b>Figura 32-3:</b>	Habilitación del gestor ELSA .....	56
<b>Figura 33-3:</b>	Finalización de la configuración de Snort y los gestores.....	56
<b>Figura 34-3:</b>	Instrucción para acceder al archivo de configuración de Snort.....	56
<b>Figura 35-3:</b>	Declaración de las redes locales en la configuración de Snort.....	57
<b>Figura 36-3:</b>	Tipos de reglas utilizados por Snort en Security Onion .....	57
<b>Figura 37-3:</b>	Importación del archivo graylog.ova en virtual box .....	58
<b>Figura 38-3:</b>	Preferencias de servicio del servidor Graylog.....	58
<b>Figura 39-3:</b>	Proceso de creación del servidor Graylog .....	59
<b>Figura 40-3:</b>	Pantalla inicial de la máquina virtual del servidor Graylog .....	59
<b>Figura 41-3:</b>	Configuración manual de la hora en el servidor Graylog .....	60
<b>Figura 42-3:</b>	Instrucción para descargar el colector de Graylog.....	61
<b>Figura 43-3:</b>	Instrucción para descomprimir los ficheros de instalación .....	61
<b>Figura 44-3:</b>	Instrucción para realizar un respaldo del archivo de configuración.....	61
<b>Figura 45-3:</b>	Instrucción para editar el archivo de configuración del colector .....	61
<b>Figura 46-3:</b>	Selección de la ruta del servidor Graylog .....	61
<b>Figura 47-3:</b>	Configuración del formato de mensajes de entrada al colector.....	62
<b>Figura 48-3:</b>	Configuración del formato de mensajes de salida al servidor Graylog..	62
<b>Figura 49-3:</b>	Instrucción para inicializar el colector Graylog.....	62
<b>Figura 50-3:</b>	Configuración del servidor Graylog para recibir mensajes desde el colector .....	63
<b>Figura 51-3:</b>	Selección del tipo de mensaje de entrada para el servidor Graylog .....	63
<b>Figura 52-3:</b>	Configuración del puerto y adicionales en el servidor .....	64
<b>Figura 53-3:</b>	Servidor configurado para la recepción de alertas.....	65

<b>Figura 54-3:</b>	Detención de servicios en Security Onion .....	65
<b>Figura 55-3:</b>	Inicialización de Snort en Security Onion .....	66
<b>Figura 56-3:</b>	Estructura general del prototipo I.....	67
<b>Figura 57-3:</b>	Estructura general del prototipo II.....	67
<b>Figura 1-4:</b>	Alerta del ataque de reconocimiento con atk6-alive6 eth0.....	73
<b>Figura 2-4:</b>	Alertas con las direcciones IPv6 obtenidas con atk6-alive6 eth0 .....	73
<b>Figura 3-4:</b>	Alerta del ataque de reconocimiento con atk6-alive6 -4 172.25.0.0/21 eth0 .....	74
<b>Figura 4-4:</b>	Direcciones IPv6 escaneadas con atk6-alive6 -4 172.25.0.0/21 eth0 ...	74
<b>Figura 5-4:</b>	Alertas con las direcciones IPv6 obtenidas con atk6-alive6 -d eth0.....	75
<b>Figura 6-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l eth0.....	75
<b>Figura 7-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -R eth0 ..	76
<b>Figura 8-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -F eth0 ..	76
<b>Figura 9-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -H eth0 ..	77
<b>Figura 10-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -R -F -H	77
<b>Figura 11-4:</b>	Alertas obtenidas al ejecutar atk6-fake_router6 eth0 2001:db8:bad::/64 .....	78
<b>Figura 12-4:</b>	Alertas obtenidas al ejecutar atk6-fake_router6 -H eth0 2001:db8:bad::/64 .....	78
<b>Figura 13-4:</b>	Alertas obtenidas al ejecutar atk6-fake_router6 -D eth0 2001:db8:bad::/64 .....	79
<b>Figura 14-4:</b>	Alertas obtenidas al ejecutar atk6-fake_router6 -F eth0 2001:db8:bad::/64 .....	79
<b>Figura 15-4:</b>	Alertas IPv6 obtenidas con atk6-fake_router6 -H -D eth0 2001:db8:bad::/64.....	80
<b>Figura 16-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_advertise6 eth0 .....	80
<b>Figura 17-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_solicitante6 eth0 .....	81
<b>Figura 18-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_router6 eth0 ...	81
<b>Figura 19-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_router6 -F eth0 .....	82
<b>Figura 20-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 eth0.....	82
<b>Figura 21-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 -s eth0.....	83

<b>Figura 22-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 -S eth0 .....	83
<b>Figura 23-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 -s -S eth0 .....	84
<b>Figura 24-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 eth0.....	84
<b>Figura 25-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 -H eth0.....	85
<b>Figura 26-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 -F eth0 .....	85
<b>Figura 27-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 -H -F eth0 .....	86
<b>Figura 28-4:</b>	Alertas IPv6 obtenidas en el intervalo de 07:00 a 09:59 con el Prototipo I .....	88
<b>Figura 29-4:</b>	Alertas IPv6 obtenidas en el intervalo de 10:00 a 12:59 con el Prototipo I .....	88
<b>Figura 30-4:</b>	Alertas IPv6 obtenidas en el intervalo de 13:00 a 15:59 con el Prototipo I .....	89
<b>Figura 31-4:</b>	Alertas IPv6 obtenidas en el intervalo de 16:00 a 18:59 con el Prototipo I .....	89
<b>Figura 32-4:</b>	Alertas IPv6 obtenidas en el intervalo de 19:00 a 21:00 con el Prototipo I .....	90
<b>Figura 33-4:</b>	Alertas IPv6 obtenidas en el intervalo de 07:00 a 21:00 con el Prototipo I .....	90
<b>Figura 34-4:</b>	Datos estadísticos de la categoría ataques de reconocimiento .....	92
<b>Figura 35-4:</b>	Datos estadísticos de las direcciones IPv6 obtenidas por el atacante ..	92
<b>Figura 36-4:</b>	Datos estadísticos de ataques MITM con la herramienta parasite6 .....	93
<b>Figura 37-4:</b>	Datos estadísticos de ataques MITM con la herramienta fake_router6 ..	93
<b>Figura 38-4:</b>	Datos estadísticos de denegación de servicios con flood_advertise6 ..	94
<b>Figura 39-4:</b>	Datos estadísticos de denegación de servicios con flood_solicitate6 ..	94
<b>Figura 40-4:</b>	Datos estadísticos de denegación de servicios con flood_router6 .....	95
<b>Figura 41-4:</b>	Datos estadísticos de denegación de servicios con flood_rs6 .....	95
<b>Figura 42-4:</b>	Datos estadísticos de denegación de servicios con flood_redir6 .....	96
<b>Figura 43-4:</b>	Archivo de logs IPv6 alojado en el módulo de Security Onion .....	97
<b>Figura 44-4:</b>	Logs IPv6 alojados en el servidor Graylog.....	97
<b>Figura 45-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-alive6 eth0 .....	98
<b>Figura 46-4:</b>	Alertas obtenidas al ejecutar el ataque atk6-alive6 -4 172.25.0.0/21 .....	99
<b>Figura 47-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-alive6 -d eth0.....	99
<b>Figura 48-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l eth0.....	100

<b>Figura 49-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -R eth0 100	
<b>Figura 50-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -F eth0 101	
<b>Figura 51-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -H eth0 101	
<b>Figura 52-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -R -F-H102	
<b>Figura 53-4:</b>	Alertas obtenidas al ejecutar atk6-fake_router6 eth0 2001:db8:bad::/64	102
<b>Figura 54-4:</b>	Alertas obtenidas al ejecutar atk6-fake_router6 -H eth0 2001:db8:bad::/64	103
<b>Figura 55-4:</b>	Alertas obtenidas al ejecutar atk6-fake_router6 -D eth0 2001:db8:bad::/64	103
<b>Figura 56-4:</b>	Error al ejecutar atk6-fake_router6 -F eth0 2001:db8:bad::/64	104
<b>Figura 57-4:</b>	Alertas obtenidas con atk6-fake_router6 -H -D eth0 0 2001:db8:bad::/64	104
<b>Figura 58-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_advertise6 eth0	105
<b>Figura 59-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_solicitate6 eth0	105
<b>Figura 60-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_router6 eth0	106
<b>Figura 61-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_router6 -F eth0	106
<b>Figura 62-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 eth0	107
<b>Figura 63-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 -s eth0	107
<b>Figura 64-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 -S eth0	108
<b>Figura 65-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_rs6 -s -S eth0	108
<b>Figura 66-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 eth0	109
<b>Figura 67-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 -H eth0	109
<b>Figura 68-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 -F eth0	110
<b>Figura 69-4:</b>	Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood_redir6 -H -F eth0	110
<b>Figura 70-4:</b>	Alertas IPv6 obtenidas en el intervalo de 07:00 a 09:59 con el Prototipo II	112
<b>Figura 71-4:</b>	Alertas IPv6 obtenidas en el intervalo de 10:00 a 12:59 con el Prototipo II	113
<b>Figura 72-4:</b>	Alertas IPv6 obtenidas en el intervalo de 13:00 a 15:59 con el Prototipo II	113

<b>Figura 73-4:</b> Alertas IPv6 obtenidas en el intervalo de 16:00 a 18:59 con el Prototipo II .....	114
<b>Figura 74-4:</b> Alertas IPv6 obtenidas en el intervalo de 19:00 a 21:00 con el Prototipo II .....	114
<b>Figura 75-4:</b> Alertas IPv6 obtenidas en el intervalo de 07:00 a 21:00 con el Prototipo II .....	115
<b>Figura 76-4:</b> Sguil gestor interno de Security Onion no compatible para IPv6 .....	116
<b>Figura 77-4:</b> Snorby gestor interno de Security Onion no compatible para IPv6 .....	117
<b>Figura 78-4:</b> Archivo de logs IPv6 alojado en Security Onion .....	118

## ÍNDICE DE GRÁFICOS

<b>Gráfico 1-4:</b>	Comparación del indicador Número de Alertas Positivas.....	120
<b>Gráfico 2-4:</b>	Comparación del indicador Número de Alertas Falsas Positivas .....	121
<b>Gráfico 3-4:</b>	Comparación del indicador Gestión de logs IPv6.....	122
<b>Gráfico 4-4:</b>	Comparación del indicador Replicación de logs IPv6.....	123
<b>Gráfico 5-4:</b>	Resultados obtenidos (de acuerdo a la escala) del Indicador 1: .....	126
<b>Gráfico 6-4:</b>	Resultados obtenidos (de acuerdo a la escala) del Indicador 2: .....	127
<b>Gráfico 7-4:</b>	Resultados obtenidos (de acuerdo a la escala) del Indicador 3: .....	128
<b>Gráfico 8-4:</b>	Resultados obtenidos (de acuerdo a la escala) del Indicador 4: .....	129
<b>Gráfico 9-4:</b>	Resultados de la comparación por Indicador .....	130
<b>Gráfico 10-4:</b>	Resultados totales de la comparación .....	130
<b>Gráfico 11-4:</b>	Curva de $X^2$ .....	135

## ÍNDICE DE ANEXOS

**Anexo A:** Sistemas Operativos más usados en el mercado actual

**Anexo B:** Instalación y configuración de la máquina atacante

**Anexo C:** Experimento 1 desde la Kali Linux

**Anexo D:** Experimento 2 desde la Kali Linux



## RESUMEN

El trabajo de investigación incrementó la seguridad de la red local mediante la detección de ataques dirigidos al protocolo IPv6 que pueden comprometer la confidencialidad, integridad y disponibilidad. Se compararon los indicadores considerados en las variables y se aplicó la estadística descriptiva e inferencial para la demostración de la hipótesis. Las herramientas software utilizadas fueron: Virtual Box que permitió la virtualización de las distribuciones Linux, Security Onion distribución especializada en sistemas detectores de intrusos, Snort como motor del sistema detector, Graylog como gestor de logs IPv6, la suite TCHIPv6 como generador de tráfico IPv6 malicioso y Wireshark como herramienta de análisis de tramas del tráfico IPv6. Se desarrolló, implementó y comparó los resultados obtenidos al trabajar sobre la red local de la Facultad de Informática y Electrónica de la ESPOCH, entre los prototipos I (Security Onion utilizando las reglas personalizadas y acoplado el módulo de gestión de logs) y II (Security Onion utilizando las reglas oficiales de Snort) los cuales obtuvieron una valoración de 16 y 4 puntos de acuerdo a las escalas de Likert respectivamente. Se concluye que el sistema propuesto detecta y gestiona las alertas de intrusión mejorando tres veces el nivel de seguridad dentro de la red local. Se recomienda a los estudiantes o profesionales interesados en el tema dar continuidad al análisis de patrones anormales de tráfico IPv6 con el objetivo de incrementar el número de alertas IPv6 de detección.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA, SEGURIDAD EN REDES> , <PROTOCOLO DE INTERNET VERSIÓN 6 (IPv6)> , <SISTEMA DETECTOR DE INTRUSOS (IDS)> , <CÓDIGO ABIERTO>, <PROGRAMA (SNORT)> , <ALERTAS (LOGS IPv6)> , <FACULTAD DE INFORMÁTICA Y ELECTRÓNICA (FIE)>

## ABSTRACT

The research work has increased security on the local network by detecting attacks targeting the IPv6 protocol that can compromise confidentiality, integrity and availability. We compared the indicators considered in the variables and applied the descriptive and inferential statistics for the demonstration of the hypothesis. The software tools used were: Virtual box that allowed the virtualization of Linux distributions, security Onion, specialized distribution in intrusion detection systems, Snort as detector system engine, Graylog as IPv6 log manager, TCHIPv6 suite as IPv6 traffic generator Malicious and Wireshark as an analysis tool for IPv6 traffic frames. It was developed implemented, and compared the results obtained by working on the local network at the Faculty of Informatics and Electronics from the ESPOCH, among the prototypes I (Security Onion using the custom rules and coupled the logs management module) and II (Security Onion using the official rules of Snort) which obtained a valuation of 16 and 4 points according to the Likert scales respectively. It is concluded that the proposed system detects and manages the intrusion alerts improving three times the level of security within the local network. It is recommended that students or professionals interested in the subject continue the analysis of abnormal patterns of IPv6 traffic in order to increase the number of IPv6 alerts to detect.

Keywords: <TECHNOLOGY AND ENGINEERING SCIENCES> , <SECURITY IN NETWORKS> , <INTERNET PROTOCOL VERSION 6 (IPv6)> , <INTRUDER DETECTOR SYSTEM (IDS) > , <OPEN CODE> , <PROGRAM (SNORT)> , <ALERTS (LOGS IPV6)> , <FACULTY OF COMPUTER SCIENCE AND ELECTRONICS (FIE)>

# CAPITULO I

## 1. INTRODUCCIÓN

### 1.1. Antecedentes

IPv6, la última versión del Protocolo de Internet, está llamado a coexistir con IPv4, y finalmente a sustituirlo, proporcionando un mayor espacio de direcciones que permita impulsar el crecimiento de internet en los próximos años. (GONT, 2014, <http://searchdatacenter.techtarget.com/es/cronica/Mitos-sobre-la-seguridad-en-IPv6-desmontando-falsas-ideas>)

Hay una variedad de aspectos de los protocolos IPv6 que resultan interesantes desde el punto de vista de la seguridad informática. En primer lugar, siendo IPv6 una nueva tecnología, el personal técnico tiene mucha menos confianza con los protocolos IPv6 que con los protocolos IPv4, y por tal motivo es muy probable que sus implicancias de seguridad sean pasadas por alto durante el despliegue de los mismos. En segundo lugar, las implementaciones de IPv6 son mucho menos maduras que las de IPv4, y por tal motivo es muy probable que se descubran en las mismas un gran número de vulnerabilidades. En tercer lugar, productos tales como firewalls y sistemas de detección de intrusos en red, tienen usualmente menor soporte para los protocolos IPv6 que para los protocolos IPv4. Cuarto, las implicancias de seguridad de IPv6 y las diversas tecnologías de transición coexistencia en las actuales redes IPv4 son usualmente ignoradas, potencialmente permitiendo que los atacantes aprovechen estas tecnologías para evadir controles de seguridad IPv4 con técnicas no anticipadas. (GONT, 2013, <http://www.es.hackingipv6networks.com/trainings/hacking-ipv6-networks>)

La detección de intrusos en redes es un enfoque para proporcionar seguridad a las redes informáticas. La detección de intrusiones de red se basa en la creencia de que el comportamiento del atacante será diferente al comportamiento de los usuarios legítimos de la red. Desde hace unos años se está avanzando hacia las redes IPv6 y no hay demanda para asegurarlas. Para proporcionar seguridad a la red IPv6 hay necesidad de una mejor detección de intrusos. Actualmente existen muchas herramientas y técnicas para detectar o evitar intrusiones en IPv4, pero en IPv6 muy pocas herramientas de detección de intrusos están disponibles. Como IPv6 es un nuevo

protocolo para la comunicación a través de Internet es más vulnerable a los ataques. La próxima generación del protocolo IPv6 trae los nuevos retos para la seguridad de la información. (SUMIT & RAVREET, 2013, p. 17)

Actualmente se han realizado varias investigaciones previas en relación al tema en cuestión, entre ellas se destacan:

- La investigación “IPv6 Network Security using Snort” (SUMIT & RAVREET, 2013, pp. 17-22), analiza un caso específico que es la intrusión por fuerza bruta en la red IPv6 para obtener acceso no autorizado. Los autores despliegan una red IPv6, utilizan dos máquinas virtuales en un host físico Ubuntu, el cual se configura como router para reenviar paquetes entre máquinas virtuales. Una máquina virtual la utilizan como atacante y la otra como víctima. Snort está configurado entre el flujo de paquetes de las máquinas virtuales para analizar los paquetes y detectar la intrusión. Sin embargo solo se aplica esta única regla de detección lo cual resulta muy limitante para el sistema y lo deja vulnerable para otro tipo de ataques de IPv6.
- La investigación “A Light-weight Penetration Test Tool for IPv6 Threats” (GU-HSIN, 2014, pp. 49-52), propone utilizar una herramienta común de test de vulnerabilidades IPv6 para atacar a una víctima virtual y generar firmas de ataques IPv6. Utiliza además un sniffer para observar los paquetes de la red y comprobar si cumple con las firmas predefinidas. El sistema sugerido plantea generar un informe para comunicar a los administradores de red si la red IPv6 es vulnerable o no. Sin embargo el autor, solo bosqueja el método a utilizar es decir utilizar firmas como procedimiento principal del sistema pero no especifica las reglas que se van a tomar para definir una firma, ni tampoco sugiere ideas de cómo se implementara el sistema, por lo que lo convierte en un artículo muy general y teórico.
- La investigación “A Study on Detecting ICMPv6 Flooding Attack based on IDS” (SAAD, RAMADASS, & MANICKAM, 2013, p. 175-181), muestra una revisión de literatura relacionada con la seguridad de ICMPv6, se presenta consideraciones y métodos de detección de ataques por inundación del protocolo ICMPv6. En este trabajo los autores proponen mitigar este tipo de ataques con técnicas neuro difusas y de minería de datos a través del uso de Snort. Sin embargo no realizan la implementación, para obtener resultados que puedan establecer la eficiencia o no del sistema.

Muchos de los sistemas de detección de intrusos están configurados para detectar la mayoría de ataques del protocolo IPv4, pero no hacen lo mismo con los ataques IPv6. Por lo que el enfoque original de este proyecto a diferencia de las investigaciones mencionadas es implementar un Prototipo como sistema detector de intrusos, que se utilizara como un recurso adicional para fortalecer la seguridad de una red con soporte IPv6 y servirá para mitigar posibles ataques de usuarios malintencionados u otras amenazas.

## **1.2. Problematización**

### **1.2.1. Formulación del problema**

¿Cuál sería el nivel de mejoría en la seguridad de una red local al implementar un Prototipo como sistema detector de intrusos para detectar ataques dirigidos al protocolo IPv6?

### **1.2.2. Sistematización del problema**

¿Cuáles son los tipos de ataques utilizados para explotar las vulnerabilidades del protocolo IPv6 en una red?

¿Cuáles son las características, ventajas y desventajas de los sistemas detectores de intrusos open source que tienen soporte para el protocolo IPv6?

¿Cuáles son las herramientas open source que permitan generar ataques de intrusión en una red local a través del protocolo IPv6?

¿Cuáles son las técnicas utilizadas para detectar y alertar las anomalías en la red en un sistema detector de intrusos con soporte del protocolo IPv6?

## **1.3. Justificación**

### **1.3.1. Justificación Teórica**

La presente investigación plantea implementar un Prototipo de un sistema detector de intrusos con el objetivo de incrementar la seguridad en una red local ante posibles ataques dirigidos al protocolo IPv6.

Un IDS es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

Actúa sobre una red capturando y analizando paquetes, es decir, es un sniffer del tráfico de red. Luego analiza los paquetes capturados, buscando patrones que supongan algún tipo de ataque y envía una señal de alerta de ser el caso.

### **1.3.2. Justificación Práctica**

El experimento se realizará en un escenario virtualizado, que estará compuesto por varios hosts y el sistema detector de intrusos dentro de una red local. Se enviarán patrones de tráfico malicioso con la ayuda de una herramienta especializada en simular ataques sobre el protocolo IPv6 desde la máquina denominada “atacante” hacia las máquinas denominadas “victimas”. Se observarán las alertas generadas por el sistema de intrusiones y se obtendrán datos, para poder realizar un análisis de resultados sobre su efectividad, con la finalidad de demostrar la mejora de la seguridad.

## **1.4. Objetivos**

### **1.4.1. Objetivo General**

Implementar un Prototipo como sistema detector de intrusos para detectar ataques dirigidos al protocolo IPv6 desarrollado con herramientas open source.

### **1.4.2. Objetivos Específicos**

- Describir los tipos de ataques que pueden realizarse en IPv6 para determinar qué vulnerabilidad del protocolo utilizan y cómo actúan.
- Estudiar las herramientas especializadas de código abierto que permitan generar ataques de intrusión en una red local a través del protocolo IPv6, para la selección de una de ellas como herramienta base.
- Analizar los sistemas detectores de intrusos con soporte de IPv6 y bajo código abierto, para la selección de uno de ellos como sistema base.
- Implementar reglas en el sistema detector de intrusos seleccionado, para generar alertas ante ataques IPv6 de intrusión.

- Comparar los prototipos de pruebas para determinar cuál posee el mayor porcentaje de eficiencia según los indicadores establecidos en la investigación.

### **1.5. Hipótesis**

La implementación de un Prototipo como sistema detector de intrusos con soporte del protocolo IPv6 desarrollado con herramientas open source servirá para mejorar el nivel de seguridad dentro de la red local.

## CAPITULO II

### 2. MARCO DE REFERENCIA

#### 2.1. Protocolo IPv6

##### 2.1.1. Introducción

IPv6 a veces referido como la próxima generación de IP, es la nueva versión del protocolo IPv4 que define direcciones numéricas a los dispositivos en una red y permite la comunicación entre ellos. La necesidad de una nueva versión del protocolo IP vino de algunos problemas asociados a las redes basadas en IPv4 y además el creciente número de redes que requieren acceso a Internet ha creado una escasez de direcciones IPv4. En el primer trimestre del 2011, la ICANN (Corporación de Internet para la Asignación de Nombres y Números) anunció que el último bloque disponible de direcciones IPv4 se había asignado. A pesar de que los usuarios domésticos pueden no necesitar una dirección IP pública para conectarse a Internet, esta escasez representa un problema para las empresas y redes de gran tamaño que requieren de direcciones IPv4 públicas. IPv6 resuelve este problema proporcionando un máximo teórico de  $2^{128}$  direcciones. (AMOL RAWAL, 2014, p. 3)

##### 2.1.2. Formato de la cabecera IPv6

A continuación se describe los campos que componen la cabecera IPv6: (DEERING & HINDEN, 1998, pp. 3-4)

- **Versión:** Campo de 4 bits, con el número 6 como versión del Protocolo de Internet.
- **Clase de Tráfico:** Campo clase de tráfico de 8 bits.
- **Etiqueta de Flujo:** Etiqueta de flujo de 20 bits.
- **Longitud de la Carga Útil:** Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos. (Cualquiera de las cabeceras de extensión presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud).



- **Siguiente cabecera:** Selector de 8 bits, identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4.
- **Límite de Saltos:** Entero sin signo de 8 bits. Disminuido en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos es disminuido hasta cero.
- **Dirección Fuente:** Dirección de 128 bits del originador del paquete.
- **Dirección Destino:** Dirección de 128 bits del destino pretendido del paquete (posiblemente no el último destino, si está presente una cabecera enrutamiento)

El formato de la cabecera IPv6 se muestra en la **Figura 1-2**



**Figura 1-2** Formato de la Cabecera IPv6  
Fuente: Martínez, 2012

### 2.1.3. *Direccionamiento*

Una dirección IPv6 puede ser clasificada en alguno de los tres tipos creados: (**NETWORK INFORMATION CENTER MEXICO S.C.**, 2013, <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>)

- **Unicast:** Se utiliza únicamente para identificar una interface de un nodo IPv6. Un paquete enviado a una dirección unicast es entregado a la interface identificada por esa dirección.
- **Multicast:** Se utiliza para identificar a un grupo de interfaces IPv6. Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.
- **Anycast:** Se asigna a múltiples interfaces (usualmente en múltiples nodos). Un paquete enviado a una dirección anycast es entregado a una de estas interfaces, usualmente la más cercana.

Cada uno de los tres tipos se subdivide en direcciones diseñadas para resolver casos específicos de direccionamiento IP, los cuales a continuación se presentan y describen.

Unicast agrupa los siguientes tipos:

- Enlace Local (Link-Local)
- Sitio Local (Site-Local)
- Agregable Global (Aggregatable Global)
- Loopback
- Sin-Especificar (Unspecified)
- Compatible con IPv4

Anycast agrupa:

- Agregable Global (Aggregatable Global)
- Sitio Local (Site Local)
- Enlace Local (Link Local)

Multicast agrupa:

- Asignada (Assigned)
- Nodo Solicitado (Solicited Node)

#### **2.1.4. Características de IPv6**

IPv6 es la reingeniería y el sucesor del protocolo de internet anterior IPv4. Algunos cambios importantes de IPv4 a IPv6 son: (SCHÜTTE, 2013, p. 410)

**Espacio de direcciones más grande:** Con 128 bits una dirección IPv6 es cuatro veces más grande que una dirección IPv4 de 32 bits y permite muchos más hosts y redes direccionables. Con direcciones IPv4 el inminente agotamiento es el incentivo más importante para desplegar IPv6.

**Cabeceras básicas y de extensión:** El número de campos en la cabecera IPv6 se ha reducido a lo mínimo para que el procesamiento de paquetes por intermedio de los routers sea más eficiente.

**Multicast:** IPv6 pone mayor énfasis en el direccionamiento por multidifusión y depende de ello para la autoconfiguración y descubrimiento de vecinos. Básicamente es un reemplazo más eficiente para las direcciones de broadcast, que se utilizó en IPv4 y ARP (Protocolo de resolución de direcciones) pero ya no se define en IPv6.

**Autoconfiguración y descubrimiento de vecinos:** IPv6 permite que los dispositivos de red puedan configurar sus propias direcciones y rutas sin configuración manual o servicios adicionales de red, como DHCP (Protocolo de configuración dinámica de host).

**Etiquetas de Flujo:** Un nuevo campo se incluye para marcar secuencias de paquetes, como flujos TCP (Protocolo de Control de Transmisión). Lo cual puede ayudar a los routers con el manejo de paquetes de flujos similares, por ejemplo para implementar calidad de servicio sin tener que leer cada paquete de la cabecera Hop-by-Hop (Opciones de salto a salto) o la información de capa superior.

**IPsec:** Brinda soporte para una fuerte autenticación, con integridad de datos y cifrado obligatorio para todos los nodos (en contraste con IPv4 con soporte opcional). Aunque los problemas principales de administración general, impiden su uso generalizado.

### 2.1.5. Conceptos básicos de IPv6

IPv6 se configura automáticamente de forma predeterminada en la mayoría de sistemas operativos y si el usuario final no toma conciencia de ello, puede convertirse en una amenaza a la seguridad. (ELEVEN PATHS, 2013, pp. 2-3)

```
Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . . . : fe80::7043:136:a2e2:afd9%10
Dirección IPv4. . . . . : 192.168.185.75
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.185.1
```

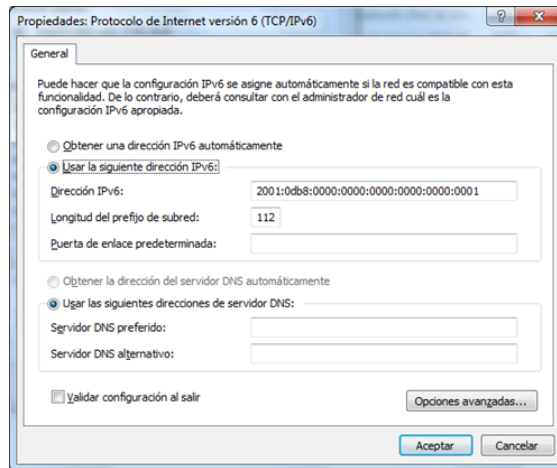
**Figura 2-2** Direccionamiento IPv6 por defecto en Windows 7  
Realizado por: Caiza Diego, 2015

Las direcciones IPv6 se componen de 128 bits separados en grupos de 16 bits en una notación hexadecimal. Esto está representado como 8 grupos de 4 valores hexadecimales. A modo de ejemplo, una dirección IPv6 puede aparecer de la siguiente manera: fe80: 123: 0000: 0000: 0000: 0000: 0000: 1ab0.

Para simplificar esta notación, cuando hay un grupo de cuatro ceros consecutivos podemos utilizar el símbolo "::", por ejemplo la dirección del ejemplo anterior se reduce a: fe80: 123 :: 1ab0.

Esta reducción se puede utilizar una única vez por cada dirección. Una dirección IPv6 común de área local (equivalente en IPv4 a 192.xxx y 10.xxx) podrían ser, por ejemplo, fc00 :: 1.

En segundo lugar, el equivalente de “mascara de red” en IPv4 es llamado prefijo de subred IPv6 o prefijo CIDR (Enrutamiento entre dominios sin clases), como se ve en la **Figura 3-2**



**Figura 3-2** Ejemplo de configuración de IPv6 en Windows  
**Fuente:** Eleventh Paths, 2013

Este término se ha cambiado debido a las cantidades de problemas que causó en muchos usuarios e implementaciones de IPv4 el uso de subnetting, supernetting o la asignación de máscaras de red del tipo 255.0.124.255, algo que fue permitido por el estándar y por tanto en algunas implementaciones, pero que no acababa de tener mucho sentido y causaba problemas a muchos técnicos cuando descubrían su existencia. (ALONSO, 2012, <http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6.html>)

En IPv6 el prefijo tiene la misma función, gestionar la visibilidad de red y utilizarse para hacer subnetting y supernetting. (ELEVEN PATHS, 2013, pp. 3-4)

Por ejemplo, si se tuviera que asignar dos direcciones IPv6 (sin configurar una puerta de enlace), tales como:

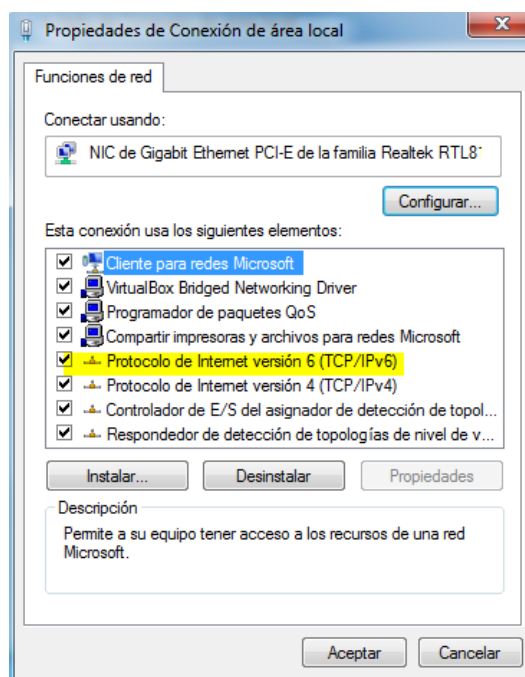
- A: fc00::2000:0001/96
- B: fc00::2001:0001/112

Al enviar una solicitud de ping en IPv6 de A a B se obtendría una respuesta de “Time-Out” y al hacer la misma solicitud de B a A se obtendría una respuesta de “Host inaccesible”, debido a que A no entra dentro de la misma red que B, pero B si está dentro de la misma red que A.

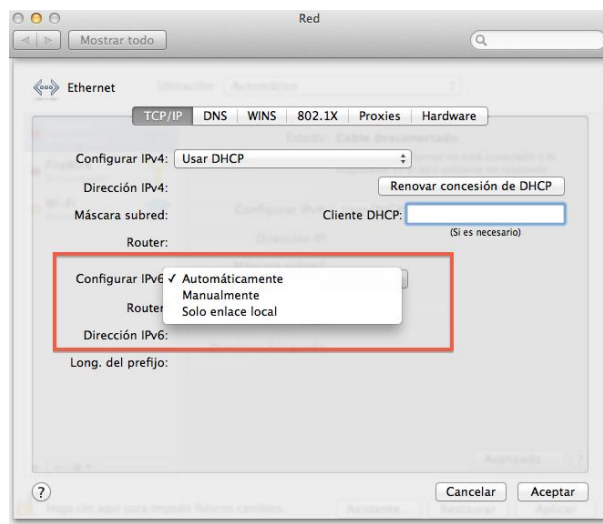
Para interconectar las redes IPv6, igual que en IPv4, es necesario utilizar una Puerta de Enlace o Gateway, que se configura en las propiedades del protocolo de red, igual que los servidores IPv6 que se van a utilizar para la resolución de nombres.

#### 2.1.5.1. Dirección de vínculo o enlace local

Cada NIC (Tarjeta de interfaz de red) que soporta IPv6, no importa si está configurado manual o automáticamente (por defecto en Windows y Mac OS X), como se muestra en la **Figura 4-2** y en la **Figura 5-2**, tendrá una dirección de enlace local asociada.



**Figura 4-2** Configuración de la NIC por defecto en Windows 7  
Realizado por: Caiza Diego, 2015



**Figura 5-2** Configuración de la NIC por defecto en Mac OS X  
**Fuente:** Eleventh Paths, 2013

Esta dirección se genera automáticamente y es anunciada por la red para evitar duplicidad de la misma usando el protocolo NDP (Neighbor Discovery Protocol). Esta duplicidad de direcciones no debería darse de forma habitual, ya que el algoritmo de generación de la misma depende de la dirección MAC (Control de acceso al medio) de la tarjeta, pero para evitar cualquier situación indeseada se hace uso de un sistema que garantice su unicidad y que resuelva estos conflictos. (ALONSO, 2012, <http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6.html>)

Esta dirección es del rango fe80::/10 y es equivalente al rango 169.254.1.X - 169.254.254.X de IPv4. La única diferencia es que en la práctica las direcciones 169.254.X.X no se suelen utilizar en IPv4 y en IPv6 estas direcciones se van a utilizar con mucha frecuencia.

Por supuesto, estas direcciones no son enrutables, pero sí que son utilizadas para comunicarse con el router o cualquier servidor de la organización que se encuentre en la red local. La configuración por defecto asigna una de estas direcciones de enlace local y se puede utilizar por ejemplo para hacer ping a cualquier otra computadora en la red LAN (Red de área local) con una dirección local de enlace IPv6. (ELEVEN PATHS, 2013, p. 5)

#### 2.1.5.2. Direcciones IPv6 comunes

Además de las direcciones de Enlace o Vínculo Local, en IPv6 hay una buena cantidad de direcciones que deben ser conocidas, así que se van a describir las más importantes para entender luego los entornos de ataque:

- **::/128**: Es una dirección con todos los bits a 0. Es la dirección IPv6 indefinida.
- **::/0**: Es la dirección de red IPv6 para describir la ruta por defecto en una tabla de enrutamiento. Es equivalente a la dirección IPv4 0.0.0.0.
- **::1/128**: Local host en IPv6. Equivalente a 127.0.0.1 (IPv4).
- **fe80::/10**: Direcciones de vínculo o enlace local. No son enrutables pero generan una red local efectiva en el rango fe80::/64. La parte de Host se suele calcular a partir de la dirección MAC de la tarjeta.
- **ff02::/16**: Direcciones de redes IPv6 Multicast. Equivalentes a las (224.X) en redes IPv4.
- **fc00::/7**: Son las direcciones para redes IPv6 privadas. Estas direcciones tampoco son enrutables en Internet y son equivalentes a 10.X, 172.16.X y 192.168.X en redes IPv4
- **::ffff:0:0/96**: Direcciones IPv4 mapeadas en IPv6. Se utilizan para conversiones e interconexiones de protocolos IPv4 e IPv6.
- **64:ff9b::/96**: Direcciones IPv6 generadas automáticamente a partir de IPv4. Se utilizan para cuando sea necesario hacer nuevas direcciones IPv6 y se quiera generar a partir de la dirección IPv4 de la máquina.
- **2002::/16**: Indica que es una red 6 to 4 mapeada y utilizará la dirección IPv4 192.88.99.X como Gateway para la interconexión. (ALONSO, El Lado Del Mal, 2012, <http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6.html>)

Además de estas direcciones, hay algunas reservadas para propósitos especiales, como son las siguientes:

- 2001::/32: Usado por el protocolo de túneles Teredo que permite hacer tunneling IPv6 sobre redes IPv4 en Internet. Este sistema es el que se utiliza a la hora de implementar Direct Access en Windows Server 2008 R2 y Windows 7.
- 2001:2::/48: Asignado a Benchmarking Methodology Working Group (BMWG) para comparativas (benchmarking) en IPv6 (similar a la red 198.18.0.0/15 para comparativas en IPv4).
- 2001:10::/28: ORCHID (Overlay Routable Cryptographic Hash Identifiers). Direcciones IPv6 no-enrutables usadas para identificadores criptográficos Hash.
- 2001:db8::/32: Direcciones utilizadas para documentación o ejemplos IPv6. Similar a las redes 192.0.2.0/24, 198.51.100.0/24 y 203.0.113.0/24 en IPv4.

### **2.1.6. Mecanismos de autoconfiguración de IPv6**

IPv6 define dos mecanismos para la autoconfiguración de direcciones IP: stateful y stateless. (AMOL RAWAL, 2014, p. 7)

El mecanismo stateless SLAAC (Autoconfiguración de direcciones libres de estado) permite a los hosts generar sus propias direcciones IP. Este mecanismo utiliza información de la red anunciada por los routers en paquetes llamados “Anuncios de router”, que incluyen el prefijo de subred para el enlace. Los hosts reciben esta información y crean una dirección IPv6 combinando el prefijo y un identificador de interfaz generada automáticamente. En ausencia de los routers, un host puede generar únicamente sus direcciones vínculo local. Sin embargo, las direcciones de vínculo local sólo son suficientes para la comunicación entre los nodos en el mismo enlace.

El mecanismo stateful, ayuda al host a obtener información de configuración de la red desde un servidor DHCPv6. La diferencia entre la configuración stateful y stateless es que el servidor DHCPv6 proporciona el servicio stateful, el recuerda el estado del cliente desde una petición a otra. El servicio stateless no mantiene ningún estado de información.

Se utiliza el mecanismo stateless cuando no se está particularmente interesado con direcciones exactas de los hosts, siempre que sean únicos y adecuadamente enrutables. Un servidor DHCPv6 se utiliza cuando un sitio requiere un control más estricto sobre las asignaciones de direcciones exactas.

#### **2.1.6.1. Proceso de autoconfiguración con el protocolo Neighbor Discovery**

Tan pronto como un dispositivo está conectado a una red IPv6, se puede obtener automáticamente una dirección IP única y adquirir toda la información de enrutamiento necesaria. Esta configuración automática se da a través del protocolo NDP (Protocolo de descubrimiento de vecinos). (SCHÜTTE, 2013, p. 415)

El protocolo de descubrimiento de vecinos se basa en mensajes ICMPv6 (Protocolo de Mensajes de Control de Internet versión 6) y define los siguientes tipos de mensajes:



- **Tipo 133, RS (Solicitud de router):** Mensaje enviado por una interfaz cuando ésta es activada. Se utiliza para solicitar a los routers de la red información sobre la configuración a utilizar.
- **Tipo 134, RA (Anuncio de router):** Mensaje de respuesta enviado por los router ante mensajes de tipo RS. Estos mensajes también se suelen enviar de forma periódica cada cierto intervalo de tiempo.
- **Tipo 135, NS (Solicitud de vecino):** Mensajes enviados por los equipos para averiguar la dirección de capa de enlace de otro equipo. También se utiliza para verificar que el nodo vecino es alcanzable o para detectar direcciones IPv6 duplicadas.
- **Tipo 136, NA (Anuncio de vecino):** Mensaje de respuesta a un NS.
- **Tipo 137, Redir (Redireccionamiento de mensaje):** Mensajes enviados por los equipos de la red para informar que existe una ruta mejor para llegar a un determinado destino. (GONZÁLEZ, 2012, p. 19)

El uso de estos mensajes NDP ofrece una serie de servicios:

#### *2.1.6.1.1. Router discovery*

Los routers IPv6 envían mensajes RA a todos los hosts; tanto no solicitados a intervalos regulares y previa solicitud cuando los hosts envían mensajes RS. Estos mensajes RA contienen la configuración de red básica es decir: la dirección del router en sí, el prefijo de subred, un indicador de si los clientes deben usar DHCPv6 para la configuración y un indicador de tiempo de vida para saber hasta cuando la información es válida. Especificaciones recientes agregan aún más información a los mensajes RA de IPv6, principalmente la configuración DNS, pero esto no está implementado en la mayoría de los sistemas. (SCHÜTTE, 2013, pp. 415-416)

Posteriormente se podrá constatar como ciertos ataques se producen manipulando los parámetros de este tipo de mensajes.

#### *2.1.6.1.2. Redirección del router*

Los routers pueden enviar mensajes de redirección para asesorar a los hosts con las mejores rutas para sus paquetes. Esto ocurre en dos casos: si un router recibe paquetes para la misma subred, entonces se puede informar al remitente de que el destino está en enlace y debe dirigirse directamente; o si una subred tiene varios routers y el router

determina que no está en el camino óptimo, entonces se puede instruir al host para utilizar otro router de primer salto (first hop) para algunos destinos.

Igual que en el caso anterior ciertos ataques se producen manipulando los parámetros de este tipo de mensajes.

#### *2.1.6.1.3. Configuración automática de direcciones*

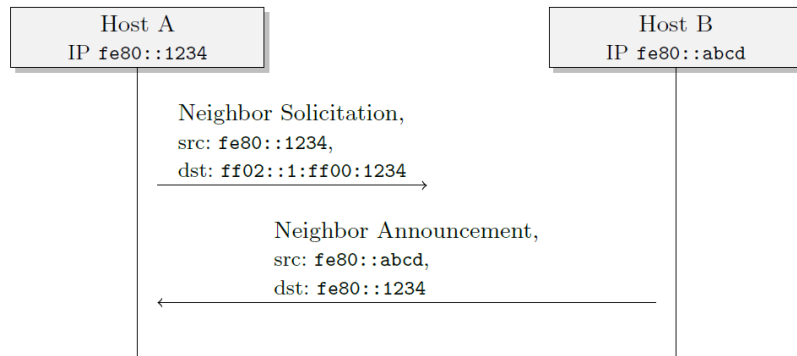
Cada vez que un host se conecta a una red se le asignará una dirección IPv6 de enlace local e iniciara el servicio de router discovery. La IP de enlace local está formado por la concatenación del prefijo de subred de enlace local (fe80:: /10) y el identificador de interfaz según el algoritmo modificado EUI-64.

Por defecto, si los mensajes RA no le dicen que use DHCPv6, un nodo IPv6 utilizará configuración automática de direcciones sin estado (SLAAC) para adquirir su dirección IP global mediante la concatenación del prefijo de subred global y el identificador de interfaz. Pero dependiendo de su configuración también puede utilizar otros esquemas de direccionamiento, por ejemplo, las extensiones de privacidad que utilizan un valor aleatorio como un identificador de interfaz.

#### *2.1.6.1.4. Resolución de direcciones*

Antes de que sea posible cualquier comunicación IP (capa 3), el emisor deberá saber la capa de enlace (capa 2, por ejemplo, Ethernet) de la dirección del host de destino (o del router, si el destino no está en enlace). Para resolver esta dirección, el host utiliza la dirección IP para obtener el grupo de multicast de nodo-solicitado y enviar una solicitud de vecino NS a esa dirección. El destino recibe los mensajes NS y contesta con un mensaje NA que incluye su dirección de capa de enlace.

La dirección de multicast de nodo-solicitado utilizado para este mecanismo se forma con el prefijo de subred: ff02:0:0:0:1:ff00:0 /104 y los últimos 24 bits (3 octetos) de la dirección IPv6. Para cada una de las direcciones unicast y anycast el host tiene que unirse al grupo multicast de nodo-solicitado asociado. Por lo tanto la resolución de dirección se vuelve más eficiente (en comparación con IPv4 usando broadcast ARP) porque incluso en grandes subredes sólo unos anfitriones tienen que recibir y procesar los mensajes NS, como se muestra en la **Figura 6-2**



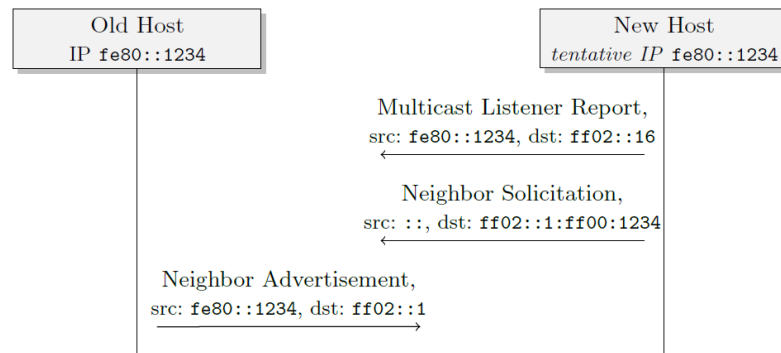
**Figura 6-2** Resolución de direcciones IPv6  
Fuente: Schütte, 2013

#### 2.1.6.1.5. DAD (Detección de direcciones duplicadas)

Antes de que un hosts adquiera una nueva IP se verifica que la dirección no esté usando otro host. El mecanismo es básicamente el mismo de la resolución de direcciones, sólo ligeramente modificado debido a que el host solicitante aún no tiene ninguna dirección IP.

El host obtendrá el grupo de multicast del nodo-solicitado y se unirá a él. Luego este enviará un mensaje NS para la IP provisional (como para la resolución de direcciones, pero tiene que utilizar una dirección no especificada :: como fuente de IP). Si cualquier otro nodo utiliza esta dirección IP, tiene que responder a los mensajes NS mediante un mensaje NA a el grupo multicast del nodo-solicitado, por lo que el nodo solicitante recibirá el NA incluso sin tener una IP. Si no hay respuesta del host al mensaje NS, entonces la IP se supone que esté disponible y el host puede comenzar a utilizarlo. El tiempo de espera aplicado es configurable, por defecto es de un segundo.

En la **Figura 7-2** se puede ver el proceso de detección de direcciones duplicadas con colisión el cual se trata de que inmediatamente después de recibir un mensaje NA del nuevo host se reconoce la colisión o dirección duplicada, por lo que se elige otra IP y se repite el proceso DAD.



**Figura 7-2** Detección de direcciones duplicadas con colisión  
Fuente: SCHÜTTE, 2013

Un host también puede implementar Optimist DAD, el cual acelera el algoritmo y permite al host utilizar la nueva dirección antes de que DAD se complete. Puede ser utilizado para las direcciones con muy baja probabilidad de colisión como direcciones EUI-64, valores aleatorios o asignaciones DHCPv6.

#### 2.1.6.1.6. NUD (Detección de inaccesibilidad de vecino)

Mientras los hosts IPv6 se comunican entre sí, verifican regularmente la accesibilidad de sus pares. Si la capa superior utilizar comunicación bidireccional (es decir, TCP) la verificación es implícita, pero si los protocolos de capa superior son unidireccionales entonces se realiza una comprobación explícita mediante el envío de un mensaje de solicitud de vecinos. Si se detecta el fallo de un host debe iniciar una nueva resolución de la dirección en caso de que la dirección IP se le colocó a otra interfaz de capa de enlace; si el error persiste el par es reconocido con errores inalcanzables y apropiados.

#### 2.1.7. Problemas de seguridad de IPv6

A pesar de los esfuerzos de los diseñadores para crear un protocolo de Internet con seguridad incorporada, IPv6 tiene algunos problemas de seguridad. Es importante recordar que IPv6 no es la solución de la seguridad.

##### 2.1.7.1. Ataques de reconocimiento

Se supone que el aumento de espacio de direcciones en IPv6 imposibilitará el escaneo de direcciones IPv6. Sin embargo, esta afirmación se basa en dos hipótesis que no son necesariamente ciertas en todos los casos. Primero, se da por supuesto que las direcciones de host IPv6 estarán uniformemente distribuidas por todo el espacio de

direcciones asignado a la subred correspondiente. Segundo, se supone que un atacante sólo podrá efectuar un escaneo de direcciones utilizando la fuerza bruta. (GONT, 2014, <http://searchdatacenter.techtarget.com/es/cronica/Mitos-sobre-la-seguridad-en-IPv6-desmontando-falsas-ideas>)

Sin embargo, diversos estudios sobre las políticas empleadas para asignar direcciones IPv6 indican que no están uniformemente distribuidas; más bien siguen patrones específicos, como los resultantes de las configuraciones automáticas sin estado (SLAAC), configuración manual o uso de tecnologías de transición/coexistencia con IPv6. Además, ya se ha descubierto en estado salvaje que los atacantes no efectúan el escaneo de direcciones IPv6 mediante la fuerza bruta, sino que intentan mejorar sus métodos de escaneo aprovechando los ya conocidos patrones de asignación de direcciones IPv6.

#### *2.1.7.2. Ataques contra el protocolo Neighbor Discovery*

De lo indicado anteriormente es obvio cuán importante es NDP para la operación de una red fiable porque todos los hosts dependen de ello para sus funciones más básicas. Como precaución básica los mensajes de descubrimiento de vecinos solamente se procesan on-link (vinculados), sus paquetes IP tienen que incluir un límite de 255 saltos y muchos ataques requieren acceso a los mensajes multicast de vínculo local. Pero con el acceso usualmente a la capa 2 de la red, no garantizado y no autenticado es obvio lo vulnerable que una red local es por las interfaces NDP de nodos maliciosos (o mal configurados) on-link. Así que a pesar de que IPv6 es a menudo visto como una reintroducción del principio de extremo a extremo en el diseño de redes, la condición especial de acceso de enlace local seguirá necesitando seguridad en el perímetro. (SCHÜTTE, 2013, pp. 416-417)

Los posibles ataques pueden ser clasificados por los nodos atacados, ya sean routers o hosts y el resultado que se obtiene es: una denegación de servicio o una configuración de hombre en el medio.

##### *2.1.7.2.1. NS / NA Spoofing*

Estos son ataques en contra del protocolo de descubrimiento de vecinos de hosts normales.

**Neighbor cache poisoning:** El funcionamiento habitual es que un equipo envíe un mensaje NS a una dirección multicast cuando vaya a comunicarse con un equipo y que el que tenga esa dirección IPv6 responda al mensaje multicast con un mensaje unicast de NA con su dirección física MAC. El receptor del mensaje NA almacenará en la tabla de vecinos la dirección IPv6 y la dirección MAC asociada. (ALONSO, 2012, <http://www.elladodelmal.com/2012/11/hacking-en-redes-de-datos-ipv6-neighbor.html>)

Sin embargo, al igual que con el protocolo ARP en IPv4, un atacante puede enviar un mensaje NA sin haber recibido el mensaje previo de NS y hacer que en la caché de la tabla de vecinos se almacene el registro. Un ataque de Neighbor Spoofing para hacer un hombre en el medio, se basará por tanto en enviar un mensaje NA a los dos equipos a los que se quiere hacer el ataque, poniendo en ambos la dirección IPv6 del otro, y la dirección MAC del atacante.

El ataque se realiza spoofeando la dirección IPv6 de origen del paquete, para simular ser un mensaje que viene del otro equipo víctima, pero en ambos casos se pone la dirección MAC del atacante, para conseguir que el switch de comunicaciones haga llegar todos los mensajes a la máquina del hombre en medio, como se muestra en **Figura 8-2** y en la **Figura 9-2**

Source	Destination	Protocol	Length	Info
fe80::f47c:d2ae:b534:40b2	fe80::f95c:b7c5:ea34:d3ff	ICMPv6	86	Neighbor Advertisement
fe80::f95c:b7c5:ea34:d3ff	fe80::f47c:d2ae:b534:40b2	ICMPv6	86	Neighbor Advertisement
fe80::f47c:d2ae:b534:40b2	ff02::1:3	LLMNR	83	Standard query A srv
192.168.1.204	224.0.0.252	LLMNR	63	Standard query A srv
fe80::f95c:b7c5:ea34:d3ff	fe80::f47c:d2ae:b534:40b2	LLMNR	102	Standard query response
192.168.1.204	224.0.0.252	LLMNR	63	Standard query AAAA srv
fe80::f95c:b7c5:ea34:d3ff	fe80::f47c:d2ae:b534:40b2	LLMNR	102	Standard query response
fe80::f47c:d2ae:b534:40b2	fe80::f95c:b7c5:ea34:d3ff	ICMPv6	150	Destination Unreachable

```

Flags: 0x80000000
 0... .. = Router: Not set
 .1.. .. = Solicited: Set
 ..1. .. = Override: Set
 ...0 0000 0000 0000 0000 0000 0000 = Reserved: 0
Target Address: fe80::f47c:d2ae:b534:40b2 (fe80::f47c:d2ae:b534:40b2)
ICMPv6 option (Target link-layer address : 08:00:27:3f:05:4e)
Type: Target link-layer address (2)
Length: 1 (8 bytes)
Link-layer address: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)

```

**Figura 8-2** Paquete NA enviado spoofeando la IPv6 fe80::f47c:d2ae:b534:40b2  
**Fuente:** <http://www.elladodelmal.com/2012/11/hacking-en-redes-de-datos-ipv6-neighbor.html>

Source	Destination	Protocol	Length	Info
fe80::f47c:d2ae:b534:40b2	fe80::f95c:b7c5:ea34:d3ff	ICMPv6	86	Neighbor Advertisement
fe80::f95c:b7c5:ea34:d3ff	fe80::f47c:d2ae:b534:40b2	ICMPv6	86	Neighbor Advertisement
fe80::f47c:d2ae:b534:40b2	192.168.1.204	LLMNR	63	Standard query A srv
192.168.1.204	224.0.0.252	LLMNR	63	Standard query A srv
fe80::f95c:b7c5:ea34:d3ff	fe80::f47c:d2ae:b534:40b2	LLMNR	102	Standard query response
192.168.1.204	224.0.0.252	LLMNR	63	Standard query AAAA srv
fe80::f95c:b7c5:ea34:d3ff	fe80::f47c:d2ae:b534:40b2	LLMNR	102	Standard query response
fe80::f47c:d2ae:b534:40b2	fe80::f95c:b7c5:ea34:d3ff	ICMPv6	150	Destination Unreachable

```

Flags: 0x80000000
 0... .. = Router: Not set
 .1.. .. = Solicited: Set
 ..1. .. = Override: Set
 ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
Target Address: fe80::f95c:b7c5:ea34:d3ff (fe80::f95c:b7c5:ea34:d3ff)
ICMPv6 Option (Target link-layer address : 08:00:27:3f:05:4e)
  Type: Target link-layer address (2)
  Length: 1 (8 bytes)
  Link-layer address: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)

```

**Figura 9-2** Paquete NA enviado spoofeando la IPv6 fe80:f95c:b7c5:ea34:d3ff

**Fuente:** <http://www.elladodelmal.com/2012/11/hacking-en-redes-de-datos-ipv6-neighbor.html>

**Falla NUD:** Si un host inicia la detección de inalcanzabilidad de vecinos (NUD) debido a que otro host ya no responde, entonces un atacante puede enviar falsas respuestas NA para pretender accesibilidad. Este es un ataque sutil de denegación de servicio cuyas consecuencias dependerá del contexto específico; en un caso bastante inofensivo sólo se necesitara más tiempo para el protocolo de capa superior (es decir, TCP) detecte la conexión timeout, mientras que un caso más grave impediría la conmutación en arquitecturas de alta disponibilidad (por ejemplo, si se usa múltiples routers redundantes). (SCHÜTTE, 2013, pp. 416-417)

**DAD DoS:** Un atacante puede escuchar los mensajes NA enviados para la detección de direcciones duplicadas y responder a ellos con su propio NS (pretendiendo realizar una segunda coincidencia DAD para la misma dirección) o un NA (fingiendo ya utilizar la IP). Esta es una situación de denegación de servicio que impide a los hosts unirse a la red (o adquirir direcciones IP adicionales).

#### 2.1.7.2.2. RA / Redir Spoofing

Estos son ataques en contra de los mecanismos de descubrimiento del router.

**Router malicioso:** Un atacante puede simplemente actuar como un router, respondiendo a mensajes de solicitud de router (RS) y enviar regularmente anuncios de router (RA); esto conduce a un escenario de hombre en el medio. Por sí solo esto es poco fiable (el host todavía podría recibir un RA benigno primero), por lo que en la práctica se combina con un ataque temporal "Kill router".

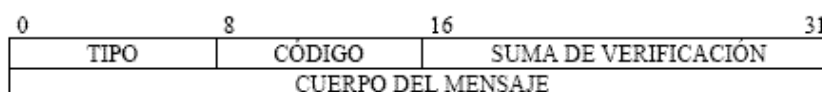
**Kill default router (Eliminar al router por defecto):** Un atacante tiene varias formas de realizar una denegación de servicio contra un router local. Un método consiste en enviar mensajes RA con un tiempo de vida igual a cero, en este caso el cliente descartara la ruta. Otra opción es sobrecargar el router, por ejemplo con un ataque de ancho de banda clásico de denegación de servicio o mediante el envío de paquetes de difícil procesamiento (posiblemente usando encabezados de opción hop-by-hop con muchas opciones o paquetes que requieran verificación criptográfica). Si el router no está disponible los hosts tratarán todos los destinos como on-link. Así que un atacante podría utilizar adicionalmente un envenenamiento de la caché de la tabla de vecinos para ganar una posición de hombre en el medio.

**Falso prefijo de configuración de dirección:** Un atacante puede enviar mensajes RA con un prefijo inválido de subred para realizar un intento de denegación de servicio contra los nuevos hosts. Los nuevos hosts que ejecuten la autoconfiguración de direcciones stateless utilizaran este prefijo para sus direcciones y luego no serán capaces de comunicarse (serán capaces de enviar paquetes, pero las respuestas no llegarán a ellos).

### 2.1.8. ICMPv6 (Protocolo de Mensajes de Control de Internet Versión 6)

El protocolo ICMP (Protocolo de Mensajes de Control de Internet) ha sido actualizado para permitir su uso bajo IPv6. ICMPv6 es una nueva versión de ICMP para IPv6 que debe estar completamente incorporada en todas las implementaciones y nodos IPv6. (VEATO, 2014, <https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/7-icmp-en-ipv6>)

ICMPv6 descrito en el RFC2463, es un protocolo de propósito múltiple que engloba funciones que en IPv4 eran facilitadas por diversos protocolos como ICMP, IGMP o ARP. ICMPv6 está diseñado para realizar funciones tales como detectar y reportar errores que se encuentran durante el procesado de los paquetes, realizar diagnósticos (comando ping), realizar funciones como Neighbor Discovery (equivalente a ARP), detectar direcciones IPv6 de multidifusión (multicast), etc.



**Figura 10-2** Formato general de ICMPv6  
Fuente: <https://ipv6nuevastecredes.wikispaces.com/12+ICMP+v6>



En donde cada uno de estos campos indica:

- Campo Tipo: Indica el tipo de mensaje y su valor determina el formato del resto de la cabecera.
- Campo Código: Depende del tipo de mensaje y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.
- Campo suma de verificación permite detectar errores en el mensaje ICMPv6. (RODRIGUEZ, 2013, <https://ipv6nuevastecredes.wikispaces.com/wiki/members>)

Los mensajes ICMPv6 se agrupan en dos clases: mensajes de error y mensajes informativos. Los mensajes de error tienen cero en el bit de mayor orden en el campo tipo, por lo que sus valores se sitúan entre 0 y 127. Los valores de los mensajes informativos varían entre 128 y 255.

Los mensajes de error de ICMPv6, que son similares a los mensajes de error de ICMPv4, se dividen en 4 categorías: destino inaccesible, paquete demasiado grande, tiempo excedido y problemas de parámetros.

Los mensajes definidos por la especificación básica se muestran en la **Tabla 1-2**

**Tabla 1-2** Mensajes de error e informativos ICMPv6

<b>Mensajes de error ICMPv6</b>		
Tipo	Descripción y códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
4	Puerto no alcanzable	
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo errónea en cabecera
	1	Tipo de Cabecera Siguiendo desconocida
	2	Opción IPv6 desconocida
<b>Mensajes informativos ICMPv6</b>		
Tipo	Descripción	
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Fuente: [http://www.see-my-ip.com/tutoriales/imagen/icmpv6\\_mensajes.jpg](http://www.see-my-ip.com/tutoriales/imagen/icmpv6_mensajes.jpg)

Los mensajes de ICMPv6 utilizados para la detección de vecinos se muestran en la **Tabla 2-2**

**Tabla 2-2** Mensajes de detección de vecino ICMPv6

<b>Tipo</b>	<b>Descripción</b>
<b>133</b>	Mensaje de solicitud del router
<b>134</b>	Mensaje de anuncio del router
<b>135</b>	Mensaje de solicitud de vecino
<b>136</b>	Mensaje de anuncio de vecino
<b>137</b>	Redirección de mensaje

Fuente: Caiza Diego, 2016

Es importante conocer los tipos y parámetros de los mensajes ICMPv6 ya que en base a estos se desarrollaran las reglas de detección de ataques IPv6.

## **2.2. Sistemas detectores de intrusos**

### **2.2.1. Descripción del soporte IPv6 en Snort**

Snort es un sistema de prevención de intrusiones de código abierto capaz de analizar el tráfico en tiempo real y registrar sus paquetes. Con más de 4 millones de descargas y cerca de 500.000 usuarios registrados, es el sistema de prevención de intrusiones de mayor despliegue en el mundo. (CISCO, 2016, <https://www.snort.org/>)

La primera mención de IPv6 en el registro de cambios de Snort muestra que el soporte de IPv6 comienza a aparecer en febrero del 2000, con el lanzamiento de la versión 1.6 ocurrido el siguiente mes. (ALLEN, 2015, pp. 10-18)

Algunos comandos grep rápidos a partir de este artículo demuestran que existen 64 reglas IPv6 específicas en el conjunto de reglas VRT + ET, con 29 reglas habilitadas por defecto en la distribución de Security Onion, como se muestra en la **Figura 11-2**

```
SO-user@so-sensor:/etc/nsm/rules$ grep -i ipv6 \
downloaded.rules | grep -c alert|
64
```

```
SO-user@so-sensor:/etc/nsm/rules$ grep -i ipv6 \
downloaded.rules | grep -cv '#'
29
```

**Figura 11-2** Firmas IPv6 del conjunto de reglas VRT + ET

Fuente: Allen, 2015

La **Tabla 3-2** muestra el desglose de las clases de firmas IPv6 específicas disponibles en la actualidad:

**Tabla 3-2** Tipos de firmas IPv6 del conjunto de reglas VRT + ET

Tipo de firmas	Total
Alerta del protocolo ICMPv6	24
Decodificador de mensajes del protocolo IPv6	24
Metasploit meterpreter binding	8
Otras	8

Fuente: Allen, 2015

En la **Figura 12-2** se muestran varias alertas de tráfico IPv6 obtenidas al utilizar Snort utilizando el gestor Sguil.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	71632	so-snort-eth1-1	1.729653	2015-04-28 12:34:58						http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
RT	8404	so-snort-eth1-1	1.729650	2015-04-28 12:34:58						stream5: TCP Small Segment Threshold Exceeded
RT	2776	so-snort-eth1-1	1.738970	2015-04-28 12:35:47						http_inspect: MESSAGE WITH INVALID CONTENT-LENGTH OR CHUNK SIZE
RT	420	so-snort-eth1-1	1.733331	2015-04-28 12:35:10						http_inspect: CHUNKED ENCODING - EXCESSIVE CONSECUTIVE SMALL CHUNKS
RT	100	so-snort-eth1-1	1.737980	2015-04-28 12:35:39						ET WEB_SERVER CRLF Injection - Newline Characters in URL
RT	49	so-snort-eth1-1	1.735207	2015-04-28 12:35:19						SQL 1 = 1 - possible sql injection attempt
RT	48	so-snort-eth1-1	1.735221	2015-04-28 12:35:19						ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
RT	11	so-snort-eth1-1	1.729773	2015-04-28 12:34:59						ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux style)
RT	10	so-snort-eth1-1	1.734929	2015-04-28 12:35:18						ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt
RT	7	so-snort-eth1-1	1.733815	2015-04-28 12:35:11						stream5: Reset outside window
RT	4	so-snort-eth1-1	1.735771	2015-04-28 12:35:22						ET WEB_SERVER SELECT USER SQL Injection Attempt in URI
RT	2	so-snort-eth1-1	1.729691	2015-04-28 12:34:58						sensitive_data: sensitive data global threshold exceeded
RT	2	so-snort-eth1-1	1.729648	2015-04-28 12:34:58						ET POLICY Unsupported/Fake Windows NT Version 5.0
RT	2	so-snort-eth1-1	1.738969	2015-04-28 12:35:47						ET POLICY ApacheBenchmark Tool User-Agent Detected

**Figura 12-2** Alertas de tráfico IPv6 obtenidas con Snort

Fuente: Allen, 2015

Las firmas históricamente han sido promovidas por el descubrimiento de ataques y su divulgación por razones obvias; por lo que es probable que estos conteos suban y la variedad de clases aumenten a medida que los ataques específicos de IPv6 se descubran y se hagan más frecuentes.

### 2.2.2. Descripción del soporte IPv6 en Suricata

Suricata es un IDS e IPS (Sistema de prevención de intrusiones) de alto rendimiento de red y es un sistema monitor de la seguridad de la red. Es Open Source de propiedad de una fundación sin fines de lucro dirigida a la comunidad, OISF (Fundación de Seguridad de Información Abierta). Suricata es desarrollado por OISF y sus proveedores de apoyo. (OISF, 2015, <http://suricata-ids.org/>)

Sus principales características como IDS es ser: altamente escalable, los protocolos más comunes son reconocidos automáticamente por Suricata en cuanto comienza el flujo de tráfico y posee identificación de archivos, comprobación Checksums MD5 y extracción de archivos.

Suricata utiliza el mismo conjunto de reglas como Snort, por lo que tiene las mismas 64 reglas IPv6 (29 activadas por defecto). Pero adicionalmente tiene un archivo llamado decoder-events.rules, con 32 reglas de decodificador extras, 31 de las cuales están habilitadas por defecto en la distribución de Security Onion, para un total de 96 reglas, con 60 activadas por defecto.

En la **Figura 13-2** se muestran varias alertas de tráfico IPv6 obtenidas al utilizar Suricata utilizando el gestor Sguil.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	so-snort-eth1	2.1	2015-04-25 04:19:49						ET POLICY Unsupported/Fake Windows NT Version 5.0
RT	72	so-snort-eth1	2.3	2015-04-25 04:20:10						ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
RT	69	so-snort-eth1	2.17	2015-04-25 04:20:10						ET WEB_SERVER PHP Possible https Local File Inclusion Attempt
RT	58	so-snort-eth1	2.58	2015-04-25 04:20:12						SQL 1 = 1 - possible sql injection attempt
RT	45	so-snort-eth1	2.188	2015-04-25 04:20:27						ET WEB_SERVER CRLF Injection - Newline Characters in URL
RT	1	so-snort-eth1	2.247	2015-04-25 04:20:31						ET POLICY ApacheBenchmark Tool User-Agent Detected
RT	201	so-snort-eth1	2.248	2015-04-25 04:20:37						SURICATA STREAM FIN2 invalid ack
RT	203	so-snort-eth1	2.249	2015-04-25 04:20:37						SURICATA STREAM Packet with invalid ack
RT	4	so-snort-eth1	2.284	2015-04-25 04:20:37						SURICATA STREAM FIN2 FIN with wrong seq
RT	9	so-snort-eth1	2.288	2015-04-25 04:20:38						SURICATA STREAM CLOSEWAIT ACK out of window
RT	2	so-snort-eth1	2.290	2015-04-25 04:20:38						SURICATA STREAM CLOSEWAIT invalid ACK
RT	2	so-snort-eth1	2.299	2015-04-25 04:20:38						SURICATA STREAM CLOSEWAIT FIN out of window

**Figura 13-2** Alertas de tráfico IPv6 obtenidas con Suricata  
Fuente: Allen, 2015

### 2.2.3. Descripción del soporte IPv6 en BRO

La primera mención de IPv6 en el registro de cambios de Bro muestra que el soporte comienza a aparecer en abril de 2012, con la versión 0.17-8. En las pruebas para este

artículo, Bro no tuvo problemas de decodificación y visualización de tráfico y alertas IPv6.

Pero mientras que el autor no encontró ninguna norma específica de IPv6, vale la pena repetir que la filosofía de Bro es significativamente diferente a cualquiera de las otras dos soluciones IDS bajo análisis.

Como se dijo anteriormente, mientras que Snort y Suricata están basadas en motores de patrones, Bro se centra más en el análisis de patrones de tráfico y como tal los registros y alertas resultantes son significativamente diferentes.

En la **Figura 14-2** se muestran varias alertas de tráfico IPv6 obtenidas al utilizar Bro utilizando líneas de comandos.

```
SO-user@so-sensor:~$ bro-cut note msg src \  
< /nsm/bro/logs/current/notice.log  
HTTP::SQL_Injection_Attacker    An SQL injection attacker was  
discovered!    10.10.2.22  
HTTP::SQL_Injection_VictimAn SQL injection victim was discovered!  
    10.10.2.21  
HTTP::SQL_Injection_Attacker    An SQL injection attacker was  
discovered!    fc00::2  
HTTP::SQL_Injection_VictimAn SQL injection victim was discovered!  
    fc00::1
```

**Figura 14-2** Alertas de tráfico IPv6 obtenidas con Bro  
Fuente: Allen, 2015

#### **2.2.4. Comparación global de los IDS analizados**

La adopción de tráfico IPv6 es creciente y aunque los IDS evaluados apoyan el nuevo protocolo, aún hay mucho trabajo por hacer antes de estar listos para responder a las demandas de consumo de todos los días.

Hay muy pocas firmas desarrolladas específicamente para IPv6 y liberadas al público, pero es potencialmente debido a la falta de ataques específicos para IPv6 descubiertos y expuestos hasta la fecha.

El IDS Bro muestra paridad tanto en la detección y gestión de alertas de ataques en IPv6, pero dada la diferente estrategia de detección, debería ser en capas con un motor más tradicional de IDS para una visión más completa de las clases de ataques en progreso.

En comparación con Snort, el rendimiento de Suricata entre IPv4 e IPv6 fue más consistente, al menos en lo que respecta a las alertas basadas en firmas. Pero el flujo proceso de reensamblaje en Suricata no maneja bien el tráfico IPv6, en relación con el tráfico IPv4.

Por tanto para Snort y Suricata tienen una detección de ataques sobre IPv6 que es comparable a los ataques similares realizados a su predecesor, pero lamentablemente y sorprendentemente carecen de la capacidad de gestionar esas alertas.

En la **Tabla 4-2** se resume la comparación global de los sistemas detectores de intrusos analizados.

**Tabla 4-2** Comparación de los IDS analizados

<b>Parámetro</b>	<b>Snort</b>	<b>Suricata</b>	<b>Bro</b>
Soporte IPv6	Sí	Sí	Sí
Gestión de logs IPv6	No	No	No (Por línea de comandos)
Estrategias de detección	Por firmas de tráfico	Por firmas de tráfico	Por patrones de eventos
Firmas IPv6 de detección	Pocas	Pocas	No
Rendimiento con tráfico IPv6	Muy Bueno	Bueno	Bueno
Detección con tráfico IPv6	Muy Bueno	Bueno	Bueno

Fuente: Allen, 2015

Después de analizar la información recolectada se optó por seleccionar a Snort como el motor adecuado del sistema detector de intrusos para continuar con el presente proceso de investigación.

## 2.3. Herramientas relacionadas con la seguridad de IPv6

### 2.3.1. *Evil Foca*

Evil Foca es una herramienta para pentesters y auditores de seguridad que tiene como finalidad poner a prueba la seguridad en redes de datos IPv4 / IPv6. (ELEVENTH PATHS, 2013, <https://www.elevenpaths.com/es/labstools/evil-focasp/index.html>)

La herramienta es capaz de realizar distintos ataques como:

- MITM sobre redes IPv4 con ARP Spoofing y DHCP ACK Injection.
- MITM sobre redes IPv6 con Neighbor Advertisement Spoofing, Ataque SLAAC, fake DHCPv6.
- DoS (Denegación de Servicio) sobre redes IPv4 con ARP Spoofing.
- DoS (Denegación de Servicio) sobre redes IPv6 con SLAAC DoS.
- DNS Hijacking.

Automáticamente se encarga de escanear la red e identificar todos los dispositivos y sus respectivas interfaces de red, especificando sus direcciones IPv4 e IPv6 y las direcciones físicas a través de una interfaz cómoda e intuitiva.

### 2.3.2. *SI6 Networks' IPv6 Toolkit*

El SI6 Networks' IPv6 Toolkit es un conjunto de herramientas de evaluación de seguridad y solución a problemas en IPv6. Se puede aprovechar para realizar evaluaciones de seguridad de las redes IPv6, evaluar la capacidad de recuperación de los dispositivos IPv6 mediante la ejecución de ataques reales contra ellos, y localizar problemas de averías en una red IPv6. (GONT, 2012, <http://www.si6networks.com/tools/ipv6toolkit/index.html>)

Sus herramientas son:

- **addr6:** Un analizador y herramienta de manipulación de direcciones IPv6.
- **blackhole6:** Una herramienta de solución de problemas que en una topología de red IPv6 puede encontrar en donde los paquetes con cabeceras de extensión IPv6 específicas están siendo rechazadas.

- **flow6**: Una herramienta para llevar a cabo una evaluación de seguridad de la etiqueta de flujo IPv6.
- **frag6**: Una herramienta para realizar ataques basados en la fragmentación de IPv6 y realizar una evaluación de seguridad de una serie de aspectos relacionados con la fragmentación.
- **icmp6**: Una herramienta para realizar ataques basados en mensajes de error ICMPv6.
- **jumbo6**: Una herramienta para evaluar posibles deficiencias en el manejo de Jumbo gramas IPv6.
- **NA6**: Una herramienta para enviar mensajes NA arbitrarios.
- **NI6**: Una herramienta para enviar mensajes ICMPv6 arbitrarios con Información del Nodo, y evaluar posibles fallas en el tratamiento de dichos paquetes.
- **NS6**: Una herramienta para enviar mensajes NS arbitrarios.
- **path6**: Una herramienta trazado de ruta basada en IPv6 versátil (con soporte de cabeceras de extensión, fragmentación de IPv6, y otras características que no están presentes en las implementaciones existentes del trazado de ruta).
- **RA6**: Una herramienta para enviar mensajes RA arbitrarios.
- **RD6**: Una herramienta para enviar mensajes ICMPv6 Redirect arbitrarios.
- **RS6**: Una herramienta para enviar mensajes RS arbitrarios.
- **scan6**: Una herramienta de análisis de direcciones IPv6.
- **script6**: Un conjunto de scripts o comandos que hacen las tareas más complejas y frecuentes fáciles.
- **tcp6**: Una herramienta para enviar segmentos TCP arbitrarios y llevar a cabo una variedad de ataques basados en TCP.
- **udp6**: Una herramienta para el envío de datagramas UDP arbitrarios basados en IPv6.

### 2.3.3. *THC-IPv6 Toolkit*

Es una completa herramienta para atacar las debilidades inherentes de protocolo IPv6 e icmp6, incluye una biblioteca de fábrica de paquetes fácil de usar. (**THE HACKERS CHOICE** , 2015, <https://www.thc.org/thc-ipv6/>)

Dentro de sus principales herramientas se incluyen (**JIMENEZ**, 2012, <http://www.hackplayers.com/2012/10/comprometiendo-ipv6.html>):

- **Parasite6**: anuncio spoofer, se encarga de hacer el arpspoof.



- **Alive6:** un escáner eficaz, que detectará todos los sistemas que estén en su rango de red.
- **Dnsdict6:** permite enumerar las entradas DNS de un dominio. Utiliza un archivo de diccionario si se le proporciona o, en caso contrario, uno propio.
- **Fake\_router6:** para anunciarse como un router en la red, con la más alta prioridad.
- **Redir6:** redirección del tráfico hacia nosotros de forma inteligente (man in the middle).
- **Toobig6:** reductor mtu con la misma inteligencia que redir6.
- **Detect-new-ip6:** detecta nuevos dispositivos ip6 que se unen a la red.
- **Dos-new-ip6:** detecta nuevos dispositivos ip6 y dice que hay conflicto de red (DoS).
- **Trace6:** traceroute6 muy rápido con soportes icmp6, solicitud de eco y TCP -SYN.
- **Flood\_router6:** inundación de un objetivo con anuncios de enrutador al azar.
- **Flood\_advertise6:** inundación de un objetivo con anuncios de neighbor al azar.
- **Exploit6:** prueba las vulnerabilidades conocidas IPv6 contra un blanco.
- **Denial6:** una colección de ensayos de denegación de servicio contra un objetivo.
- **Fuzz\_ip6:** fuzzer para ipv6.
- **Implementation6:** lleva a cabo diversos controles de aplicación sobre ipv6.
- **Implementation6d:** Pone en modo demonio implementation6.
- **Fake\_mld6:** para anunciarse en un grupo multicast de su elección en la red.
- **Fake\_mld26:** lo mismo pero para MLDv2.
- **Fake\_mldrouter6:** falsos mensajes de router MLD.
- **Fake\_mipv6:** robar una IP móvil si IPSEC no es necesario para la autenticación.
- **Fake\_advertiser6:** para anunciarse en la red.
- **Smurf6:** smurfer local
- **Rsmurf6:** smurfer remoto, se sabe que por el momento funciona sólo contra Linux.
- **Thcping6:** envía un paquete ping6 modificado a mano.

Esta suite de pequeñas herramientas, es la más popular dentro del mundo de la seguridad IPv6 y viene incluida en las últimas distribuciones de Kali Linux por lo que se utilizó para ejecutar los ataques planificados en contra del protocolo IPv6.

## CAPITULO III

### 3. DISEÑO DE INVESTIGACIÓN

#### 3.1. Tipo de investigación

La presente investigación es de tipo aplicativo y experimental.

- Aplicativo: ya que se basa en conocimientos existentes, derivados de investigaciones previas, dirigida al desarrollo tecnológico para establecer nuevos procesos para mejorar los existentes.
- Experimental: ya que se basa en pruebas realizadas en escenarios de laboratorio, en las que se observa los elementos más importantes del objeto de estudio que se investiga para obtener una captación de los fenómenos a primera vista.

#### 3.2. Diseño de la investigación

El diseño de la presente investigación es del tipo cuasi experimental, previa recolección de información se seleccionara el sistema detector de intrusos open source más adecuado para el propósito y sobre el mismo se establecerán reglas o firmas con el objetivo de monitorear la red local con soporte IPv6 y mejorar la seguridad interna; además todos los datos de pruebas son originales y generados a partir de esta investigación por el autor.

#### 3.3. Métodos y técnicas

##### 3.3.1. *Métodos*

Para el desarrollo de esta investigación se aplicó el método científico, el mismo que ayuda a seguir una secuencia ordenada de acciones.

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados

- Comprobación de la hipótesis
- Difusión de resultados

### **3.3.2. Técnicas**

Las técnicas utilizadas en la presente investigación son:

- Búsqueda de información: permite obtener la información necesaria acerca del objeto de estudio para su posterior desarrollo, utilizando las fuentes secundarias disponibles.
- Pruebas: permite realizar experimentos en escenarios de laboratorio.
- Observación: permite determinar resultados de las pruebas realizadas en los escenarios de laboratorio.
- Análisis: permite determinar los resultados de la investigación.

### **3.3.3. Fuentes**

Las principales fuentes utilizadas en el estudio de investigación son:

#### **Primarias**

- Pruebas
- Observación de resultados

#### **Secundarias**

- Artículos publicados en revistas científicas indexadas y no indexadas serias.
- Tesis de postgrado publicadas a nivel nacional e internacional con temas afines al investigado.
- Conferencias académicas, congresos, seminarios.
- Sitios Web de los distribuidores de las herramientas open source a utilizar en la investigación.
- Páginas de internet que brinden información confiable y especializada.
- Trabajos de investigaciones internacionales y nacionales.
- Libros especializados de biblioteca y electrónicos.
- Revistas electrónicas.

### 3.4. Instrumentos

Los instrumentos que se utilizó para el desarrollo de la investigación fueron:

- Virtual Box, esta aplicación permite la virtualización de los sistemas operativos que se utilizan para la implementación de las distribuciones Linux Security Onion y Graylog.
- Security Onion, es la distribución especializada en sistemas detectores de intrusos.
- Snort, es el motor del sistema detector su función principal es la detección de patrones de tráfico IPv6 anómalos a través de reglas predefinidas.
- Graylog, permite la gestión de logs IPv6 en modo servidor.
- TCHIPv6, es una suite de herramientas que generan tráfico IPv6 malicioso.
- Wireshark es una herramienta indispensable para detectar trama a trama el tráfico IPv6.

### 3.5. Validación de instrumentos

Los instrumentos software utilizados en la investigación fueron elegidos debido a sus características, beneficios y ventajas, que se mencionan a continuación:

#### Security Onion



**Figura 1-3** Logo de Security Onion

Fuente: <http://blog.securityonion.net/>

Es una distribución de Linux para la detección de intrusos, control de seguridad de la red y de gestión de logs. Está basado en Ubuntu, contiene: Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, Network Miner, y muchas otras herramientas de seguridad. El asistente de configuración es fácil de usar y permite construir un ejército de sensores distribuidos por la empresa en cuestión de minutos. (SECURITY ONION SOLUTIONS, 2015, <https://security-onion-solutions.github.io/security-onion/>)

Para la detección de intrusiones de red basada en reglas, Security Onion ofrece la opción de utilizar Snort o Suricata. Estos sistemas basados en reglas miran al tráfico de red como huellas dactilares y los identificadores que coinciden son conocidos como tráfico malicioso, anómalo o sospechoso. Se podría decir que son semejantes a las

firmas de antivirus de la red, pero son un poco más profundos y más flexibles que eso. (SECURITY ONION SOLUTIONS, 2015, <https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion>)

## Snort



**Figura 2-3** Logo de Snort  
Fuente: <https://www.snort.org/>

Snort es un sistema de prevención de intrusiones en la red de código abierto, capaz de realizar análisis de tráfico en tiempo real y registrar los paquetes de las redes IP. Se puede realizar análisis de protocolos, búsquedas o coincidencias de contenido y es utilizado para detectar una variedad de ataques, tales como desbordamientos de búfer, escaneo de puertos, intentos de fingerprinting y mucho más. (CISCO, 2016, <https://www.snort.org/faq/what-is-snort>)

## Graylog



**Figura 3-3** Logo de Graylog  
Fuente: <https://www.graylog.org/>

Es un gestor de logs de código abierto. Permite tener todos los registros en un solo lugar, centraliza y acumula todos los logs para tener visibilidad del 100%. Utiliza un propio lenguaje de consulta para buscar a través de terabytes de datos de logs para analizar y descubrir información importante. (GRAYLOG INC, 2016, <https://www.graylog.org/>)

Elimina el cuello de botella de la información generada entre los equipos. Brinda a todos un acceso seguro a los datos en tiempo real cuando lo necesitan para colaborar con eficacia, manteniendo su desempeño.

Los componentes de la arquitectura de Graylog se detallan a continuación: (JERONIMO, 2016, <http://javierjeronimo.es/2015/03/23/graylog-arquitectura-tolerante-a-fallos-y-escalable/>)

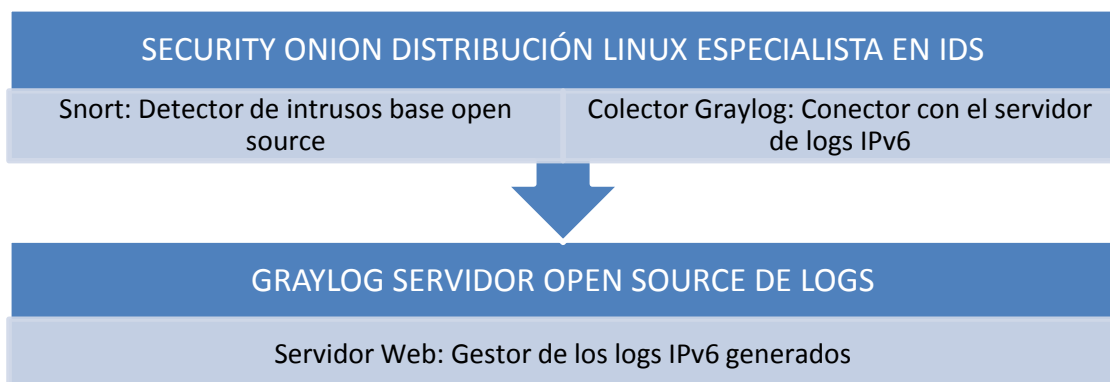
- graylog-server: el núcleo de Graylog2. Procesa los mensajes y los guarda.
  - graylog-radio: Tipo de servidor más ligero, con funciones reducidas.

- Entrada (“input”): Punto de ingesta de datos, es decir de trazas, al sistema. Por ejemplo: protocolo GELF (propio Graylog2) por UDP, TCP, HTTP; syslog, etc.
- graylog-web: Interfaz de consulta y configuración del clúster de Graylog.
- Elasticsearch: Sistema de almacenamiento de registros.
- MongoDB: Base de datos de configuración.

### 3.6. Sistema Detector De Intrusos IPv6

#### 3.6.1. Introducción

El sistema detector de intrusos desarrollado en la investigación se lo puede dividir en dos importantes módulos como se observa en la **Figura 4-3**



**Figura 4-3** Módulos del sistema desarrollado

Realizado por: Caiza Diego, 2016

El primer módulo está constituido por la distribución Linux Security Onion especialista en IDS, la cual se combina de un conjunto de software experto que facilita la monitorización y detección de anomalías en la red.

Dentro de este módulo existen dos componentes indispensables, por un lado Snort como motor detector de intrusos elegido y por otro el colector de Graylog que permite la conexión con el siguiente módulo.

El segundo módulo está constituido por el servidor open source Graylog el cual se encarga de la gestión y administración de logs IPv6 a través de una interfaz web, se acopló al sistema debido a la falta de soporte de logs con direccionamiento IPv6 de los gestores en Security Onion.

### **3.6.2. Reglas para los patrones de tráfico malicioso**

THCIPv6 del grupo Hacker Choise es el software referencial cuando se trata de detectar vulnerabilidades del protocolo IPv6 si su objetivo primordial es evaluar la seguridad de una red de datos. Pero dentro de su suite existen herramientas que debido a la sencillez de uso pueden generar grandes riesgos si son utilizadas por personas malintencionadas.

En el transcurso de la investigación se determinó que la información disponible para ejecutar ataques con esta suite está al alcance de cualquier persona que indague en fuentes primarias y secundarias de información; es por este motivo que se seleccionó las herramientas más populares dentro de todo el conjunto de la suite y aquellas que puedan comprometer la confidencialidad, integridad y disponibilidad en la seguridad de una red local.

La ejecución de cualquiera de estas herramientas altera el comportamiento normal de una red y a la vez generan patrones de tráfico IPv6 anormales, definidos en la investigación como ataques IPv6. Estos ataques dejan un rastro el cual claramente podría ser descubierto por un detector de intrusos; lastimosamente como se ha mencionado, estos sistemas se enfocan principalmente en el tráfico IPv4.

Es por esta razón que fue necesario crear nuevas reglas, específicas para detectar los patrones de tráfico IPv6 generados por la suite THCIPv6, como consecuencia de que las reglas que componen el paquete oficial de Snort no cumplieron con la premisa de identificar este tipo de tráfico.

Para identificar estos patrones de tráfico se utilizó la herramienta Wireshark, la cual permitió efectuar (en el momento de la ejecución de la suite THCIPv6) un análisis byte a byte de todos los paquetes de datos inyectados en la red, con el objetivo de distinguir los tipos de rastros que se producen y con estos datos poder diseñar las reglas personalizadas para detección. Es importante señalar en este apartado que todas las reglas fueron creadas tomando como referencia a ICMPv6 (Protocolo de mensajes de control de internet versión 6) de cada rastro.

Cada una de las reglas que se va a examinar posee una estructura estandarizada como se muestra en la **Figura 5-3**

```
<acción> <protocolo> <red origen> <puerto origen> <dirección> <red destino> <puerto destino>
```

**Figura 5-3** Estructura de una regla en Snort

Fuente: [http://www.adminso.es/index.php/Snort-CABECERA\\_DE\\_UNA\\_REGLA](http://www.adminso.es/index.php/Snort-CABECERA_DE_UNA_REGLA)

En donde, el significado de cada campo es: (UNIVERSIDAD DE ALMERÍA, 2013, [http://www.adminso.es/index.php/Snort-CABECERA\\_DE\\_UNA\\_REGLA](http://www.adminso.es/index.php/Snort-CABECERA_DE_UNA_REGLA))

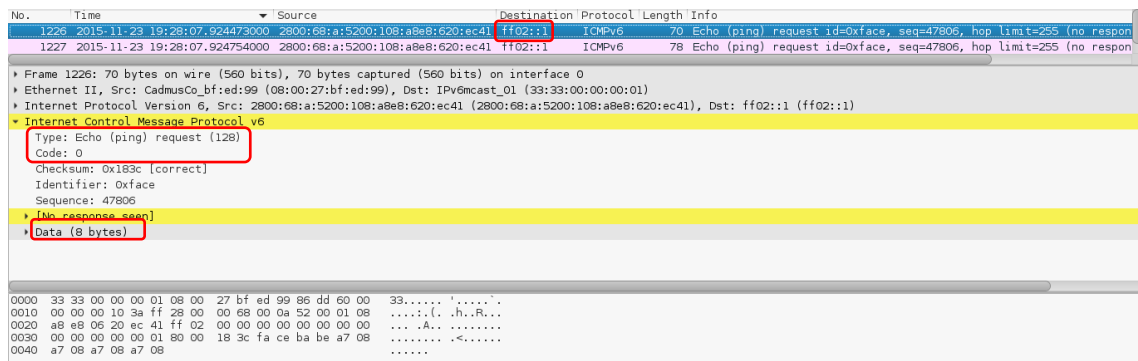
- **Acción:** Permite indicar la acción que se debe realizar sobre dicho paquete. Los posibles valores son:
  - **alert:** Genera una alerta usando el método de alerta seleccionado y posteriormente registra el paquete.
  - **log:** Registra el paquete
  - **pass:** Ignora el paquete
  - **activate:** Activa la alerta y llama a una regla dinámica
  - **dynamic:** Se pone en funcionamiento cuando se activa una regla anterior.
  - **Drop:** Se utiliza en modo inline y le indica a iptables que elimine el paquete.
  - **Reject:** Se utiliza en modo inline y le indica a iptables que rechace el paquete.
  - **Sdrop:** Se utiliza en modo inline y le indica a iptables que elimine el paquete pero no lo registre.
- **Protocolo:** Permite establecer el protocolo de comunicaciones que se va a utilizar. Los posibles valores son: TCP, UDP, ICMP O IP.
- **Red de origen y red de destino:** Permite establecer el origen y destino de la comunicación. Se puede indicar de las siguientes formas:
  - Indicar directamente la dirección de red. Ejemplo: 10.0.0.0/24
  - Indicar el conjunto de direcciones de red utilizando corchetes. Ejemplo: [10.0.0.11, 10.0.0.12]
  - Utilizar variables. Las variables utilizadas por defecto son \$EXTERNAL\_NET (red externa), \$HOME\_NET (red local) y ANY (cualquier red).
- **Puerto de origen y destino:** Permite establecer los puertos origen y destino de la comunicación. Se puede especificar un puerto determinado (ejemplo 80), un rango de puertos (ejemplo 100-200), cualquier puerto (ANY) o cualquier puerto excepto el 80 (ejemplo !80).
- **Dirección:** Permite establecer el sentido de la comunicación. Las posibles opciones son: ->, <- y <>.



### 3.6.2.1. Patrón de tráfico IPv6 para ataque de reconocimiento con alive6

Dentro de la suite THCIPv6 se puede utilizar la herramienta alive6 la cual permite identificar los hosts vecinos que están activos dentro de la red local, se identificó dos patrones de tráfico IPv6, lo que hizo necesario crear dos tipos de reglas.

La primera regla se la diseño de acuerdo al patrón mostrado en la **Figura 6-3**



**Figura 6-3** Primer patrón de tráfico IPv6 generado por alive6  
Realizado por: Caiza Diego, 2016

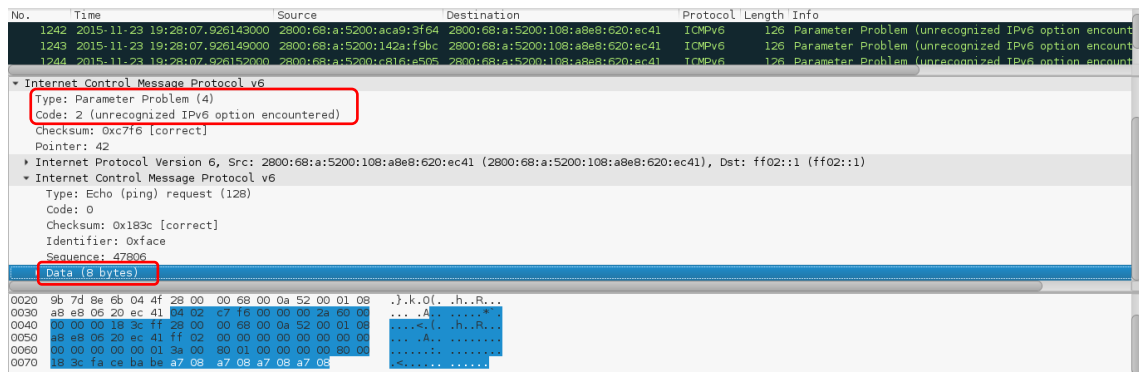
Esta regla reconoce el momento que un host intenta escanear la red para obtener información de los hosts vivos, se activará cuando coincidan con todos los parámetros estipulados de la regla:

```
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE DE RECONOCIMIENTO IPv6 CON THCIPv6 TOOLKIT"; itype:128; icode:0; dsize:8; classtype:network-scan; sid:10000011; rev:3)
```

Es decir:

- Cuando el paquete sea enviado a todos los hosts del enlace local
- Cuando el tipo de mensaje sea del tipo Echo request (128)
- Cuando el código del paquete sea 0
- Cuando el payload del paquete sea de 8
- Adicionalmente pertenecerá al tipo de alerta: escaneo de red, catalogada de riesgo medio.

La segunda regla se la diseño de acuerdo al patrón mostrado en la **Figura 7-3**



**Figura 7-3** Segundo patrón de tráfico IPv6 generado por alive6  
**Realizado por:** Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante obtiene la dirección IPv6 de un host vivo, se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```

alert icmp $HOME_NET any -> $HOME_NET any (msg:"DIRECCIÓN IPv6
ESCANEADA CON THCIPv6 TOOLKIT"; dsize:64; itype:4; icode:2;
classtype:network-scan; sid:10000010; rev:3)

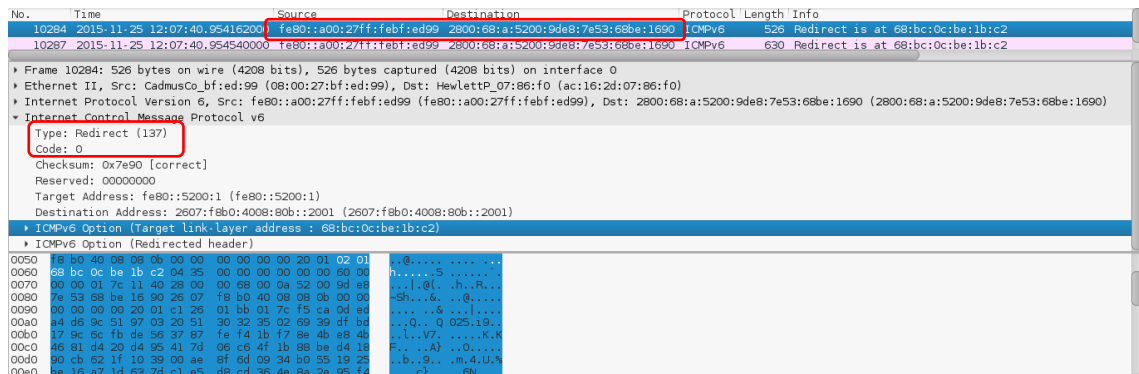
```

Es decir:

- Cuando el paquete sea enviado desde y hacia la red local
- Cuando el tipo de mensaje sea del tipo Parameter Problem (4)
- Cuando el código del paquete sea 2
- Cuando el payload del paquete sea de 64
- Adicionalmente pertenecerá al tipo de alerta: escaneo de red, catalogada de riesgo medio.

### 3.6.2.2. Patrón de tráfico IPv6 para ataque Mitm con parasite6

Dentro de la suite THCIPv6 se puede utilizar la herramienta parasite6 la cual realiza ataques de hombre en el medio con listas de vecinos spoofeados. La regla se la diseño de acuerdo al patrón mostrado en la **Figura 8-3**



**Figura 8-3** Patrón de tráfico IPv6 generado por parasite6  
 Realizado por: Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante redirige todo el tráfico local hacia su sistema, se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```

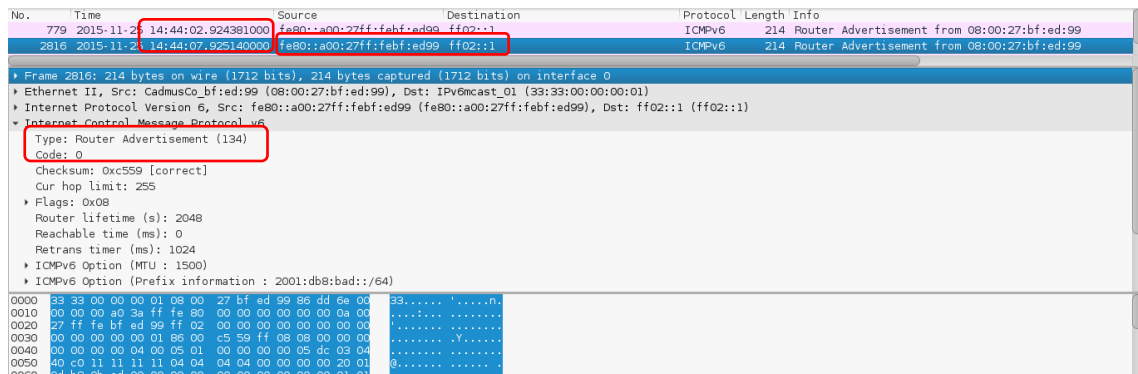
alert icmp $HOME_NET any -> $HOME_NET any (msg:"ATAQUE MITM
PARASITE6 CON THCIPv6 TOOLKIT"; dsize:132<>1236; itype:137;
icode:0; classtype:policy-violation; sid:10000025; rev:3)
  
```

Es decir:

- Cuando el paquete sea enviado desde y hacia la red local
- Cuando el tipo de mensaje sea del tipo Redirect (137)
- Cuando el código del paquete sea 0
- Cuando el payload del paquete este entre 132 y 1236
- Adicionalmente pertenecerá al tipo de alerta: violación de políticas de seguridad, catalogada de riesgo alto.

### 3.6.2.3. Patrón de tráfico IPv6 para ataque Mitm con fake-router6

Dentro de la suite THCIPv6 se puede utilizar la herramienta fake-router6 que permite al equipo anunciarse como router IPv6 con la más alta prioridad. La regla se la diseño de acuerdo al patrón mostrado en la **Figura 9-3**



**Figura 9-3** Patrón de tráfico IPv6 generado por fake-router6  
**Realizado por:** Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante intenta quedar como router por defecto para los otros hosts, se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```
alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FAKE-ROUTER6
CON THCIPv6 TOOLKIT"; dsize:156; itype:134; icode:0;
detection_filter:track by_dst, count 9, seconds 50;
classtype:policy-violation; sid:10000033; rev:3;)
```

Es decir:

- Cuando el paquete sea enviado a todos los hosts del enlace local
- Cuando el tipo de mensaje sea del tipo Router Advertisement (134)
- Cuando el código del paquete sea 0
- Cuando el payload del paquete sea de 156
- Otra conducta adicional de fake-router6 es el de enviar un paquete cada 5 segundos, por lo que se estableció un control adicional de coincidencia para evitar falsos positivos; dicho paquete debe coincidir 9 veces durante 50 segundos desde que inicia el ataque.
- Adicionalmente pertenecerá al tipo de alerta: violación de políticas de seguridad, catalogada de riesgo alto.

### 3.6.2.4. Patrón de tráfico IPv6 para ataque de denegación de servicio con flood\_advertise6

Dentro de la suite THCIPv6 se puede usar la herramienta flood\_advertise6 la cual provoca una inundación con paquetes NA aleatorios sobre la red local. La regla se la diseño de acuerdo al patrón mostrado en la **Figura 10-3**

No.	Time	Source	Destination	Protocol	Length	Info
1114	2015-11-26 17:02:38.289815000	fe80::218:44ff:fe21:c80a	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:44ff:fe21:c80a (ov
1115	2015-11-26 17:02:38.289924000	fe80::218:55ff:fe08:b562	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:55ff:fe08:b562 (ov

Frame 1114: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0 Ethernet II, Src: HeadsUpT_21:c8:0a (00:18:44:21:c8:0a), Dst: IPv6mcast_01 (33:33:00:00:00:01) Internet Protocol Version 6, Src: fe80::218:44ff:fe21:c80a (fe80::218:44ff:fe21:c80a), Dst: ff02::1 (ff02::1) Internet Control Message Protocol v6 Type: Neighbor Advertisement (136) Code: 0 Checksum: 0x32d2 [correct] Flags: 0x20000000 Target Address: fe80::218:44ff:fe21:c80a (fe80::218:44ff:fe21:c80a) ICMPv6 Option (Target Link-Layer address : 00:18:44:21:c8:0a)						
---	--	--	--	--	--	--

0000	33 33 00 00 00 01 00 18	44 21 c8 0a 96 dd 60 00	33..... D1.....
0010	00 00 00 20 3a ff fe 80	00 00 00 00 00 00 02 18	..... D.....
0020	44 ff fe 21 c8 0a ff 02	00 00 00 00 00 00 00 00	D..... D.....
0030	00 00 00 00 00 01 88 00	32 42 20 00 00 00 fe 80	..... 2:.....
0040	88 00 00 00 00 02 18	44 ff fe 21 c8 0a 02 01	..... D.....
0050	00 18 44 21 c8 0a		..D.....

**Figura 10-3** Patrón de tráfico IPv6 generado por flood\_advertise6  
 Realizado por: Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante intenta inundar con mensajes de anuncios de vecinos la red; se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```

alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE
FLOOD_ADVERTISE6 (NA) CON THCIPv6 TOOLKIT"; itype:136; icode:0;
detection_filter:track by_dst, count 50000, seconds 20;
classtype:policy-violation; sid:10000018; rev:3)

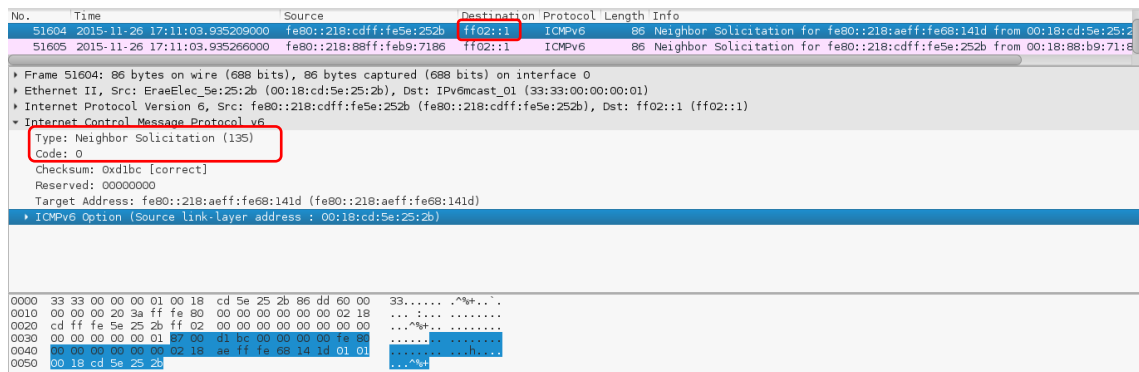
```

Es decir:

- o Cuando el paquete sea enviado a todos los hosts del enlace local
- o Cuando el tipo de mensaje sea del tipo Neighbor Advertisement (136)
- o Cuando el código del paquete sea 0
- o Otra conducta adicional de flood\_advertise6 es el de enviar miles de paquetes en periodos de tiempo muy pequeños, por lo que se estableció un control adicional de coincidencia para evitar falsos positivos; dicho paquete debe coincidir 50000 veces en 20 segundos desde que inicia el ataque.
- o Adicionalmente pertenecerá al tipo de alerta: violación de políticas de seguridad, catalogada de riesgo alto.

### 3.6.2.5. Patrón de tráfico IPv6 para ataque de denegación de servicio con flood\_solicitare6

Dentro de la suite THCIPv6 se puede usar la herramienta flood\_solicitare6 la cual provoca una inundación con paquetes NS aleatorios sobre la red local. La regla se la diseño de acuerdo al patrón mostrado en la **Figura 11-3**



**Figura 11-3** Patrón de tráfico IPv6 generado por flood\_advertise6  
**Realizado por:** Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante intenta inundar con falsos mensajes de solicitud de vecino; se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```

alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE
FLOOD_SOLICITATE6 (NS) CON THCIPv6 TOOLKIT"; itype:135; icode:0;
detection_filter:track by_dst, count 50000, seconds 20;
classtype:policy-violation; sid:10000020; rev:3)

```

Es decir:

- o Cuando el paquete sea enviado a todos los hosts del enlace local
- o Cuando el tipo de mensaje sea del tipo Neighbor Solicitation (135)
- o Cuando el código del paquete sea 0
- o Otra conducta adicional de flood\_solicitatie6 es el de enviar miles de paquetes en periodos de tiempo muy pequeños, por lo que se estableció un control adicional de coincidencia para evitar falsos positivos; dicho paquete debe coincidir 50000 veces en 20 segundos desde que inicia el ataque.
- o Adicionalmente pertenecerá al tipo de alerta: violación de políticas de seguridad catalogada de riesgo alto.

### 3.6.2.6. Patrón de tráfico IPv6 para ataque de denegación de servicio con flood\_router6

Dentro de la suite THCIPv6 se puede usar la herramienta flood\_router6 la cual provoca una inundación con paquetes RA aleatorios sobre la red local. La regla se la diseño de acuerdo al patrón mostrado en la **Figura 12-3**

No.	Time	Source	Destination	Protocol	Length	Info
324922	2015-11-26 19:46:10.742081000	fe80::218:9dff:fe16:5628	ff02::1	ICMPv6	118	Router Advertisement from 00:18:9d:16:56:28
324923	2015-11-26 19:46:10.742153000	fe80::218:44ff:fe78:24a1	ff02::1	ICMPv6	118	Router Advertisement from 00:18:44:78:24:a1

```

* Frame 324922: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
* Ethernet II, Src: Navcast_16:56:28 (00:18:9d:16:56:28), Dst: IPv6mcast_01 (33:33:00:00:00:01)
* Internet Protocol Version 6, Src: fe80::218:9dff:fe16:5628 (fe80::218:9dff:fe16:5628), Dst: ff02::1 (ff02::1)
* Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0xc946 [correct]
  cur hop limit: 255
  Flags: 0x09
  Router lifetime (s): 65535
  Reachable time (ms): 16384000
  Retrans timer (ms): 1966080
  * ICMPv6 Option (MTU : 1500)
0000 33 33 00 00 01 00 18 9d 16 56 28 e6 dd 60 00 33.....V(..
0010 00 00 00 40 3a ff fe 80 00 00 00 00 00 02 18 ...@:..
0020 9d ff fe 16 56 28 ff 02 00 00 00 00 00 00 00 ...V(..
0030 00 00 00 00 01 86 00 c9 46 ff 08 ff ff 00 fa .....F.....
0040 00 00 00 1e 00 05 01 00 00 00 05 dc 03 04 @.....*.....
0050 40 e0 ff ff ff ff ff ff ff ff 00 00 00 2a 01 }..).Q.....
0060 5d ac e6 29 0d 51 00 00 00 00 00 00 01 01 }..).Q.....
0070 00 18 9d 16 56 28 .....V(

```

**Figura 12-3** Patrón de tráfico IPv6 generado por flood\_advertise6  
Realizado por: Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante intenta inundar con falsos mensajes de anuncios de un router; se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```

alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_ROUTER6
(RA) CON THCIPv6 TOOLKIT"; dsize:60; itype:134; icode:0;
detection_filter:track by_dst, count 50000, seconds 20;
classtype:policy-violation; sid:10000019; rev:3)

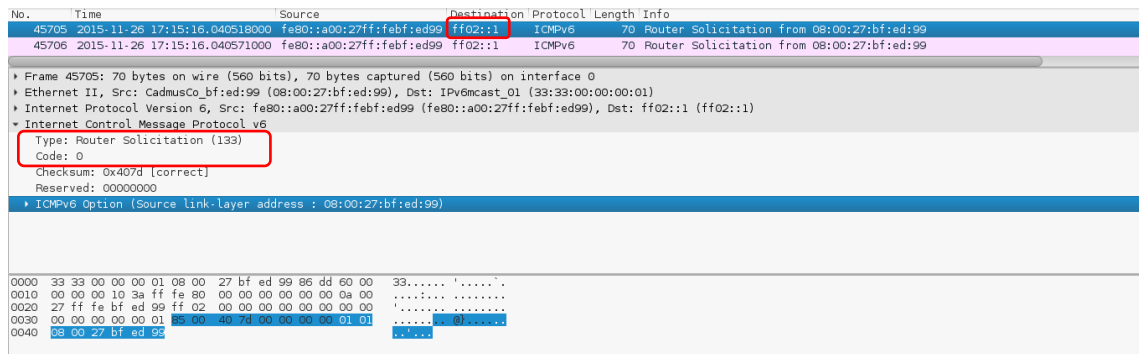
```

Es decir:

- o Cuando el paquete sea enviado a todos los hosts del enlace local
- o Cuando el tipo de mensaje sea del tipo Router Advertisement (134)
- o Cuando el código del paquete sea 0
- o Otra conducta adicional de flood\_router6 es el de enviar miles de paquetes en periodos de tiempo muy pequeños, por lo que se estableció un control adicional de coincidencia para evitar falsos positivos; dicho paquete debe coincidir 50000 veces en 20 segundos desde que inicia el ataque.
- o Adicionalmente pertenecerá al tipo de alerta: violación de políticas de seguridad, catalogada de riesgo alto.

### 3.6.2.7. Patrón de tráfico IPv6 para ataque de denegación de servicio con flood\_rs6

Dentro de la suite THCIPv6 se puede usar la herramienta flood\_rs6 la cual provoca una inundación con paquetes RS aleatorios sobre la red local. La regla se la diseño de acuerdo al patrón mostrado en la **Figura 13-3**



**Figura 13-3** Patrón de tráfico IPv6 generado por flood\_advertise6  
 Realizado por: Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante intenta inundar con falsos mensajes de solicitud de router; se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```

alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_RS6
(RS)      CON      THCIPv6      TOOLKIT";      itype:133;      icode:0;
detection_filter:track by_dst, count 50000, seconds 20;
classtype:policy-violation; sid:10000021; rev:3)
  
```

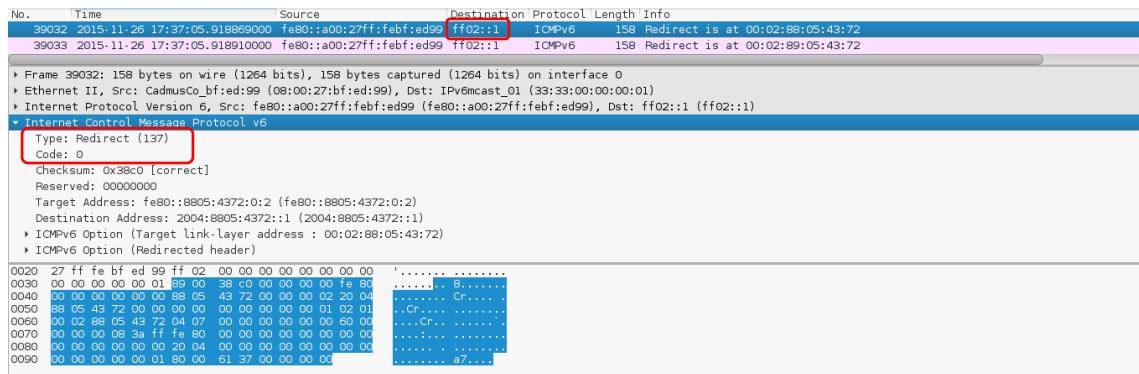
Es decir:

- o Cuando el paquete sea enviado a todos los hosts del enlace local
- o Cuando el tipo de mensaje sea del tipo Router Solicitation (133)
- o Cuando el código del paquete sea 0
- o Otra conducta adicional de flood\_solicitate6 es el de enviar miles de paquetes en periodos de tiempo muy pequeños, por lo que se estableció un control adicional de coincidencia para evitar falsos positivos; dicho paquete debe coincidir 50000 veces en 20 segundos desde que inicia el ataque.
- o Adicionalmente pertenecerá al tipo de alerta: violación de políticas de seguridad, catalogada de riesgo alto.

### 3.6.2.8. Patrón de tráfico IPv6 para ataque de denegación de servicio con flood\_redir6

Dentro de la suite THCIPv6 se puede usar la herramienta flood\_redir6 la cual provoca una inundación con paquetes RE aleatorios sobre la red local. La regla se la diseño de acuerdo al patrón mostrado en la **Figura 14-3**





**Figura 14-3** Patrón de tráfico IPv6 generado por flood\_advertise6  
 Realizado por: Caiza Diego, 2016

Esta regla reconoce el momento que un host atacante intenta inundar con falsos mensajes de redireccionamiento; se activará cada vez que coincidan con todos los parámetros estipulados de la regla:

```

alert icmp $HOME_NET any -> ff02::1 any (msg:"ATAQUE FLOOD_REDIR6
(RE)      CON      THCIPv6      TOOLKIT";      itype:137;      icode:0;
detection_filter:track by_dst, count 50000, seconds 20;
classtype:policy-violation; sid:10000022; rev:3)

```

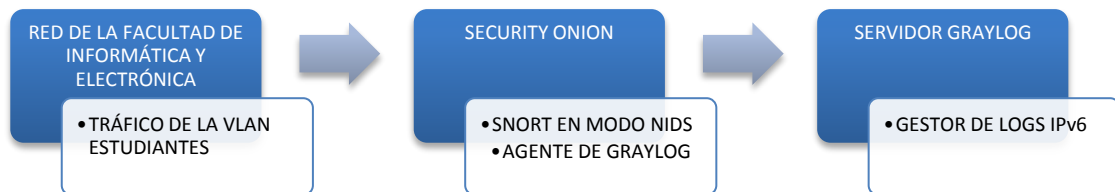
Es decir:

- Cuando el paquete sea enviado a todos los hosts del enlace local
- Cuando el tipo de mensaje sea del tipo Redirect (137)
- Cuando el código del paquete sea 0
- Otra conducta adicional de flood\_redir6 es el de enviar miles de paquetes en periodos de tiempo muy pequeños, por lo que se estableció un control adicional de coincidencia para evitar falsos positivos; dicho paquete debe coincidir 50000 veces en 20 segundos desde que inicia el ataque.
- Adicionalmente pertenecerá al tipo de alerta: violación de políticas de seguridad.

### 3.6.3. Infraestructura para la implementación del sistema

Una vez diseñadas la reglas del motor detector de intrusos se procedió a acoplar el sistema, todas las pruebas se realizan en el mismo escenario debido a que se usa la infraestructura de la red de la FIE (Facultad de Informática y Electrónica) de la ESPOCH, específicamente se trabaja con la VLAN de Estudiantes aprovechando el tráfico nativo bajo IPv6.

El administrador de red de la Dirección de Tecnologías de la Información y Comunicación, configuro un puerto del Switch de distribución del Edificio de la FIE, en modo SPAN (Switched Port Analyzer) permitiéndole al Prototipo a través de este puerto tener acceso a todo el tráfico que circula en la VLAN.



**Figura 15-3** Estructura general del sistema detector de intrusos IPv6 propuesto  
Realizado por: Caiza Diego, 2016

Una vez instalado el Prototipo en la sala de servidores se procedió a realizar las pruebas desde cualquiera de los laboratorios del edificio, de esta forma la máquina denominada atacante empezará a inyectar tráfico malicioso sobre la red local. Las computadoras de los laboratorios de la FIE que estén conectadas a la VLAN se denominarán máquinas víctimas.

Para demostrar el correcto funcionamiento, el Prototipo debe ser capaz de detectar el tráfico anómalo y generar alertas identificando el tipo de ataque que se ha realizado desde la máquina atacante con la herramienta THCIPv6.

Los Logs de alertas que se originen durante la fase de pruebas quedarán almacenados en el servidor Graylog, el mismo facilitará la posterior gestión y manejo de los datos, para desarrollar en el siguiente capítulo el análisis de los resultados obtenidos.

#### **3.6.4. Requerimientos software y hardware para la implementación del sistema**

Los requerimientos hardware y software para implementar el sistema detector de intrusos dentro de la red de FIE se detallan en la **Tabla 1-3** y en la **Tabla 2-3**

**Tabla 1-3** Requerimientos hardware del sistema

Equipo	Cantidad
Switch Cisco (Switch distribuidor del edificio) configurado con un puerto en modo SPAN y uno en modo access para administración	1
Laptop Toshiba Satellite S55-b, procesador Intel® Core™ I7-5500U- 2.45 GHZ, y 12 GB en RAM	1

Adaptador USB 3.0 a Ethernet Gigabit Trendnet modelo TU3-ETG.	1
Cable UTP CAT5e	2

Realizado por: Caiza Diego, 2016

**Tabla 2-3** Requerimientos software del sistema

Descripción	Cantidad
Virtual Box 5.0	1
Máquina virtual con la distribución Security Onion 12.04.5.3	1
Snort 2.7.	1
Máquina virtual con la distribución Graylog 1.3	1

Realizado por: Caiza Diego, 2016

Los requerimientos hardware y software de la máquina atacante se detallan en la **Tabla 3-3** y en la **Tabla 4**

**Tabla 3-3** Requerimientos hardware de la máquina atacante

Equipo	Cantidad
Pc de escritorio o portátil con soporte de virtualización	1
Punto de Red de los laboratorios de la FIE	1
Cable UTP CAT5e	1

Fuente: Caiza Diego, 2016

**Tabla 4-3** Requerimientos software de la máquina atacante

Descripción	Cantidad
Máquina virtual con la distribución Kali Linux 2.0	1
Suite de herramientas THCIPv6	1
Wireshark	1

Fuente: Caiza Diego, 2016

### **3.6.5. Instalación, configuración y acoplamiento del sistema**

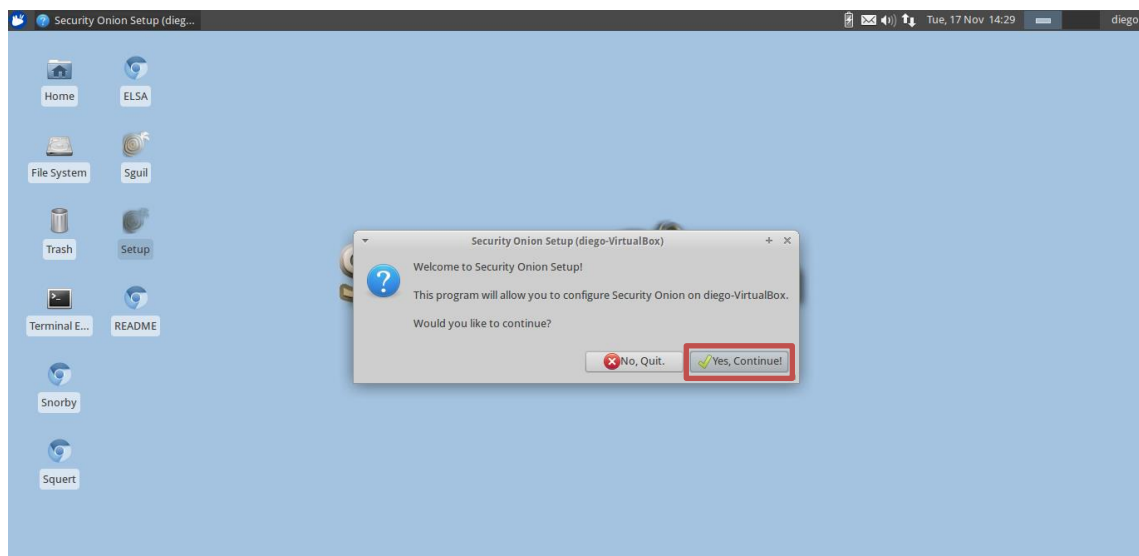
#### **3.6.5.1. Security Onion**

En esta parte del documento se va a detallar la:

- Instalación de la máquina virtual con la distribución Security Onion 12.04.5.3
- Configuración de las interfaces de red necesarias para el sistema
- Habilitación de los gestores de incidencia
- Habilitación del motor del sistema detector de intrusos.

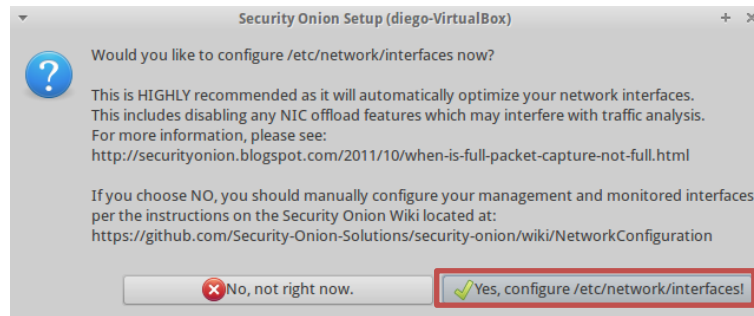
El primer paso para instalar la distribución Linux de Security Onion en la máquina virtual es descargar el archivo securityonion-12.04.5.3-20150825.iso desde la dirección <http://sourceforge.net/projects/security-onion/files/12.04.5.3/securityonion-12.04.5.3-20150825.iso/download>. Para una correcta instalación es recomendable revisar la página oficial de la distribución <https://security-onion-solutions.github.io/security-onion/>, en donde se encuentra explicado en videos tutoriales la forma correcta de hacerlo. Una vez instalado Security Onion se configuran las dos interfaces de red requeridas, la primera interfaz se utiliza para administración y está conectada a un puerto en modo access del switch de distribución del edificio de la FIE, mientras que la otra interfaz está conectada al puerto spam para escuchar todo el tráfico que circula por la VLAN que se va a monitorear.

La configuración es sencilla ya que Security Onion cuenta con un asistente grafico a través del cual se puede ir estableciendo la configuración. Se accede mediante el icono Setup como se muestra en la **Figura 16-3**. Es necesario especificar ciertos parámetros de trabajo, como se indican en las figuras posteriores.



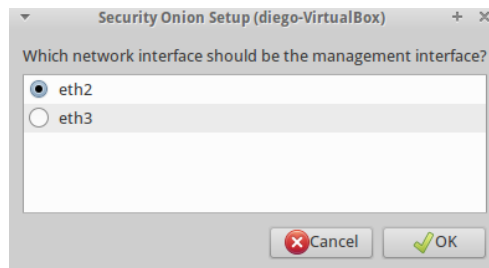
**Figura 16-3** Asistente de configuración en Security Onion  
Realizado por: Caiza Diego, 2016

La **Figura 17-3** muestra el inicio de la configuración de las interfaces de red que se van a utilizar en la implementación del sistema



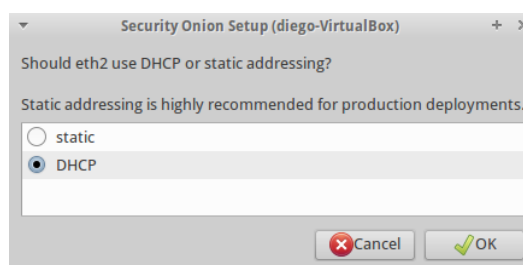
**Figura 17-3** Inicio de configuración de las interfaces de red  
Realizado por: Caiza Diego, 2016

El primer paso dentro de la configuración es seleccionar la interfaz de red que se va a utilizar para la administración, como se muestra en la **Figura 18-3**. En el montaje físico del sistema eth2 corresponde al adaptador de red Trendnet, sus características se especifican en los requerimientos de hardware descritos posteriormente.



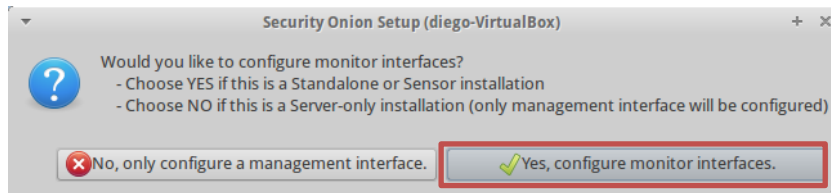
**Figura 18-3** Selección de la interfaz eth2 como administrador  
Realizado por: Caiza Diego, 2016

Se especifica si se usa DHCP o una dirección estática, para el caso se eligió que la dirección ip sea resuelta a través del servidor DHCP, como se muestra en la **Figura 19-3**. Esta selección depende de la infraestructura en donde se vaya a implantar el Prototipo.



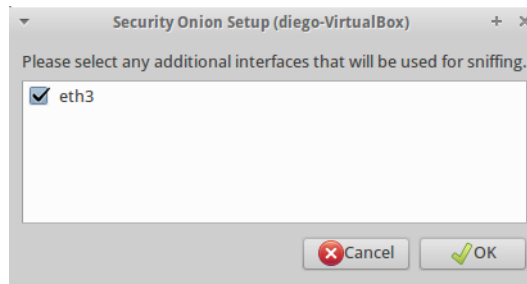
**Figura 19-3** Selección dinámica o estática de la dirección IP  
Realizado por: Caiza Diego, 2016

Se configura la segunda interfaz de red en modo monitor esto permitirá capturar todo el tráfico que circule por la VLAN, como se muestra en la **Figura 20-3**. En el montaje físico que tiene el Prototipo, eth3 corresponde al adaptador interno de red del computador Toshiba.



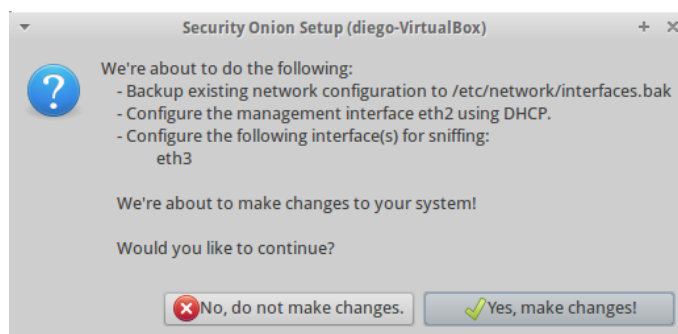
**Figura 20-3** Configuración de la interfaz de red en modo monitor  
Realizado por: Caiza Diego, 2016

Se adiciona la interfaz eth3, como se muestra en la **Figura 21-3**



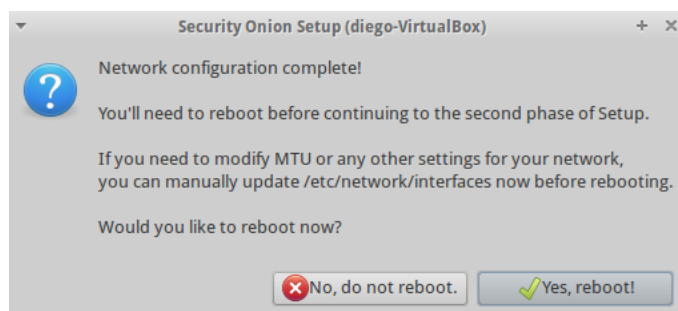
**Figura 21-3** Selección de la interfaz de red eth3 como monitor  
Realizado por: Caiza Diego, 2016

Se guardan los cambios realizados, como se muestra en la **Figura 22-3**



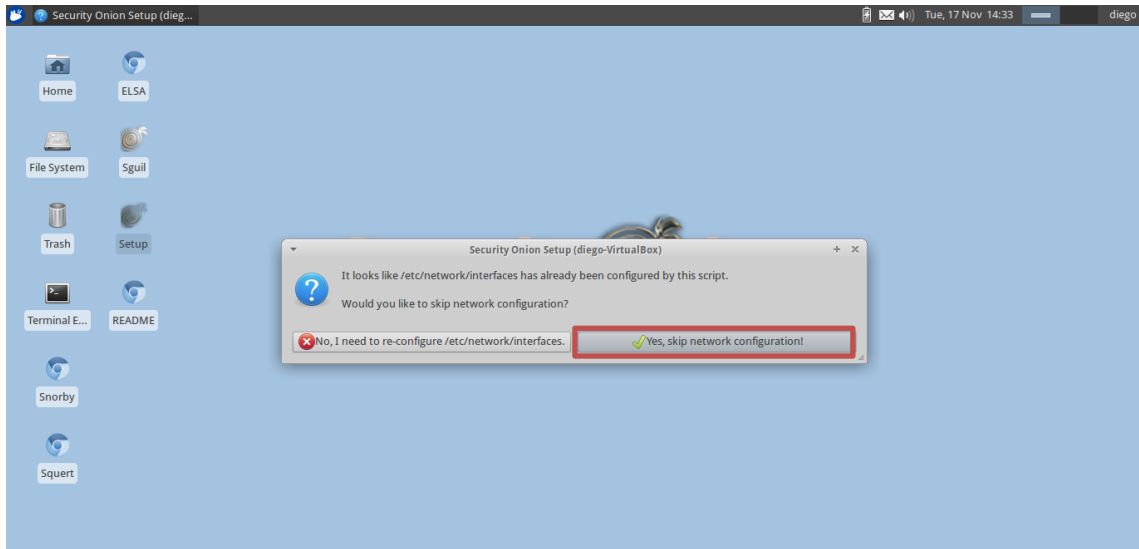
**Figura 22-3** Cambios guardados de la configuración de interfaces  
Realizado por: Caiza Diego, 2016

Se culmina con la configuración de las interfaces y se reinicia la distribución Security Onion, como se muestra en la **Figura 23-3**



**Figura 23-3** Reinicio de Security Onion  
Realizado por: Caiza Diego, 2016

Especificadas las interfaces con las que trabajará el sistema, se continúa con la siguiente fase, la cual se centra en la configuración del motor detector de intrusos. Nuevamente a través de un clic en el icono Setup se comienza con este proceso, como se muestra en la **Figura 24-3**



**Figura 24-3** Inicio de configuración del motor detector de intrusos  
Realizado por: Caiza Diego, 2016

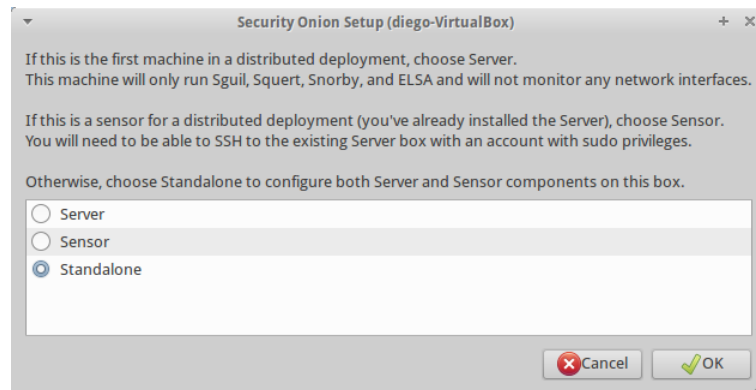
La primera parte de la configuración de esta fase se la realiza a través de la instalación avanzada, como se muestra en la **Figura 25-3**



**Figura 25-3** Inicio de la configuración avanzada del IDS  
Realizado por: Caiza Diego, 2016

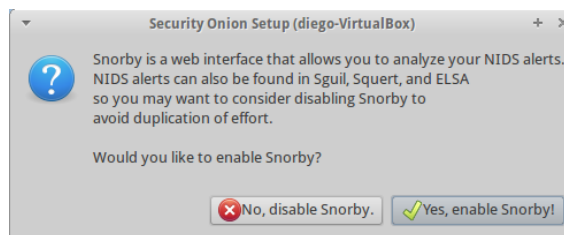
Se selecciona el modo de trabajo, las opciones posibles son en modo servidor (gestión de incidencias), en modo sensor (monitoreo) o la combinación de ambas. Para el

sistema se opta por la combinación de los dos modos es decir la configuración standalone, como se muestra en la **Figura 26-3**



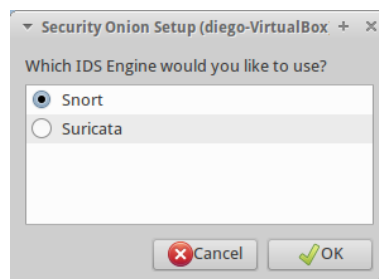
**Figura 26-3** Selección del modo de trabajo del detector de intrusos  
Realizado por: Caiza Diego, 2016

Se habilita Snorby que es uno de los gestores de incidencias de Security Onion, como se muestra en la **Figura 27-3**



**Figura 27-3** Selección de Snorby como gestor de incidencias  
Realizado por: Caiza Diego, 2016

Este paso es uno de los más importantes ya que se selecciona el motor de detección de intrusiones de la red, en el capítulo previo se definió utilizar snort por este motivo se lo habilita, como se muestra en la **Figura 28-3**

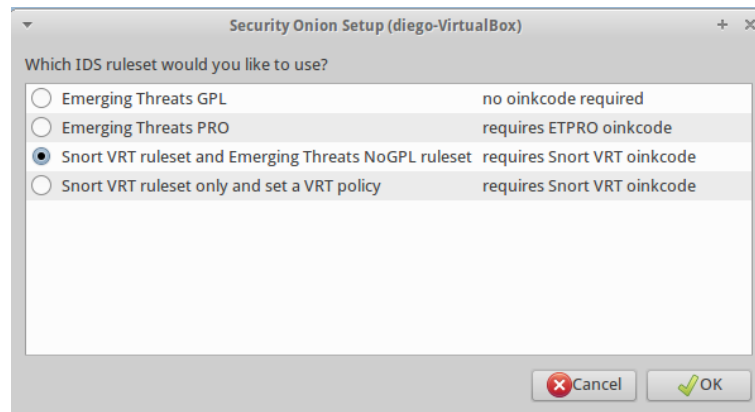


**Figura 28-3** Selección del motor detector de intrusos  
Realizado por: Caiza Diego, 2016

Se selecciona las reglas para el sistema detector de intrusos que serán definidas como las reglas por defecto de Snort, se optó por escoger las reglas VTR and Emerging Threats ya que se identificó como el paquete de reglas más completo, como se muestra

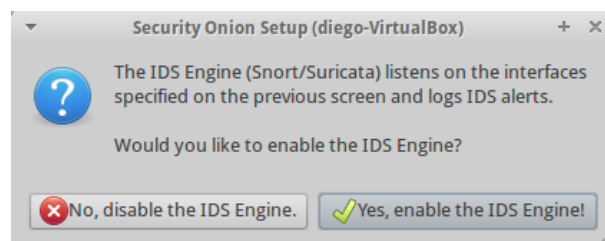


en la **Figura 29-3**. Es importante señalar que para descargar este tipo de reglas oficiales, se requiere tener una cuenta en la página oficial de Snort <https://snort.org/> , a través de esta se tiene acceso a un código con el cual se puede descargar estos ficheros (no está por demás mencionar que todo este proceso es gratuito y sencillo de realizarlo).



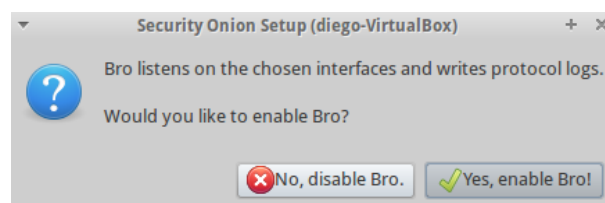
**Figura 29-3** Selección de las reglas por defecto de Snort  
Realizado por: Caiza Diego, 2016

Se habilita la ingeniería IDS útil para Snort y Suricata, como se muestra en la **Figura 30-3**



**Figura 30-3** Habilitación de ingeniería IDS  
Realizado por: Caiza Diego, 2016

En este punto de la instalación aparece la opción para habilitar el tercer sistema detector de intrusos con la que cuenta la distribución Security Onion, pero para el caso no se lo ocupa por lo queda deshabilitado, como se muestra en la **Figura 31-3**



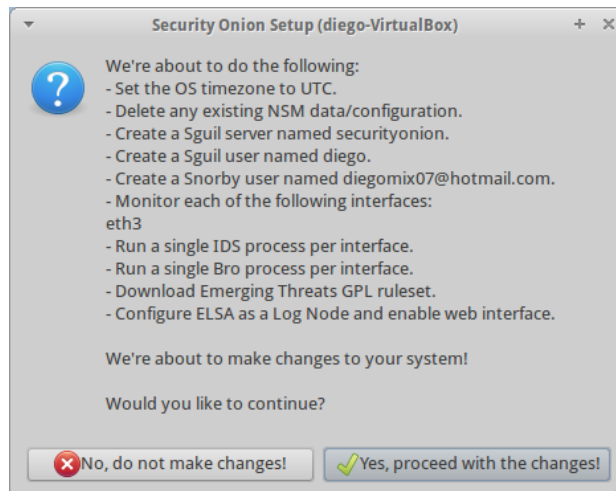
**Figura 31-3** Desactivación del IDS Bro  
Realizado por: Caiza Diego, 2016

Se habilita ELSA que es otro gestor para la administración de logs o alertas de Snort, como se muestra en la **Figura 32-3**



**Figura 32-3** Habilitación del gestor ELSA  
Realizado por: Caiza Diego, 2016

Finalmente se guarda la configuración seleccionada y se reinicia la máquina, como se muestra en la **Figura 33-3**



**Figura 33-3** Finalización de la configuración de Snort y los gestores  
Realizado por: Caiza Diego, 2016

### 3.6.5.2. Snort

Es importante indicar que Snort cuenta con un archivo principal de configuración a través del cual se puede establecer el modo de funcionamiento, para editar este archivo (que está alojado en el directorio de la interfaz de red que trabaja como monitor, es decir eth3) se lo hace mediante el comando mostrado en la **Figura 34-3**

```
diego@diego-VirtualBox:~/Desktop$ sudo nano /etc/nsm/diego-VirtualBox-eth3/snort.conf
```

**Figura 34-3** Instrucción para acceder al archivo de configuración de Snort  
Realizado por: Caiza Diego, 2016

En el archivo snort.conf como primer paso es indispensable añadir todas las redes consideradas locales dentro del entorno de pruebas del sistema, como se puede apreciar en la **Figura 35-3** están incluidas: la red de direcciones link-local, direcciones multicast IPv6 y la dirección de red IPv6 local de la FIE. Se declararon estas direcciones como locales después de analizar el tráfico IPv6 que circula por la red de la FIE.

```
# Setup the network addresses you are protecting
ipvar HOME_NET [fe80::/64,ff02::16,ff02::1,2800:68:a:5200::/64]
```

**Figura 35-3** Declaración de las redes locales en la configuración de Snort  
Realizado por: Caiza Diego, 2016

Además en este archivo se debe determinar el tipo de reglas que Snort va a utilizar para monitorear el tráfico, por lo que se hace necesario para evitar confusiones en la investigación precisar un nombre y especificar el tipo de regla que está utilizando el sistema detector de intrusos.

Por esta razón a partir de este punto se establece denominar como Prototipo I:

- Al sistema que va a trabajar con las reglas creadas en la investigación definidas como local.rules, ver **Figura 36-3**
- Al sistema completo es decir que cuente con el módulo de gestión de logs.

En cambio se denomina como Prototipo II:

- Al sistema que va a trabajar con las reglas propietarias de Snort y de libre distribución definidas como downloaded.rules, ver **Figura 36-3**
- Al sistema que no esté acoplado al módulo de gestión de logs.

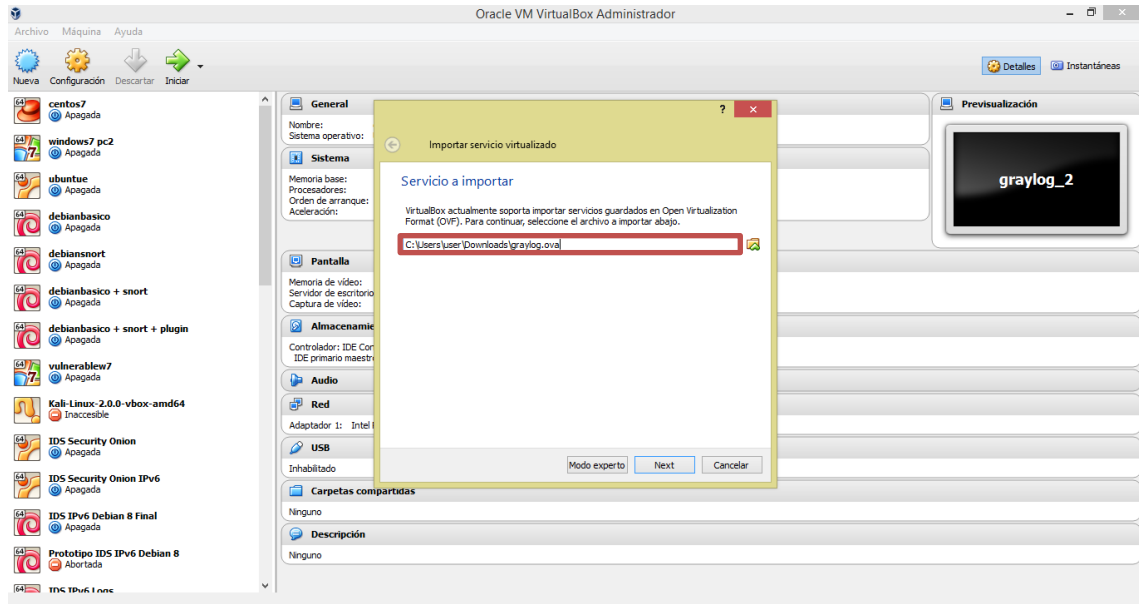
```
# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/downloaded.rules
```

**Figura 36-3** Tipos de reglas utilizados por Snort en Security Onion  
Realizado por: Caiza Diego, 2016

### 3.6.5.3. Servidor Graylog

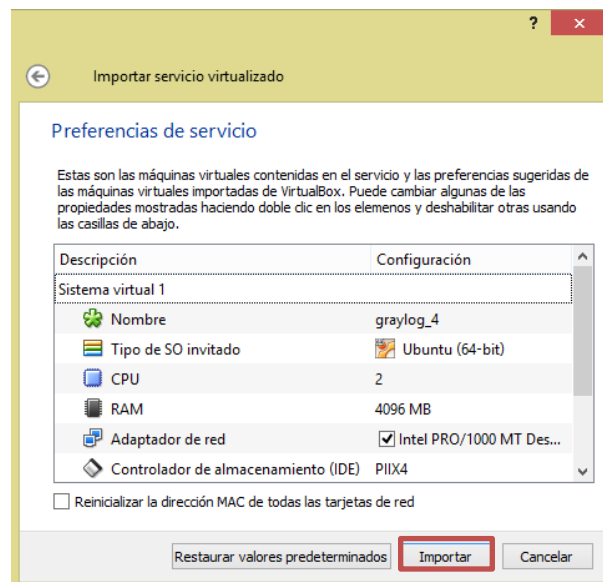
Como primer paso es necesario registrarse en la página <https://www.graylog.org/sign-in/?glredirect=/links/images-ova/>, para acceder a la descarga del archivo graylog.ova el cual contiene una máquina virtual con todo el software necesario para funcionar como un potente gestor de logs.

Para montar la imagen en Virtual Box se accede al menú Archivo ➤ Importar servicio virtualizado, se selecciona el archivo graylog.ova y se da clic en next para especificar las características y recursos de la máquina virtual, como se muestra en la **Figura 37-3**



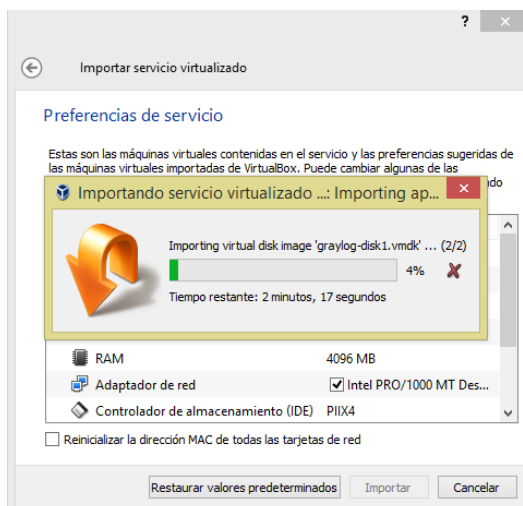
**Figura 37-3** Importación del archivo graylog.ova en virtual box  
Realizado por: Caiza Diego, 2016

Es recomendable mantener los valores predeterminados, para asegurar el buen rendimiento de Graylog, como se muestra en la **Figura 38-3**



**Figura 38-3** Preferencias de servicio del servidor Graylog  
Realizado por: Caiza Diego, 2016

Para terminar de cargar el archivo graylog.ova se da clic en importar, y la máquina virtual queda montada, como se muestra en la **Figura 39-3**



**Figura 39-3** Proceso de creación del servidor Graylog  
 Realizado por: Caiza Diego, 2016

Culminado el proceso anterior, se enciende la máquina Graylog e inmediatamente se solicita las credenciales de acceso. Para iniciar la sesión del sistema operativo las credenciales por defecto son user: **ubuntu** y el password: **ubuntu**, como se muestra en la **Figura 40-3**

La interfaz web es accesible en el puerto 80 de la dirección IP de la máquina virtual para el caso 172.25.200.230 (dirección asignada por el servidor DHCP). El usuario estándar para la interfaz web es **admin** con la contraseña **admin**.

```

Open http://172.25.200.230 in your browser to access Graylog.
Login to the web interface with username/password: 'admin'.
Or try the console here with username/password: 'ubuntu'.
graylog login: ubuntu
Password:
Last login: Fri Nov 27 06:05:57 ECT 2015 on tty1
Welcome to Graylog (GNU/Linux 3.19.0-25-generic x86_64)

* Documentation: http://docs.graylog.org/en/latest/pages/installation.html#vir
tual-machine-appliances
ubuntu@graylog:~$ ifconfig
eth0    Link encap:Ethernet  HWaddr 08:00:27:81:22:22
        inet addr:172.25.200.230 Bcast:172.25.201.255 Mask:255.255.248.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
        RX packets:2210 errors:0 dropped:0 overruns:0 frame:0
        TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:204075 (204.0 KB)  TX bytes:8640 (8.6 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:65536 Metric:1
        RX packets:286 errors:0 dropped:0 overruns:0 frame:0
        TX packets:286 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:23586 (23.5 KB)  TX bytes:23586 (23.5 KB)

```

**Figura 40-3** Pantalla inicial de la máquina virtual del servidor Graylog  
 Realizado por: Caiza Diego, 2016

Una vez iniciada la sesión en el servidor Graylog se realizan configuraciones básicas con los siguientes comandos:

- `sudo graylog-ctl set-admin-password <password>`
  - Establece una nueva contraseña
- `sudo graylog-ctl set-admin-username <username>`
  - Establece un nuevo nombre de usuario
- `sudo graylog-ctl set-timezone <zone acronym>`
  - Establece la zona horaria de Graylog, para el caso el acrónimo de la zona es América/Guayaquil. En caso de tener problemas con este comando se recomienda configurar manualmente la hora con el comando `sudo date --set <hora>`, ver **Figura 41-3**

```
ubuntu@graylog:~$ sudo date --set 17:38  
Tue Dec 1 17:38:00 ECT 2015
```

**Figura 41-3** Configuración manual de la hora en el servidor Graylog  
Fuente: Caiza Diego, 2016

Es sumamente importante asegurarse que el sistema de tiempo entre todas las máquinas este sincronizado, ya que caso contrario los colectores de Graylog acoplados no funcionarían y los logs de alertas no llegarían al servidor Graylog.

Después de configurar una o más de estas opciones, se ejecutan los comandos:

- `sudo graylog-ctl reconfigure`
- `sudo graylog-ctl restart`

El servidor Graylog esta finalmente está preparado, en pasos posteriores se debe especificar el puerto o los puertos para escuchar a los colectores que se conecten a él.

#### 3.6.5.4. *Instalación del colector de Graylog en Security Onion*

El agente colector de Graylog está encargado de acoplar el sistema detector de intrusos con el servidor Graylog y tiene la función de enviar todos los mensajes de alertas que se originen desde la distribución de Security Onion hacia el servidor. Para su instalación se deben seguir los siguientes pasos:

Descargar el colector desde <https://github.com/Graylog2/collector#binary-download>, (el cual es su repositorio oficial), como se muestra en la **Figura 42-3**

```
diego@diego-VirtualBox:~/Downloads$ wget https://packages.graylog2.org/releases/graylog-collector/graylog-collector-0.4.1.tgz
```

**Figura 42-3** Instrucción para descargar el colector de Graylog

Realizado por: Caiza Diego, 2016

Descomprimir el archivo .tgz desde la ubicación en donde se guardó el archivo, como se muestra en la **Figura 43-3**

```
diego@diego-VirtualBox:~/Downloads$ tar -xvzf graylog-collector-0.4.1
```

**Figura 43-3** Instrucción para descomprimir los ficheros de instalación

Realizado por: Caiza Diego, 2016

Se copia y respalda la configuración por defecto, como se muestra en la **Figura 44-3**

```
diego@diego-VirtualBox:~/Downloads/graylog-collector-0.4.1$ sudo cp config/collector.conf.example config/collector.conf
```

**Figura 44-3** Instrucción para realizar un respaldo del archivo de configuración

Realizado por: Caiza Diego, 2016

En el archivo collector.conf se actualiza la dirección url del servidor Graylog, como se puede muestra en la **Figura 45-3** y en la **Figura 46-3**

```
diego@diego-VirtualBox:~/Downloads/graylog-collector-0.4.1$ sudo nano config/collector.conf
```

**Figura 45-3** Instrucción para editar el archivo de configuración del colector

Realizado por: Caiza Diego, 2016

```
// Graylog Collector example configuration.  
  
// URL to REST API of Graylog server this collector registers at  
server-url = "http://172.25.200.230:12900"
```

**Figura 46-3** Selección de la ruta del servidor Graylog

Realizado por: Caiza Diego, 2016

Añadir la configuración de entrada, es decir establecer la conexión con el detector de intrusos para enviar las alertas que se registren desde su ubicación nativa, como se muestra en la **Figura 47-3**

```

inputs {

snort-access {
    type = "file"
    path-glob-root = "/nsm/sensor_data/diego-VirtualBox-eth3/snort-1"
    path-glob-pattern = "alert"
    outputs = "gelf-1"
}
}

```

**Figura 47-3** Configuración del formato de mensajes de entrada al colector  
Realizado por: Caiza Diego, 2016

Añadir la configuración de salida, Graylog trabaja con gelf el cual es un formato de registro que evita las deficiencias del clásico syslog y es muy útil para el presente trabajo. Se actualiza nuevamente la dirección del servidor y además se define el puerto a través del cual se va a establecer la conexión, como se muestra en la **Figura 48-3**

```

outputs {
// // GELF output to send messages to a Graylog server. Usually only type, hos$
// // The other options are for TLS support and to fine-tune the GELF client l$
gelf-1{
    type = "gelf"
    host = "172.25.200.230"
    port = 12201
}
}

```

**Figura 48-3** Configuración del formato de mensajes de salida al servidor Graylog  
Realizado por: Caiza Diego, 2016

Una vez terminada la configuración se debe iniciar el agente desde la ubicación en donde se encuentran guardados sus archivos con el siguiente comando, como se muestra en la **Figura 49-3**

```

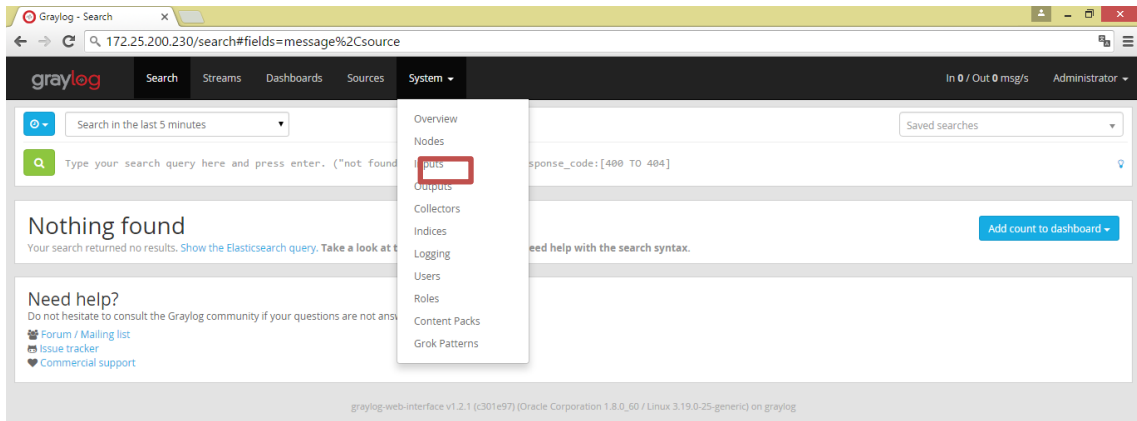
diego@diego-VirtualBox:~/Downloads/graylog-collector-0.4.1$ sudo bin/graylog-collector run -f config/collector.conf

```

**Figura 49-3** Instrucción para inicializar el colector Graylog  
Realizado por: Caiza Diego, 2016

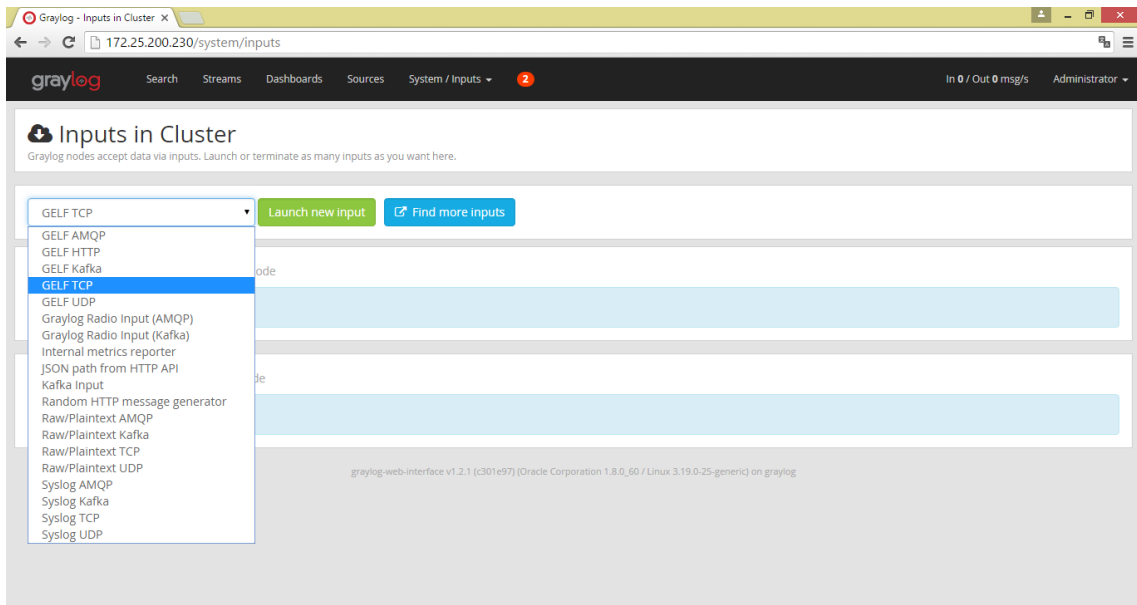
Hasta el momento se pueden enviar las alertas que genera Snort pero la conexión aún no está terminada y el servidor Graylog no recibe ningún mensaje debido a que es necesario establecer el puerto a través del cual el servidor va a escuchar los mensajes o alertas entrantes. Para realizar este paso se accede vía web a la dirección del servidor Graylog, lo primero es ingresar las credenciales de autenticación, luego establecer la conexión de entrada mediante el menú System ▶ Inputs, como se muestra en la **Figura 50-3**





**Figura 50-3** Configuración del servidor Graylog para recibir mensajes desde el colector  
**Realizado por:** Caiza Diego, 2016

Luego se trabaja con el formato GELF a través de la interfaz, se elige la opción GELF TCP y se la dispone como una nueva entrada, como se muestra en la **Figura 51-3**



**Figura 51-3** Selección del tipo de mensaje de entrada para el servidor Graylog  
**Realizado por:** Caiza Diego, 2016

Se elige el modo de entrada si es de tipo local o global, se establece el nombre de la entrada y el puerto para establecer la comunicación con Security Onion (el cual debe ser el mismo que se definió en el colector), los demás parámetros se los precisa por defecto, como se muestra en la **Figura 52-3**

### Launch new input: *GELF TCP*

**Node(s) to spawn input on:**  
 Select the node you want to spawn this input on.

or:

Global input (started on all nodes)

**Title**  
  
 Select a name of your new input that describes it.

**Bind address**  
  
 Address to listen on. For example 0.0.0.0 or 127.0.0.1.

**Port**  
  
 Port to listen on.

**Receive Buffer Size (optional)**

---

Whether clients need to authenticate themselves in a TLS connection

**TLS Client Auth Trusted Certs (optional)**  
  
 TLS Client Auth Trusted Certs (File or Directory)

**Maximum message size (optional)**  
  
 The maximum length of a message.

**Override source (optional)**  
  
 The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

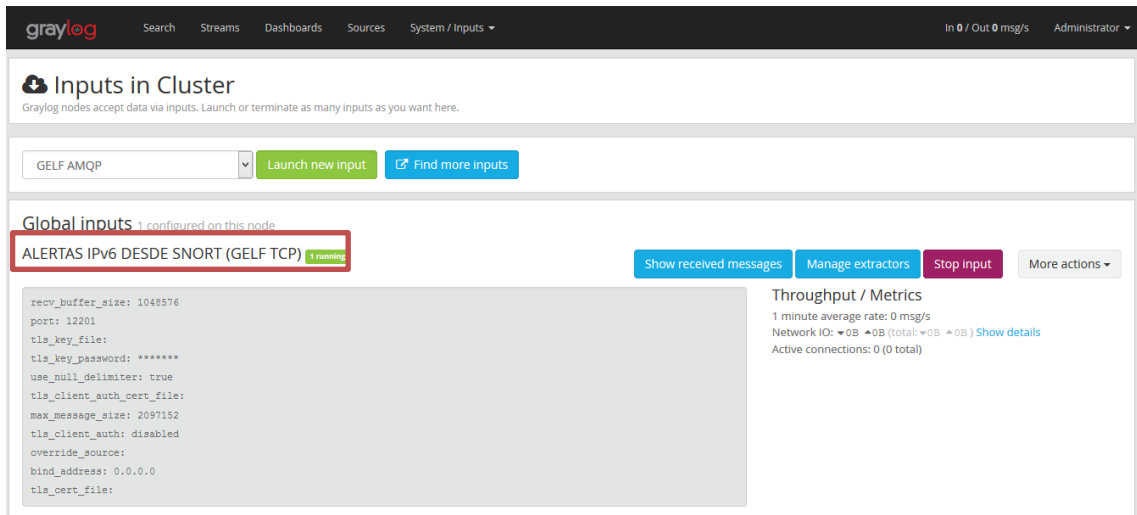
Enable TLS (optional)  
 Accept TLS connections

Null frame delimiter? (optional)  
 Use null byte as frame delimiter? Otherwise newline delimiter is used.

TCP keepalive (optional)  
 Enable TCP keepalive packets

**Figura 52-3** Configuración del puerto y adicionales en el servidor  
 Realizado por: Caiza Diego, 2016

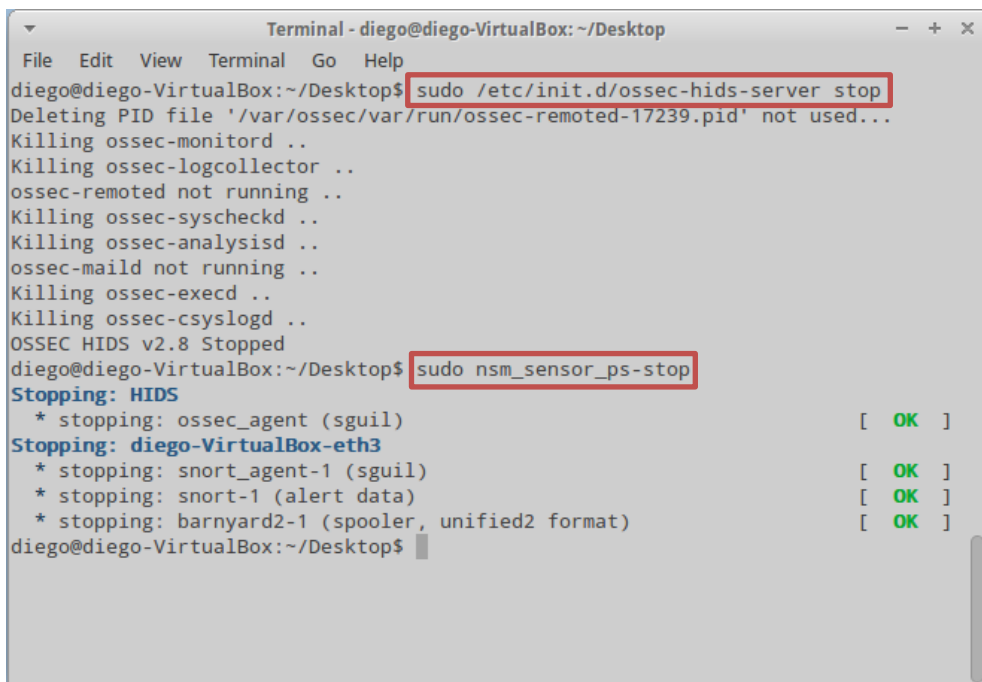
Concluidos los pasos anteriores la conexión se encuentra totalmente preparada para recibir todos los mensajes que se generen desde la máquina virtual de Security Onion. En este punto el sistema se encuentra listo para iniciar con la fase de pruebas, como se muestra en la **Figura 53-3**



**Figura 53-3** Servidor configurado para la recepción de alertas  
**Realizado por:** Caiza Diego, 2016

### 3.6.5.5. Inicialización del sistema

En este proceso es indispensable tener correctamente configurados y concluidos los pasos indicados en los ítems anteriores, caso contrario el sistema no se podrá activar de manera apropiada. Dentro del entorno IDS del sistema, es necesario parar o apagar los servicios que inicia por defecto los sensores de Security Onion, como se muestra en la **Figura 54-3**



**Figura 54-3** Detención de servicios en Security Onion  
**Realizado por:** Caiza Diego, 2016

Se debe especificar en Snort los parámetros de trabajo para empezar a enviar los registros de alertas al servidor Graylog, se ejecuta a través de la instrucción como se muestra en la **Figura 55-3**

```
diego@diego-VirtualBox:~/Desktop$ sudo snort -A fast -c /etc/nsm/diego-VirtualBo  
x-eth3/snort.conf -i eth3 -l /nsm/sensor_data/diego-VirtualBox-eth3/snort-1
```

**Figura 55-3** Inicialización de Snort en Security Onion

Realizado por: Caiza Diego, 2016

En donde cada parámetro de la instrucción significa:

- **-A fast:** Define utilizar el modo de alerta rápido, es decir se escribe la alerta en un formato sencillo y solamente con los campos básicos: Fecha, mensaje de alerta, Direcciones IP y puertos de origen y destino.
- **-c /etc/nsm/diego-VirtualBox-eth3/snort.conf:** Especifica que se va a trabajar en modo NIDS y define la ruta en donde se encuentra alojado el archivo de configuración de Snort.
- **-i eth3:** Define la interfaz de red que va a estar monitoreando el tráfico que circule por la red.
- **-l /nsm/sensor\_data/diego-VirtualBox-eth3/snort-1:** Define la ruta interna en donde se van a guardar los logs generados por Snort.

Concluidos estos pasos el sistema está completamente acoplado y funcionando, preparado para iniciar el monitoreo del tráfico IPv6 de la red local de la FIE, adicionalmente en el **Anexo B** se indica la fase de instalación y configuración del host que va ser utilizado como máquina atacante.

### 3.7. Definición de los escenarios de pruebas

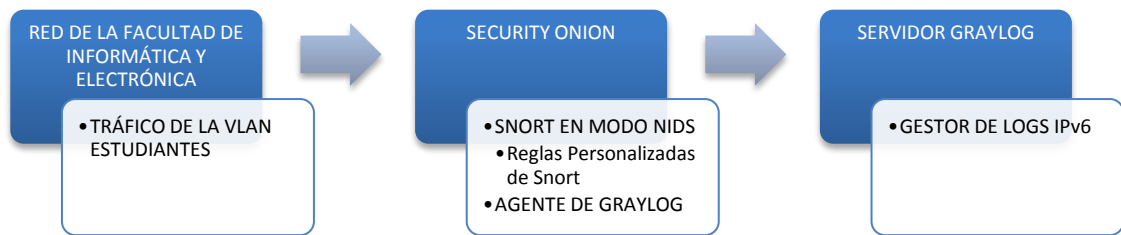
#### 3.7.1. Prototipos de prueba

##### 3.7.1.1. Prototipo I

El Prototipo I establecido para ejecutar los experimentos de pruebas, se compone de dos módulos funcionales:

- El módulo de Security Onion, cuyos componentes internos son: el motor detector de intrusos Snort trabajando con las reglas creadas para la investigación y el agente de Graylog que permite el acoplamiento con el módulo del servidor Graylog.

- El módulo del servidor Graylog es el encargado de mostrar y gestionar los logs IPv6 recolectados.



**Figura 56-3** Estructura general del prototipo I

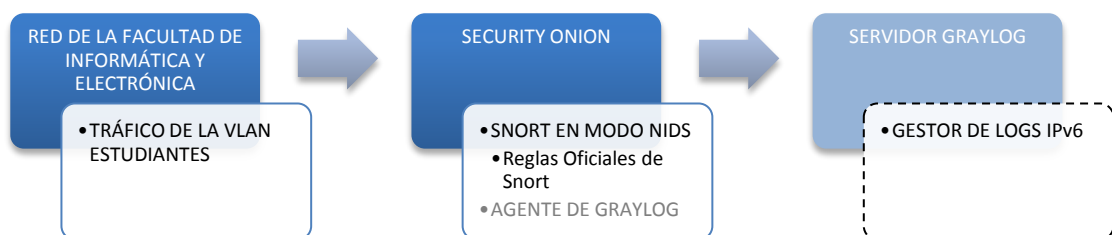
Realizado por: Caiza Diego, 2016

### 3.7.1.2. Prototipo II

El Prototipo II establecido para ejecutar los experimentos de pruebas, se compone de un módulo funcional:

- El módulo de Security Onion, cuyo componente interno es el motor detector de intrusos Snort trabajando con sus reglas oficiales.

Como se mencionó en la parte teórica de la investigación Security Onion carece de la funcionalidad de mostrar y gestionar los logs IPv6 recolectados, debido a este problema se optó por incluir el módulo del servidor Graylog. Es importante señalar que este módulo no es parte del prototipo II pero es necesario, ya que sería imposible visualizar los resultados obtenidos en la fase de los experimentos.



**Figura 57-3** Estructura general del prototipo II

Realizado por: Caiza Diego, 2016

### 3.7.2. Experimento 1

El experimento 1 analiza la efectividad de detección del Prototipo I ante el tráfico malicioso inyectado en la VLAN de Estudiantes durante la jornada normal de actividades, los pasos requeridos para iniciar la prueba son:

- Iniciar el sistema detector de intrusos (reglas local.rules)
- Conectar la máquina atacante a la VLAN de Estudiantes

- Ejecutar cada uno de los ataques detallados en la **Tabla 5-3**, los mismos que han sido categorizados en tres tipos de acuerdo a su modo de proceder: reconocimiento, hombre en el medio y denegación de servicio.

**Tabla 5-3** Nombre del ataque ejecutado y categorización

<b>Ataque</b>	<b>Categoría</b>
atk6-alive6 eth0	Reconocimiento
atk6-alive6 -4 192.168.1.0/24 eth0	Reconocimiento
atk6-alive6 -d eth0	Reconocimiento
atk6-parasite6 -l eth0	Hombre en el medio
atk6-parasite6 -l -R eth0	Hombre en el medio
atk6-parasite6 -l -F eth0	Hombre en el medio
atk6-parasite6 -l -H eth0	Hombre en el medio
atk6-parasite6 -l -R -F -H	Hombre en el medio
atk6-fake_router6 eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -H eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -D eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -F eth0 2001:db8:bad::/64	Hombre en el medio
atk6-fake_router6 -H -D eth0 2001:db8:bad::/64	Hombre en el medio
atk6-flood_advertise6 eth0	Denegación de servicios
atk6-flood_solicit6 eth0	Denegación de servicios
atk6-flood_router6 eth0	Denegación de servicios
atk6-flood_router6 -F eth0	Denegación de servicios
atk6-flood_rs6 eth0	Denegación de servicios
atk6-flood_rs6 -s eth0	Denegación de servicios
atk6-flood_rs6 -S eth0	Denegación de servicios
atk6-flood_rs6 -s -S eth0	Denegación de servicios
atk6-flood_redir6 eth0	Denegación de servicios
atk6-flood_redir6 -H eth0	Denegación de servicios
atk6-flood_redir6 -F eth0	Denegación de servicios
atk6-flood_redir6 -H -F eth0	Denegación de servicios

Realizado por: Caiza Diego, 2016

### 3.7.3. Experimento 2

El experimento 2 analiza la efectividad de detección del Prototipo II ante el tráfico malicioso inyectado en la VLAN de Estudiantes durante la jornada normal de actividades, los pasos requeridos para iniciar la prueba son:

- Iniciar el sistema detector de intrusos (reglas download.rules)
- Conectar la máquina atacante a la VLAN de Estudiantes
- Ejecutar cada uno de los ataques detallados en la **Tabla 5-3**, los mismos que han sido categorizados en tres tipos de acuerdo a su modo de proceder: reconocimiento, hombre en el medio y denegación de servicio.

### 3.7.4. Experimento 3

En el experimento 3 se monitorea el tráfico que circula en la VLAN estudiantes durante un día en la jornada normal de actividades, con esta prueba se identificara la cantidad de alertas denominadas falsas positivas que se originan al utilizar el Prototipo I.

Esta fase de prueba comienza cuando los laboratorios de la FIE son abiertos para el ingreso y uso de los estudiantes y termina cuando el edificio es cerrado, es decir inicia a las 07:00 de la mañana y finaliza a las 21:00 de la noche.

Como medida adicional para verificar que el detector esté trabajando de manera correcta se generaran ataques específicos en cada uno de los intervalos de tiempo estipulados, como se detallan en la **Tabla 6-3**

**Tabla 6-3** Intervalos de tiempo experimento 3

Intervalos de tiempo	Categorización del ataque	Número de Intervalo
07:00 – 09:59	Ataque de reconocimiento	Intervalo 1
10:00 – 12:59	Ataque de MITM	Intervalo 2
13:00 – 15:59	Ataque de MITM	Intervalo 3
16:00 – 18:59	Ataque DDos	Intervalo 4
19:00 – 21:00	Ataque DDos	Intervalo 5

Realizado por: Caiza Diego, 2016

### **3.7.5. Experimento 4**

El experimento 4 es equivalente al proceso anterior pero en este caso se utiliza el Prototipo II, de igual manera el monitoreo se lo realiza durante otro día en la jornada normal de actividades, recopilando los datos para analizarlos y cuyos resultados se muestran en el siguiente capítulo.

### **3.7.6. Experimento 5**

El experimento 5 verifica la capacidad de presentación y gestión de los logs IPv6 obtenidos durante el proceso de pruebas, debido a que los campos de dirección origen y dirección destino de las alertas tienen direccionamiento IPv6. Esta prueba evidenciará si el Prototipo I cumple con la premisa de gestionar alertas con direccionamiento IPv6.

### **3.7.7. Experimento 6**

El experimento 6 es equivalente al proceso anterior pero aplicado al Prototipo II, esta prueba evidenciará si este Prototipo cumple con la premisa de gestionar y administrar las alertas que contengan direccionamiento IPv6.

## **3.8. Hipótesis**

### **3.8.1. Determinación de variables**

Dentro de la hipótesis para realizar la validación de los resultados de la presente investigación se hallan definidas dos variables:

#### **Variable Independiente**

- Prototipo como sistema detector de intrusos para el protocolo IPv6 desarrollado con herramientas open source

#### **Variable Dependiente**

- Seguridad en la red local

La operacionalización conceptual y metodológica de las variables se muestra en la



### 3.8.2. Operacionalización conceptual

La **Tabla 7-3** muestra la operacionalización conceptual de las variables determinadas.

**Tabla 7-3** Operacionalización conceptual de las variables de la investigación

VARIABLE	TIPO	DEFINICIÓN
Prototipo como sistema detector de intrusos para el protocolo IPv6 desarrollado con herramientas open source	Independiente	Sistema detector de tráfico IPv6 malicioso utilizando herramientas open source
Seguridad en la red local	Dependiente	Detención de actividad anormal en la red local Gestión y backup en tiempo real de logs IPv6

Realizado por: Caiza Diego, 2016

### 3.8.3. Operacionalización metodológica

La **Tabla 8-3** muestra la operacionalización metodológica de las variables determinadas.

**Tabla 8-3** Operacionalización metodológica de las variables de la investigación

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTOS
Prototipo como sistema detector de intrusos para el protocolo IPv6 desarrollado con herramientas open source	<ul style="list-style-type: none"> <li>○ Escases de direcciones IPv4</li> <li>○ Facilidad de uso de herramientas de pentesting para el protocolo IPv6</li> <li>○ Sistema operativo vulnerable</li> </ul>	<ul style="list-style-type: none"> <li>○ Búsqueda de información</li> <li>○ Pruebas</li> <li>○ Observación</li> </ul>	<ul style="list-style-type: none"> <li>○ THCIPv6 Toolkit</li> <li>○ Wireshark</li> <li>○ Virtual Box</li> <li>○ Distribución Security Onion</li> <li>○ Snort</li> <li>○ Windows 7</li> </ul>
Seguridad en la red local	<ul style="list-style-type: none"> <li>○ Gestión de Logs IPv6</li> <li>○ No. Alertas Positivas Verdaderas</li> <li>○ No. Alertas Falsas Positivas</li> <li>○ Replicación de Logs IPv6</li> </ul>	<ul style="list-style-type: none"> <li>○ Observación</li> <li>○ Análisis del tráfico IPv6 de la red</li> <li>○ Pruebas de vulnerabilidades del protocolo IPv6 en la red local</li> </ul>	<ul style="list-style-type: none"> <li>○ Virtual Box</li> <li>○ Distribución Security Onion</li> <li>○ Snort</li> <li>○ Graylog</li> </ul>

Realizado por: Caiza Diego, 2016

## CAPITULO IV

### 4. RESULTADOS Y DISCUSIÓN

En este capítulo, se desarrollan las pruebas en los experimentos establecidos, se analizan, se compara los resultados obtenidos y se demuestra la hipótesis definida.

#### 4.1. Desarrollo de las pruebas

##### 4.1.1. Prototipo I

Se desarrollaron las pruebas utilizando el Prototipo I en los experimentos establecidos para:

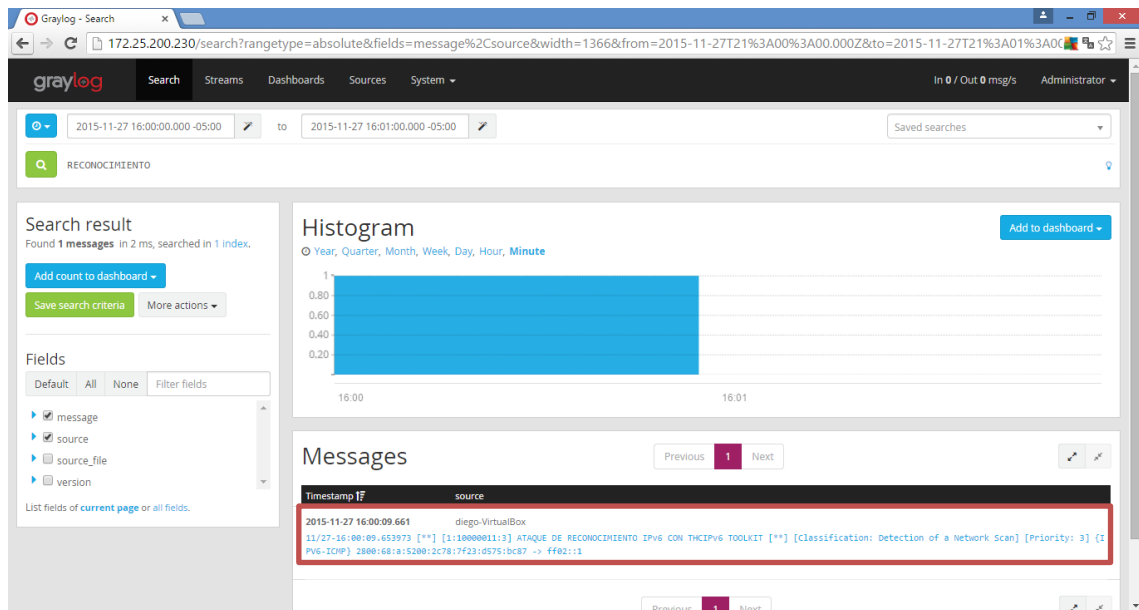
- No. Alertas positivas verdaderas
- No. Alertas falsas positivas
- Gestión de logs IPv6
- Replicación de logs IPv6

##### 4.1.1.1. No. Alertas positivas verdaderas (ataques detectados)

Los resultados obtenidos al realizar el experimento 1 se especifican en los siguientes ítems, y el detalle del tráfico malicioso capturado en el **Anexo C**.

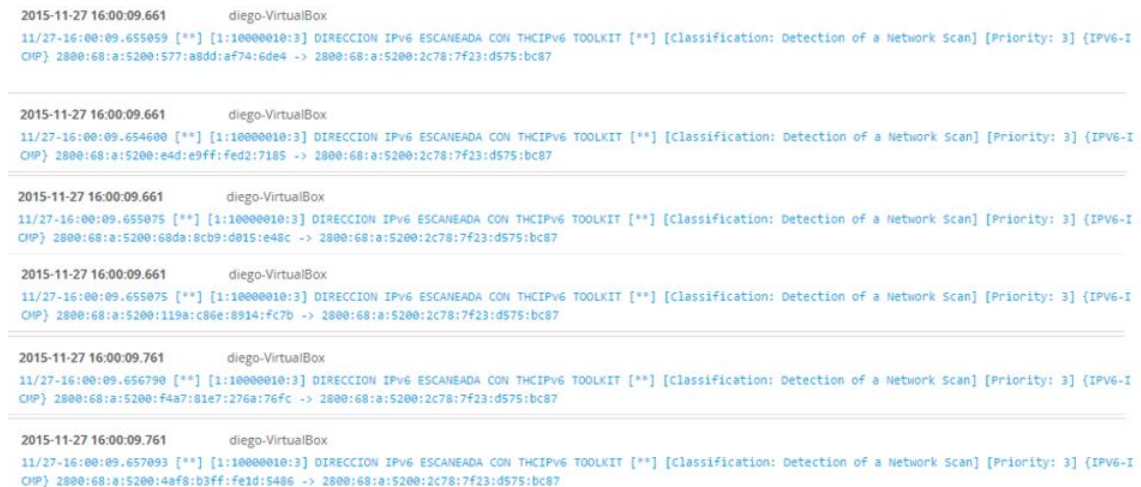
##### 4.1.1.1.1. Prueba 1 atk6-alive6 eth0

En la prueba 1 se realizó el ataque categorizado como de reconocimiento atk6-alive6 sobre la interfaz eth0, en la **Figura 1-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 1-4** Alerta del ataque de reconocimiento con atk6-alive6 eth0  
Realizado por: Caiza Diego, 2016

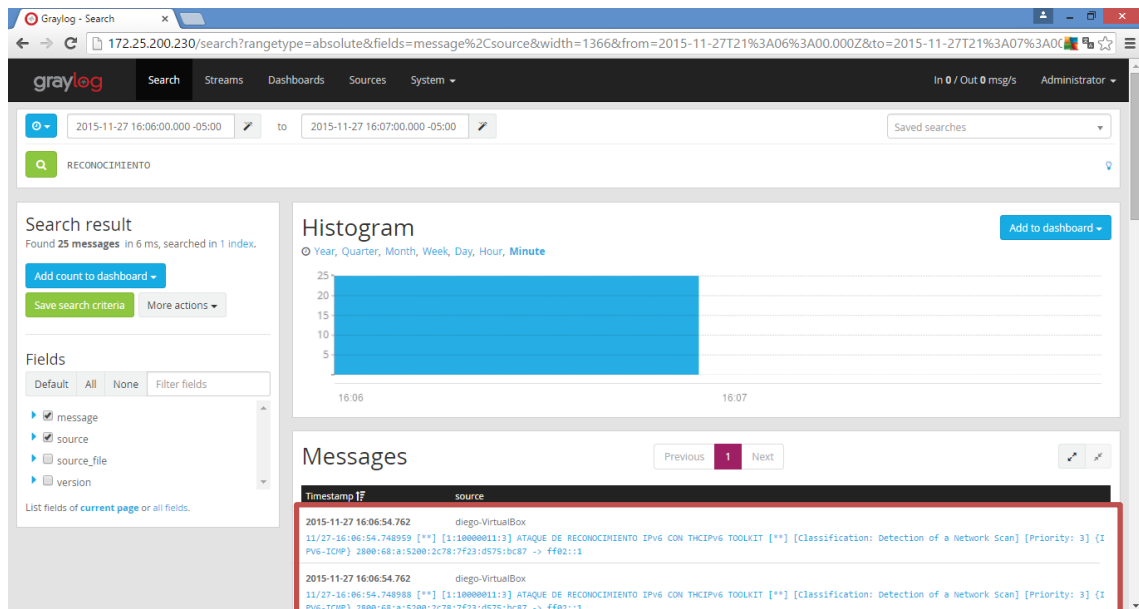
En la **Figura 2-4** se muestra el detalle de las direcciones IPv6 escaneadas durante esta prueba.



**Figura 2-4** Alertas con las direcciones IPv6 obtenidas con atk6-alive6 eth0  
Realizado por: Caiza Diego, 2016

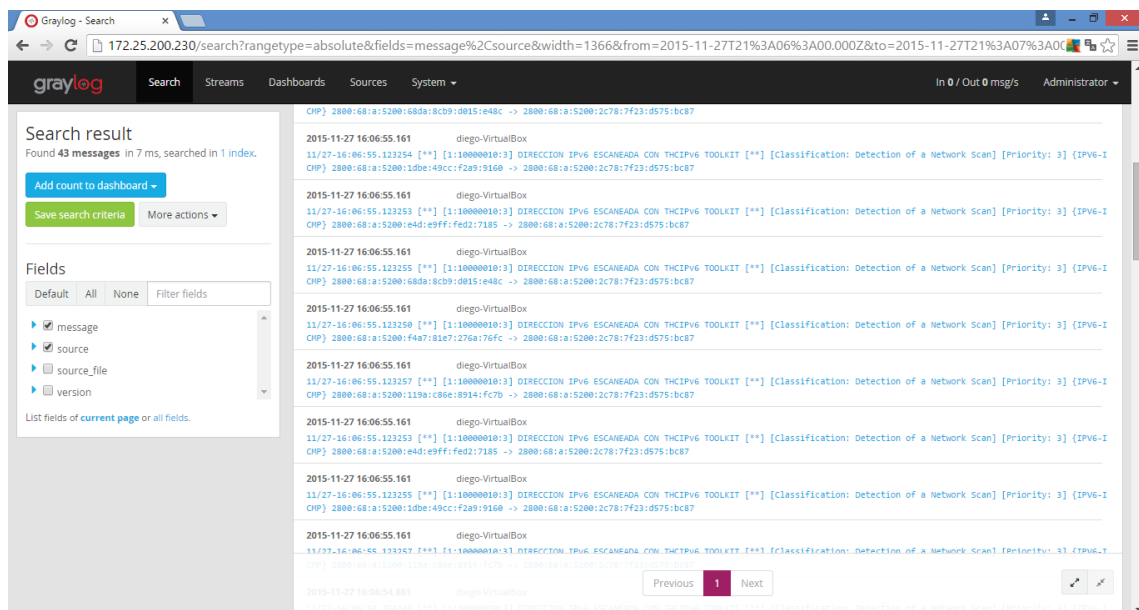
#### 4.1.1.1.2. Prueba 2 atk6-alive6 -4 172.25.0.0/21 eth0

En la prueba 2 se realiza el ataque categorizado como de reconocimiento atk6-alive6 - 4 172.25.0.0/21 sobre la interfaz eth0, en la **Figura 3-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 3-4** Alerta del ataque de reconocimiento con atk6-alive6 -4 172.25.0.0/21 eth0  
Realizado por: Caiza Diego, 2016

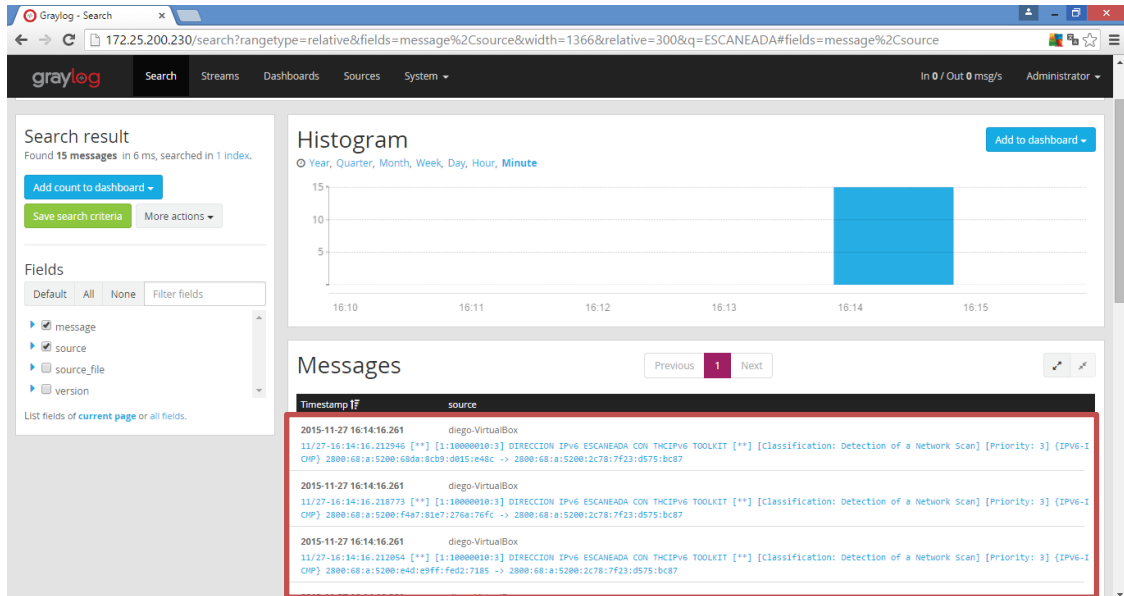
En la **Figura 4-4** se muestra el detalle de las direcciones IPv6 escaneadas durante esta prueba.



**Figura 4-4** Direcciones IPv6 escaneadas con atk6-alive6 -4 172.25.0.0/21 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.3. Prueba 3 atk6-alive6 -d eth0

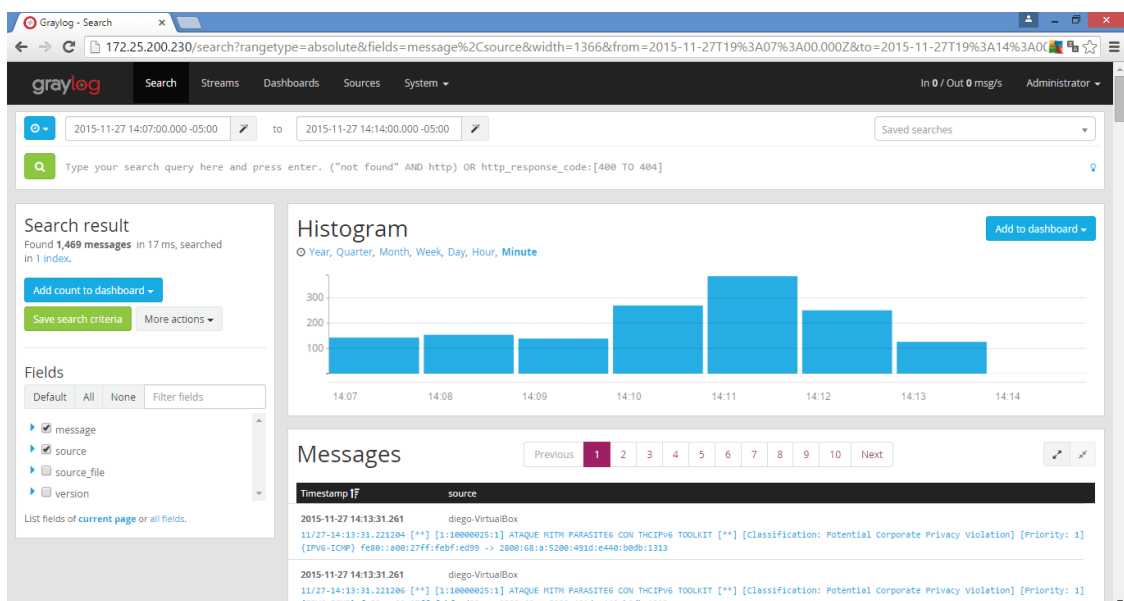
En la prueba 3 se realiza el ataque de reconocimiento atk6-alive6 -d sobre la interfaz eth0, en la **Figura 5-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 5-4** Alertas con las direcciones IPv6 obtenidas con atk6-alive6 -d eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.4. Prueba 4 atk6-parasite6 -l eth0

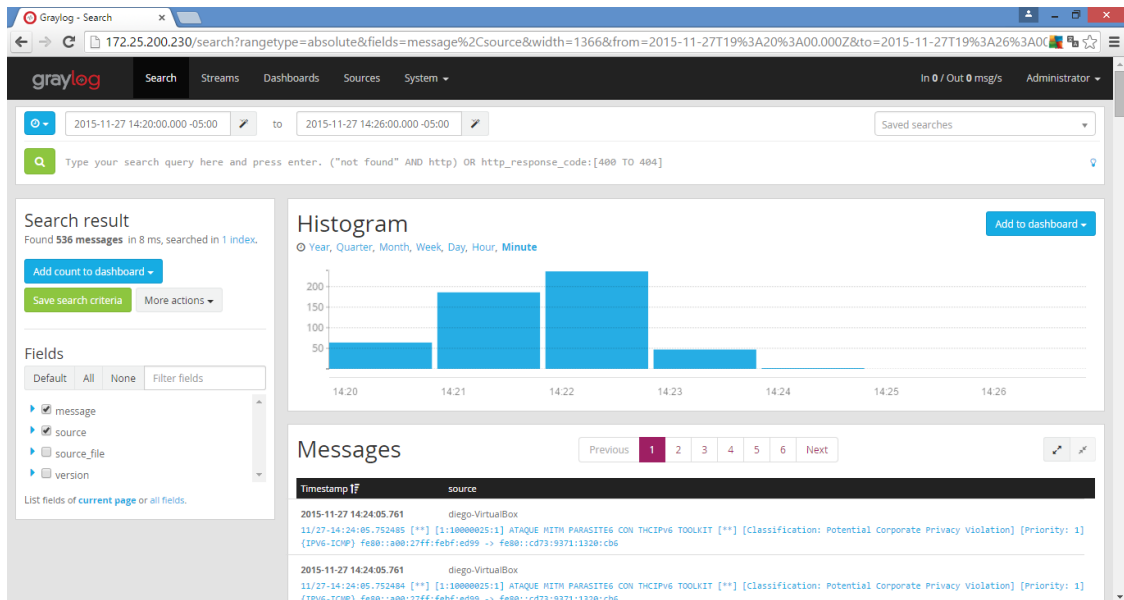
En la prueba 4 se realiza el ataque MITM atk6-parasite6 -l sobre la interfaz eth0, en la **Figura 6-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 6-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.5. Prueba 5 atk6-parasite6 -I -R eth0

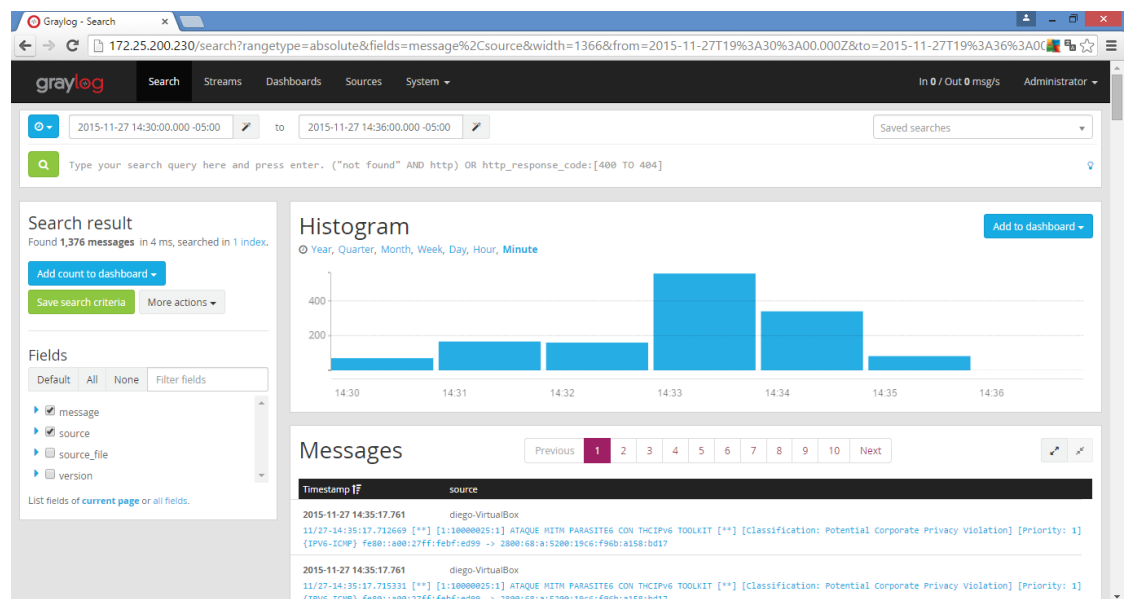
En la prueba 5 se realiza el ataque MITM atk6-parasite6 -I -R sobre la interfaz eth0, en la **Figura 7-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 7-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -I -R eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.6. Prueba 6 atk6-parasite6 -I -F eth0

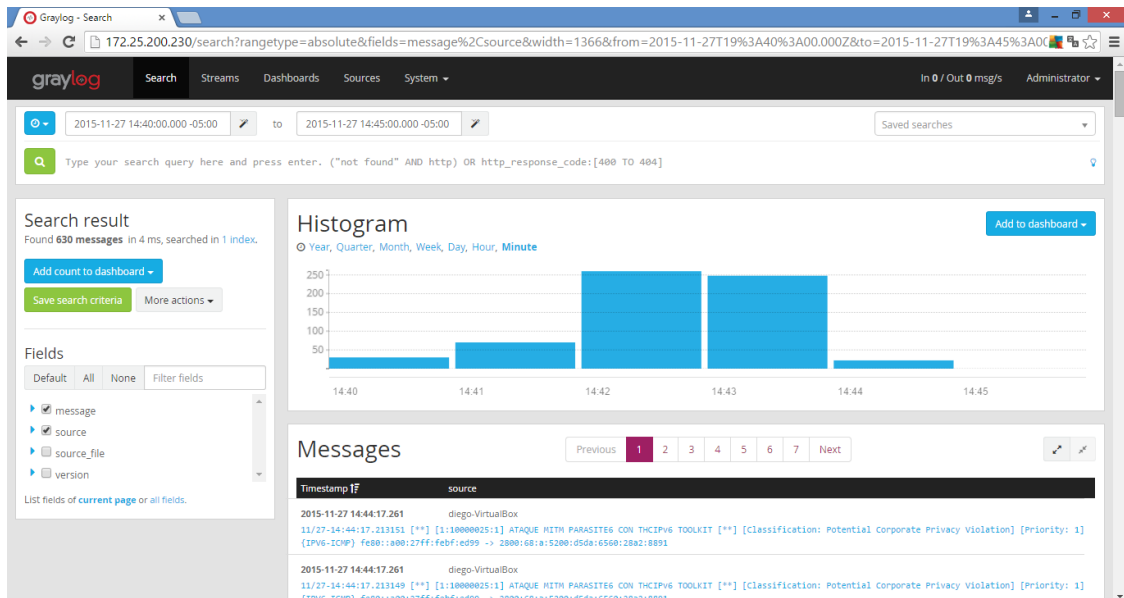
En la prueba 6 se realiza el ataque MITM atk6-parasite6 -I -F sobre la interfaz eth0, en la **Figura 8-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 8-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -I -F eth0  
Fuente: Caiza Diego, 2016

#### 4.1.1.1.7. Prueba 7 atk6-parasite6 -I -H eth0

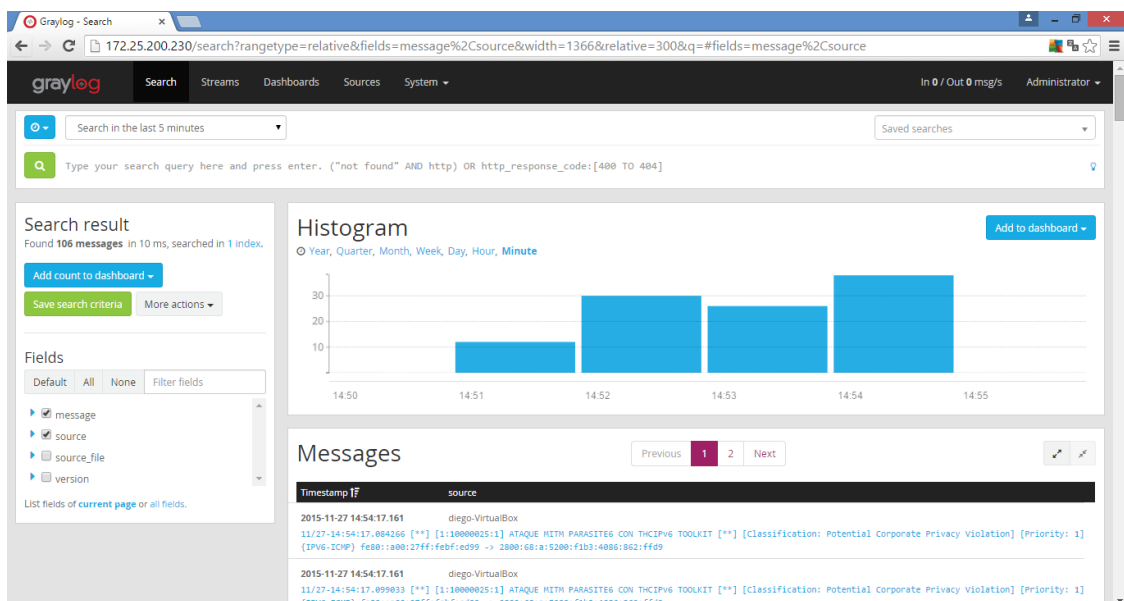
En la prueba 7 se realiza el ataque MITM atk6-parasite6 -I -H sobre la interfaz eth0, en la **Figura 9-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 9-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -I -H eth0  
Fuente: Caiza Diego, 2016

#### 4.1.1.1.8. Prueba 8 atk6-parasite6 -I -R -F -H

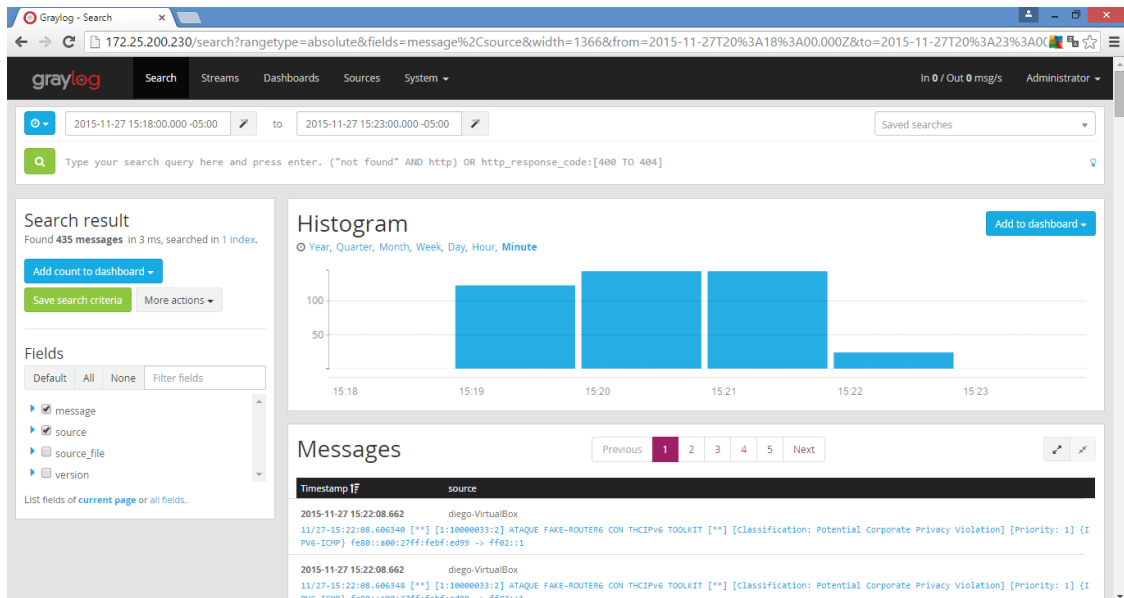
En la prueba 8 se realiza el ataque MITM atk6-parasite6 -I -H sobre la interfaz eth0, en la **Figura 10-4** se muestran las alertas originadas por este tipo de ataque.



**Figura 10-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -I -R -F -H  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.9. Prueba 9 atk6-fake\_router6 eth0 2001:db8:bad::/64

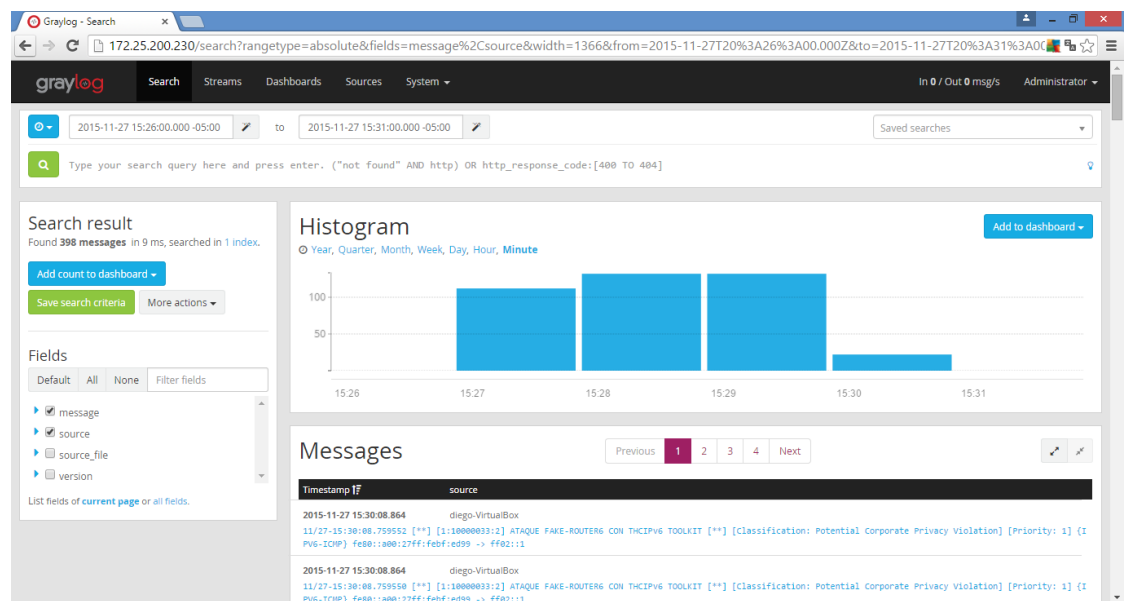
En la prueba 9 se realiza el ataque MITM atk6-fake\_router6 eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 11-4** se muestran las alertas originadas.



**Figura 11-4** Alertas obtenidas al ejecutar atk6-fake\_router6 eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.10. Prueba 10 atk6-fake\_router6 -H eth0 2001:db8:bad::/64

En la prueba 10 se realiza el ataque MITM atk6-fake\_router6 -H eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 12-4** se muestran las alertas originadas.

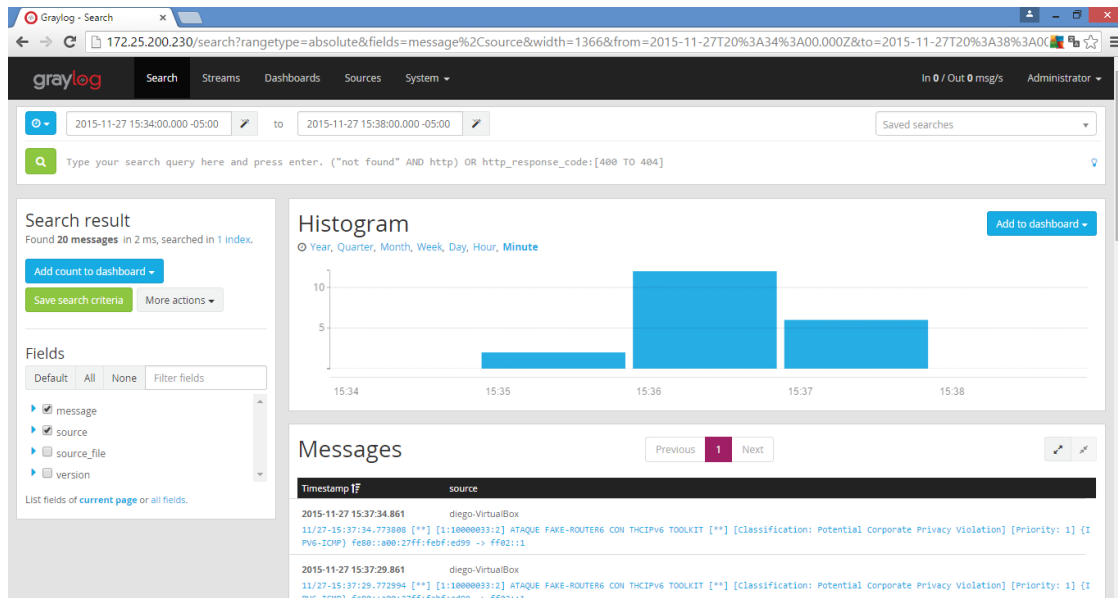


**Figura 12-4** Alertas obtenidas al ejecutar atk6-fake\_router6 -H eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016



#### 4.1.1.1.11. Prueba 11 atk6-fake\_router6 -D eth0 2001:db8:bad::/64

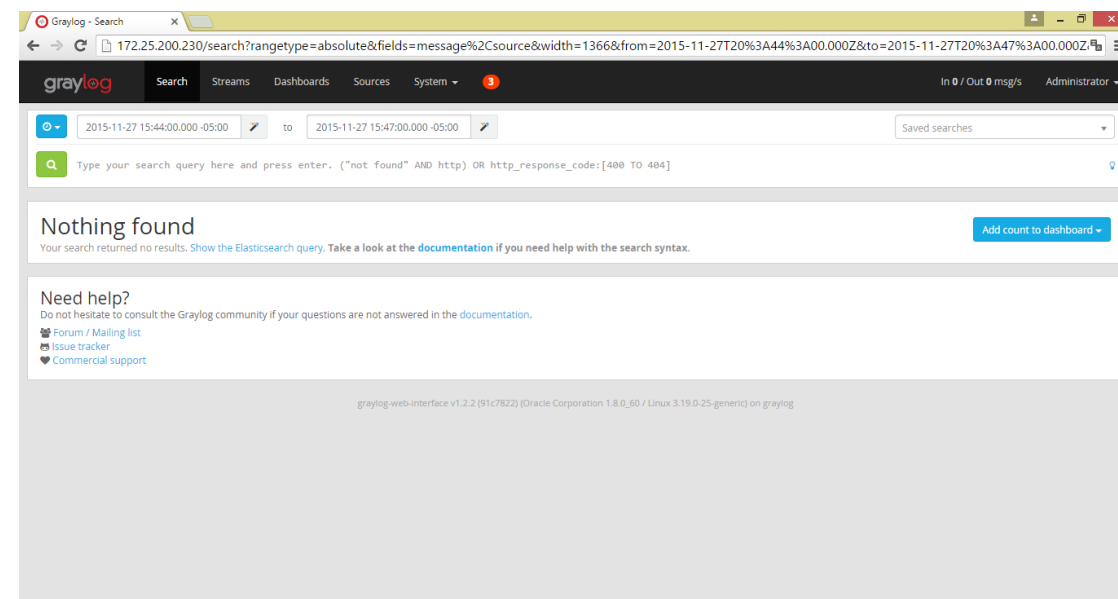
En la prueba 11 se realiza el ataque MITM atk6-fake\_router6 -D eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 13-4** se muestran las alertas originadas.



**Figura 13-4** Alertas obtenidas al ejecutar atk6-fake\_router6 -D eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.12. Prueba 12 atk6-fake\_router6 -F eth0 2001:db8:bad::/64

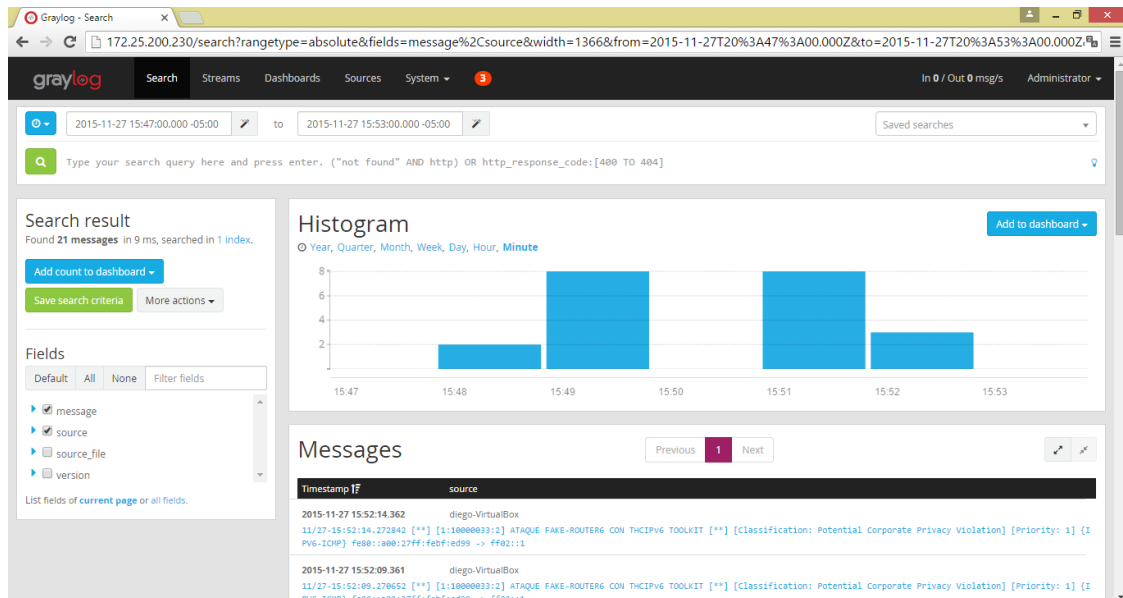
En la prueba 12 se realiza el ataque MITM atk6-fake\_router6 -F eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 14-4** se muestran las alertas originadas.



**Figura 14-4** Alertas obtenidas al ejecutar atk6-fake\_router6 -F eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.13. Prueba 13 atk6-fake\_router6 -H -D eth0 2001:db8:bad::/64

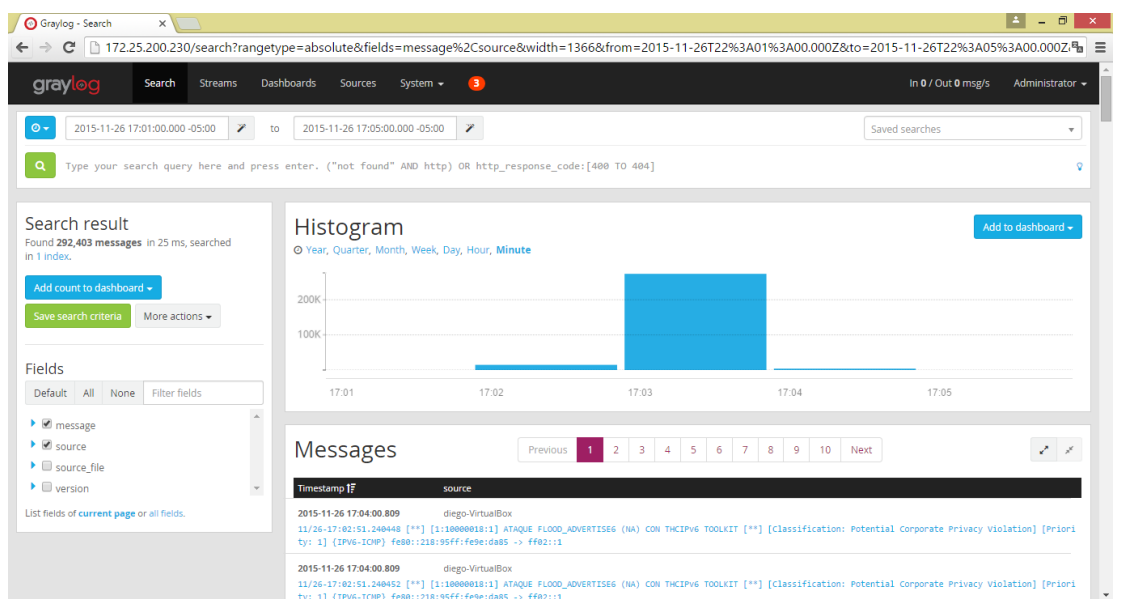
En la prueba 13 se realiza el ataque MITM atk6-fake\_router6 -H -D eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 15-4** se muestran las alertas originadas.



**Figura 15-4** Alertas IPv6 obtenidas con atk6-fake\_router6 -H -D eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.14. Prueba 14 atk6-flood\_advertise6 eth0

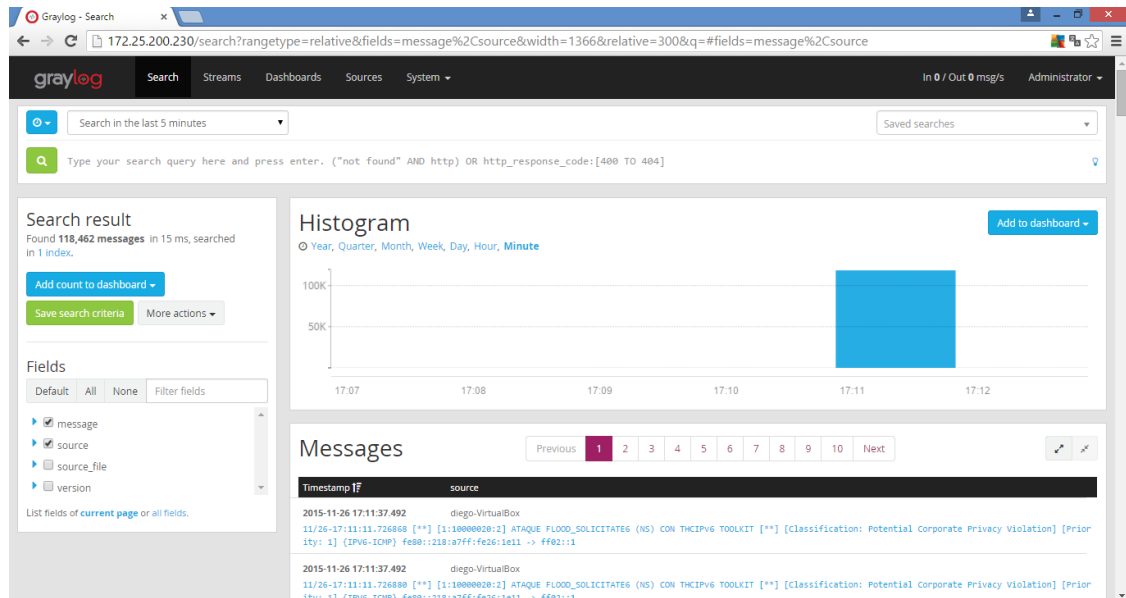
En la prueba 14 se realiza el ataque de denegación de servicios atk6-flood\_advertise6 sobre la interfaz eth0, en la **Figura 16-4** se muestran las alertas originadas.



**Figura 16-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_advertise6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.15. Prueba 15 atk6-flood\_solicitate6 eth0

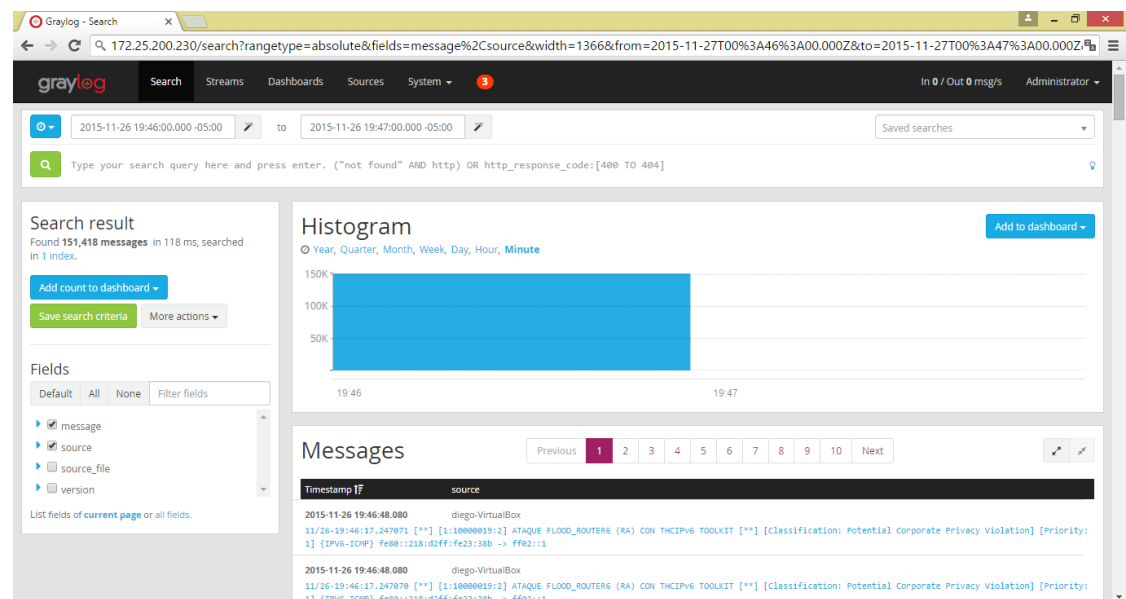
En la prueba 15 se realiza el ataque de denegación de servicios atk6-flood\_solicitate6 sobre la interfaz eth0, en la **Figura 17-4** se muestran las alertas originadas.



**Figura 17-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_solicitate6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.16. Prueba 16 atk6-flood\_router6 eth0

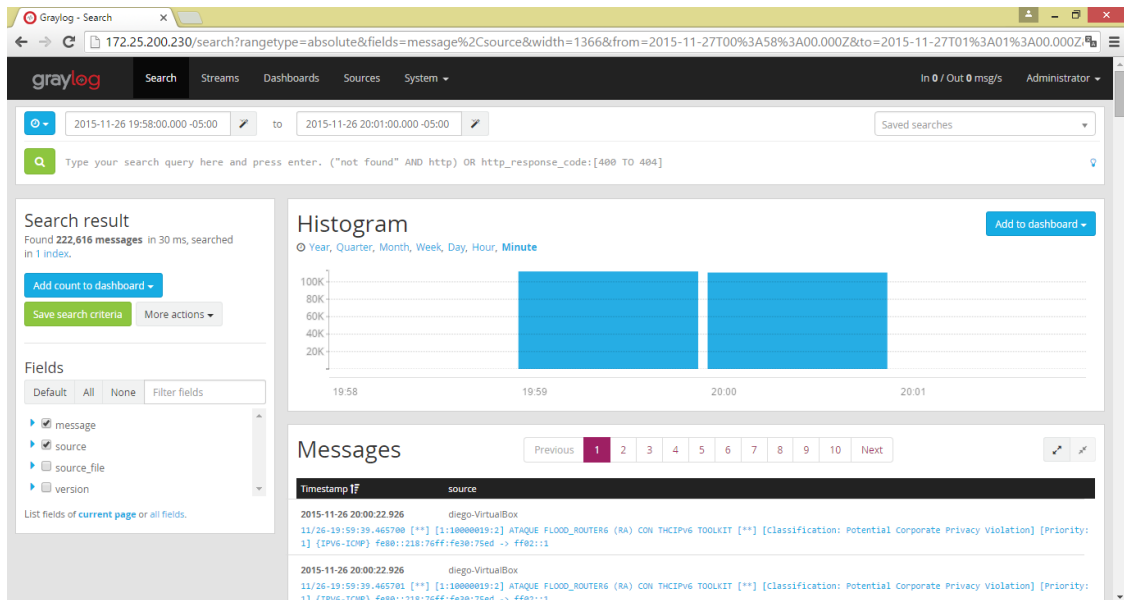
En la prueba 16 se realiza el ataque de denegación de servicios atk6-flood\_router6 sobre la interfaz eth0, en la **Figura 18-4** se muestran las alertas originadas.



**Figura 18-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_router6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.17. Prueba 17 atk6-flood\_router6 -F eth0

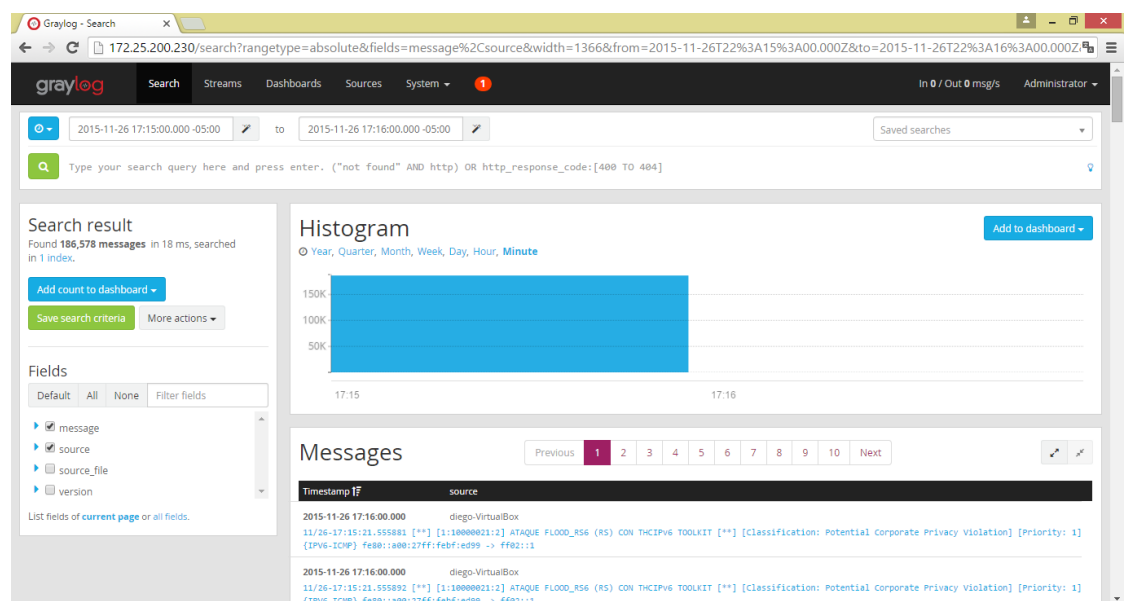
En la prueba 17 se realiza el ataque de denegación de servicios atk6-flood\_router6 -F sobre la interfaz eth0, en la **Figura 19-4** se muestran las alertas originadas.



**Figura 19-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_router6 -F eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.18. Prueba 18 atk6-flood\_rs6 eth0

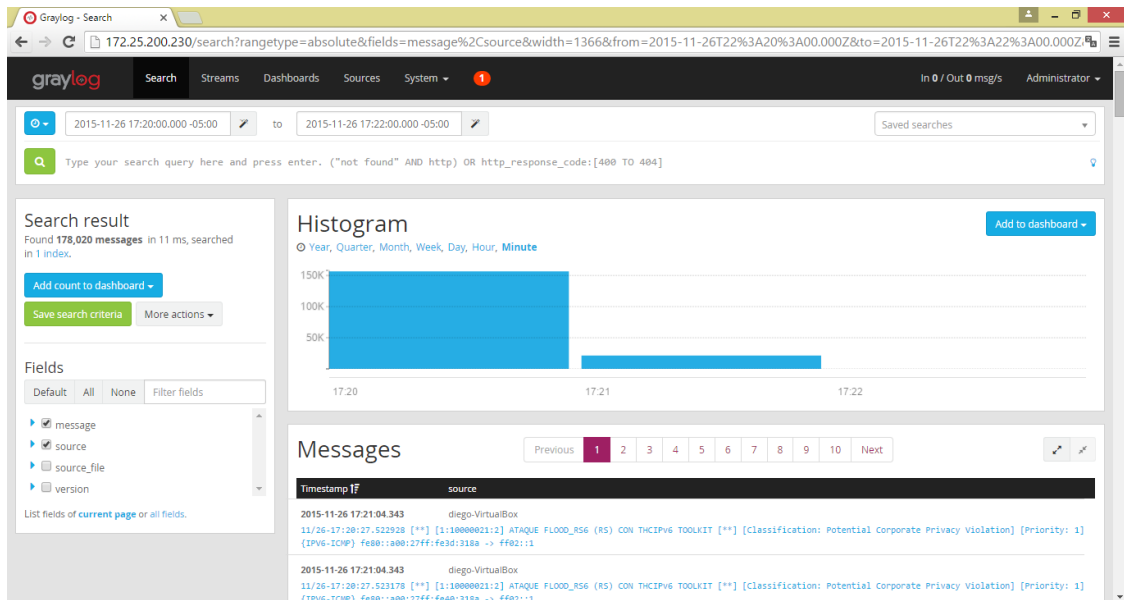
En la prueba 18 se realiza el ataque de denegación de servicios atk6-flood\_rs6 sobre la interfaz eth0, en la **Figura 20-4** se muestran las alertas originadas.



**Figura 20-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.19. Prueba 19 atk6-flood\_rs6 -s eth0

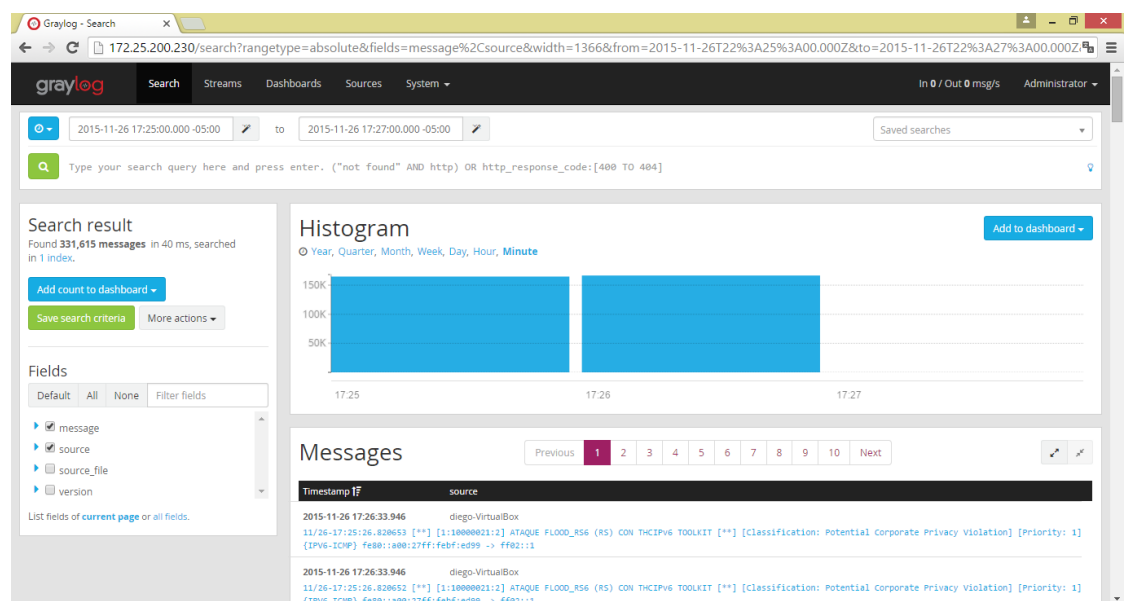
En la prueba 19 se realiza el ataque de denegación de servicios atk6-flood\_rs6 -s sobre la interfaz eth0, en la **Figura 21-4** se muestran las alertas originadas.



**Figura 21-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 -s eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.20. Prueba 20 atk6-flood\_rs6 -S eth0

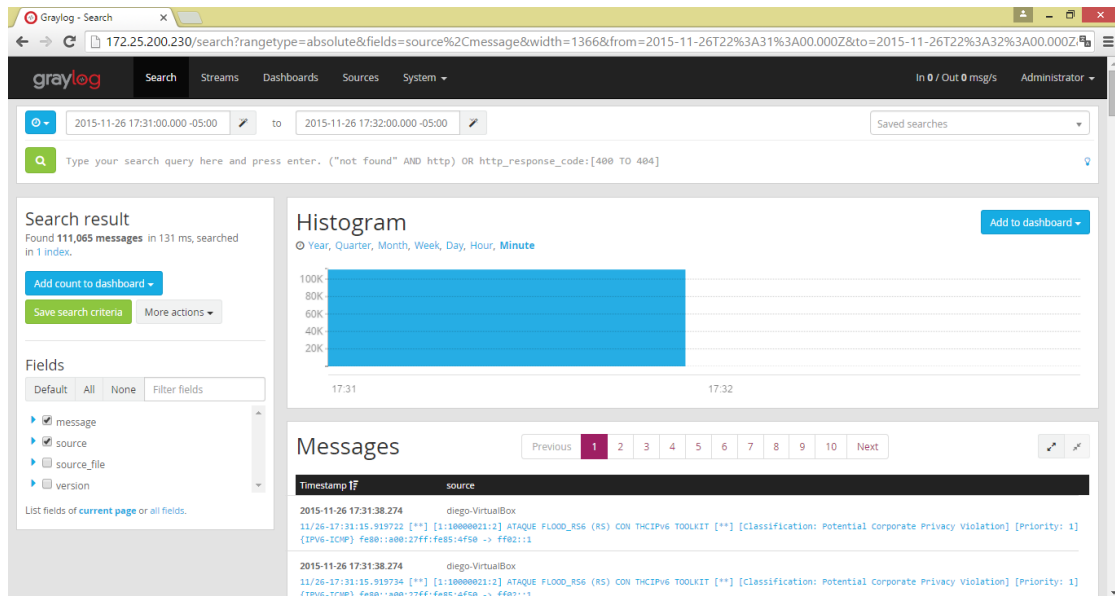
En la prueba 20 se realiza el ataque de denegación de servicios atk6-flood\_rs6 -S sobre la interfaz eth0, en la **Figura 22-4** se muestran las alertas originadas.



**Figura 22-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 -S eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.21. Prueba 21 atk6-flood\_rs6 -s -S eth0

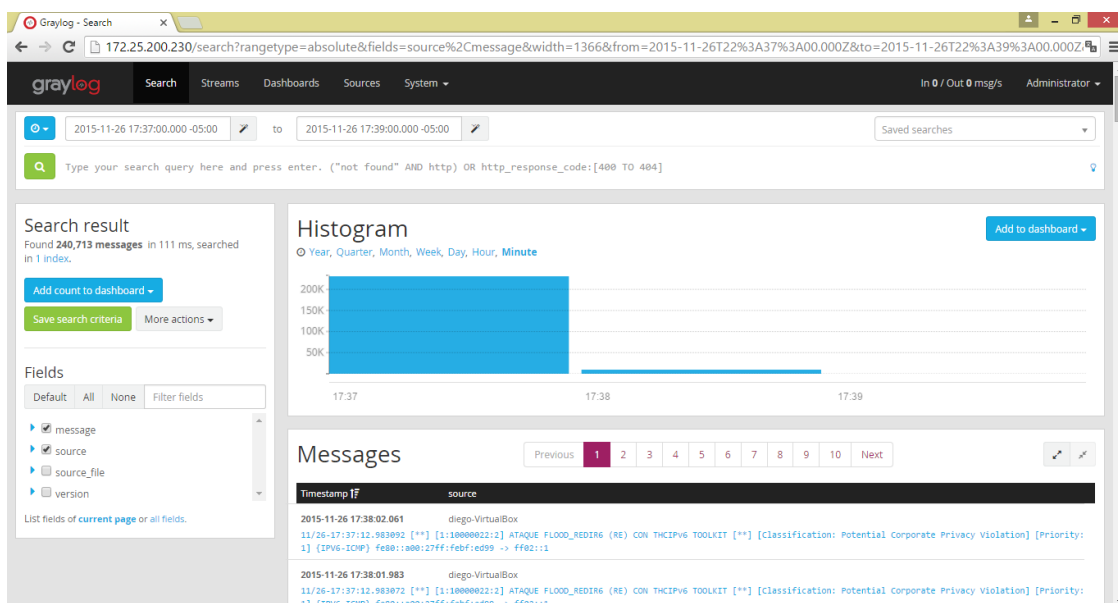
En la prueba 21 se realiza el ataque de denegación de servicios atk6-flood\_rs6 -s -S sobre la interfaz eth0, en la **Figura 23-4** se muestran las alertas originadas.



**Figura 23-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 -s -S eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.22. Prueba 22 atk6-flood\_redir6 eth0

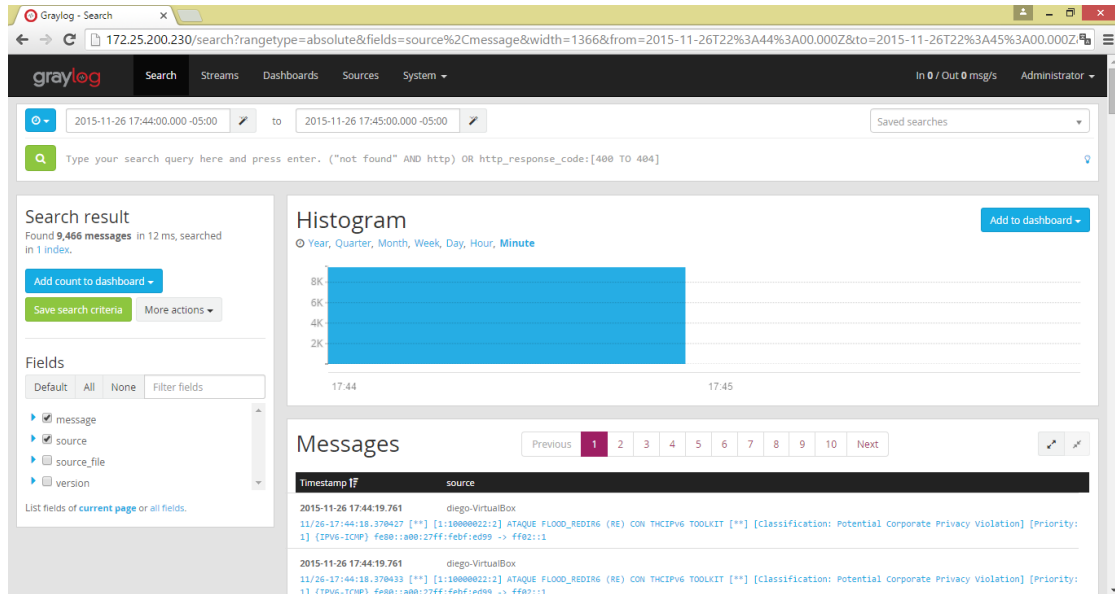
En la prueba 22 se realiza el ataque de denegación de servicios atk6-flood\_redir6 sobre la interfaz eth0, en la **Figura 24-4** se muestran las alertas originadas.



**Figura 24-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.23. Prueba 23 atk6-flood\_redir6 -H eth0

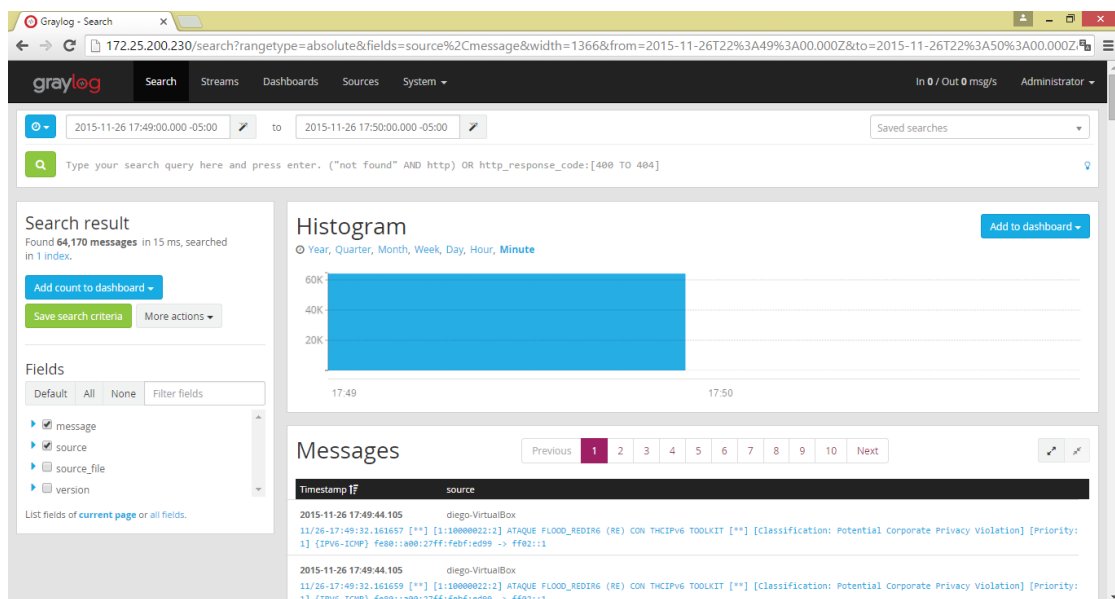
En la prueba 23 se realiza el ataque de denegación de servicios atk6-flood\_redir6 -H sobre la interfaz eth0, en la **Figura 25-4** se muestran las alertas originadas.



**Figura 25-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 -H eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.24. Prueba 24 atk6-flood\_redir6 -F eth0

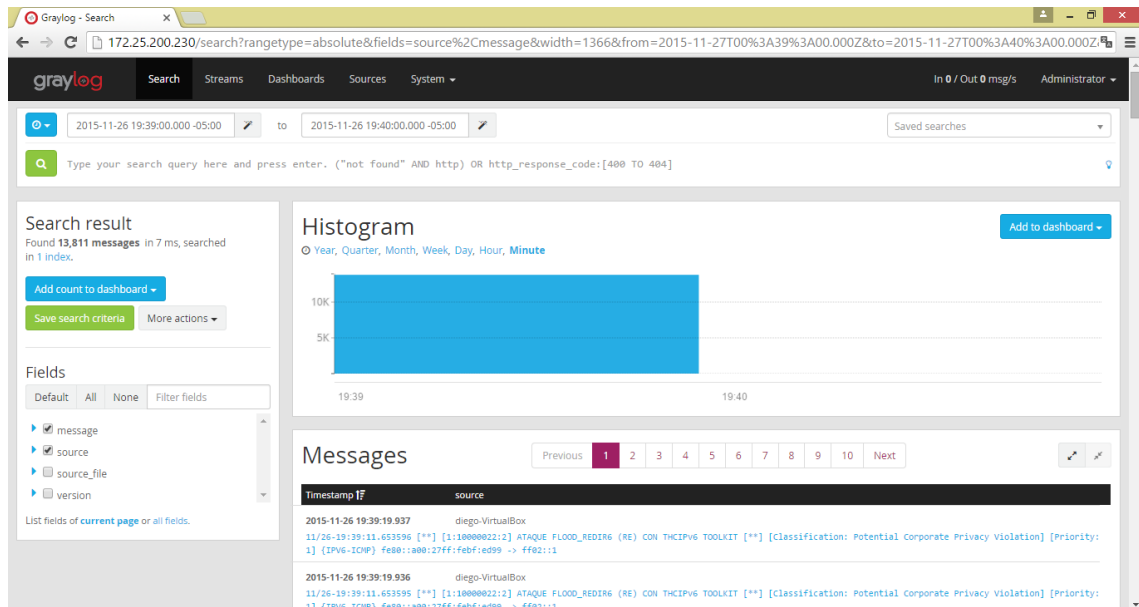
En la prueba 24 se realiza el ataque de denegación de servicios atk6-flood\_redir6 -F sobre la interfaz eth0, en la **Figura 26-4** se muestran las alertas originadas.



**Figura 26-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 -F eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.25. Prueba 25 atk6-flood\_redir6 -H -F eth0

En la prueba 25 se realiza el ataque de denegación de servicios atk6-flood\_redir6 -H -F sobre la interfaz eth0, en la **Figura 27-4** se muestran las alertas originadas.



**Figura 27-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 -H -F eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.1.1.26. Resumen de resultados

Los resultados obtenidos por este indicador una vez que se concluyó el experimento 1 se detallan en la **Tabla 1-4** es necesario señalar que por cada ataque detectado se cuantificó al indicador con un valor equivalente a 1, por el contrario por cada ataque que no es detectado se aplicó un valor igual a 0.

**Tabla 1-4** Resultados del indicador No. Alertas Positivas del Prototipo I

Pruebas Ejecutadas	Prototipo I
Prueba 1	1
Prueba 2	1
Prueba 3	1
Prueba 4	1
Prueba 5	1
Prueba 6	1
Prueba 7	1
Prueba 8	1



Prueba 9	1
Prueba 10	1
Prueba 11	1
Prueba 12	0
Prueba 13	1
Prueba 14	1
Prueba 15	1
Prueba 16	1
Prueba 17	1
Prueba 18	1
Prueba 19	1
Prueba 20	1
Prueba 21	1
Prueba 22	1
Prueba 23	1
Prueba 24	1
Prueba 25	1
<b>Total</b>	<b>24</b>

Realizado por: Caiza Diego, 2016

El resumen final de resultados del experimento 1 se detalla en la **Tabla 2-4**

**Tabla 2-4** Resumen de resultados del indicador No. Alertas Positivas del Prototipo I

<b>Indicador</b>	<b>Prototipo I</b>
No. alertas positivas	24

Realizado por: Caiza Diego, 2016

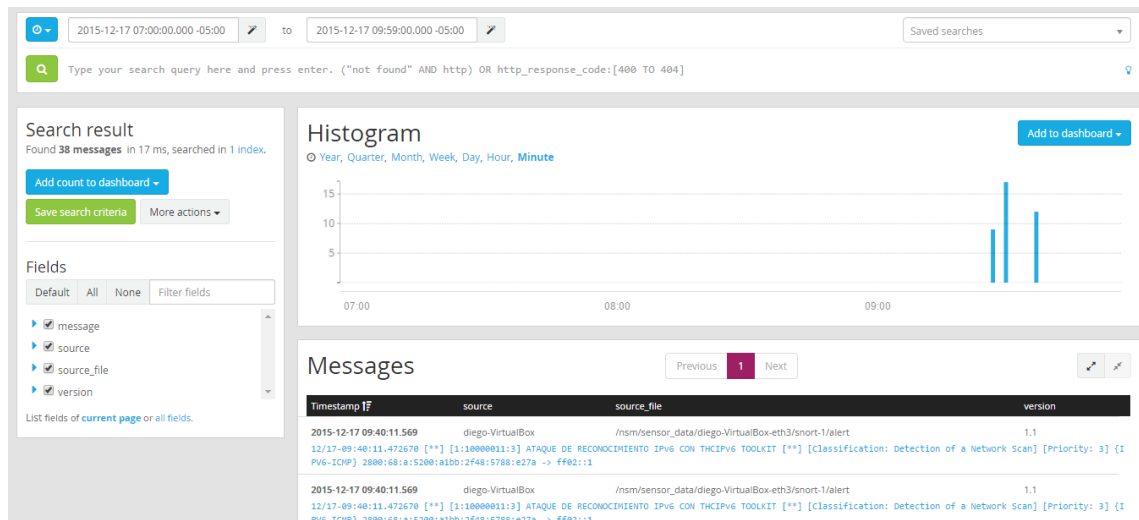
Los resultados obtenidos concluido el experimento 1 muestran la efectividad del Prototipo I durante la fase de detección de patrones de tráfico IPv6 anormal en la VLAN de Estudiantes en la FIE. De un total de 25 ataques generados se detectaron 24 es decir el Prototipo I tiene un 96% de efectividad para este experimento, se debe señalar que en la Prueba 12 el ataque atk6-fake\_router6 -F eth0 2001:db8:bad::/64 tiene un error en su ejecución ya que crea paquetes mal formados, razón por la cual se hace imposible su detección.

#### 4.1.1.2. No. Alertas falsas positivas

Los resultados obtenidos al realizar el experimento 3 durante un día normal de actividades en la FIE, se detallan en los siguientes ítems:

#### 4.1.1.2.1. Intervalo 1

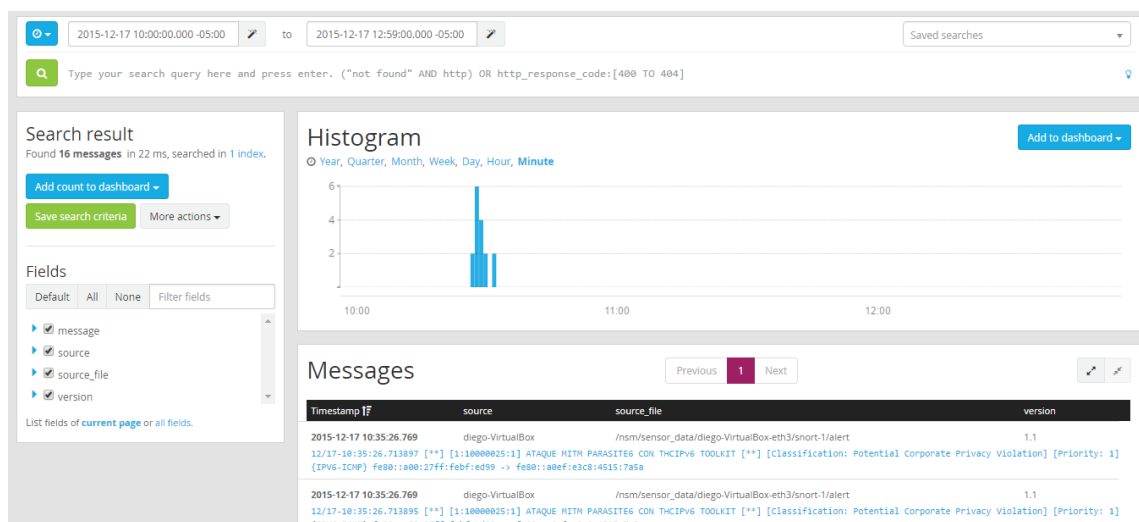
Durante el primer intervalo de tiempo comprendido entre las 07:00 y 09:59 horas, se obtuvieron los resultados mostrados en la **Figura 28-4**



**Figura 28-4** Alertas IPv6 obtenidas en el intervalo de 07:00 a 09:59 con el Prototipo I  
Realizado por: Caiza Diego, 2016

#### 4.1.1.2.2. Intervalo 2

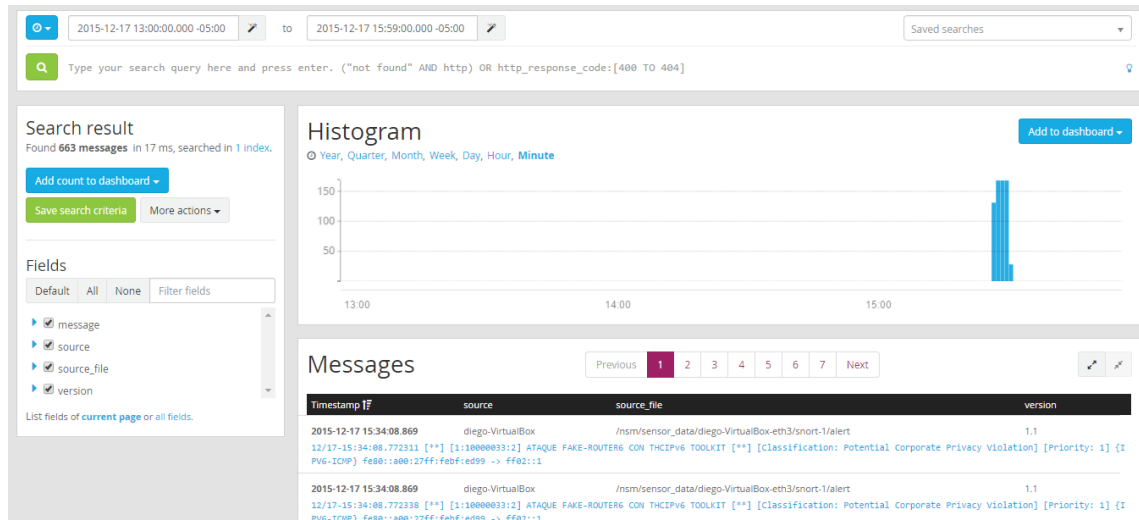
Durante el segundo intervalo de tiempo comprendido entre las 10:00 y 12:59 horas, se obtuvieron los resultados mostrados en la **Figura 29-4**



**Figura 29-4** Alertas IPv6 obtenidas en el intervalo de 10:00 a 12:59 con el Prototipo I  
Realizado por: Caiza Diego, 2016

#### 4.1.1.2.3. Intervalo 3

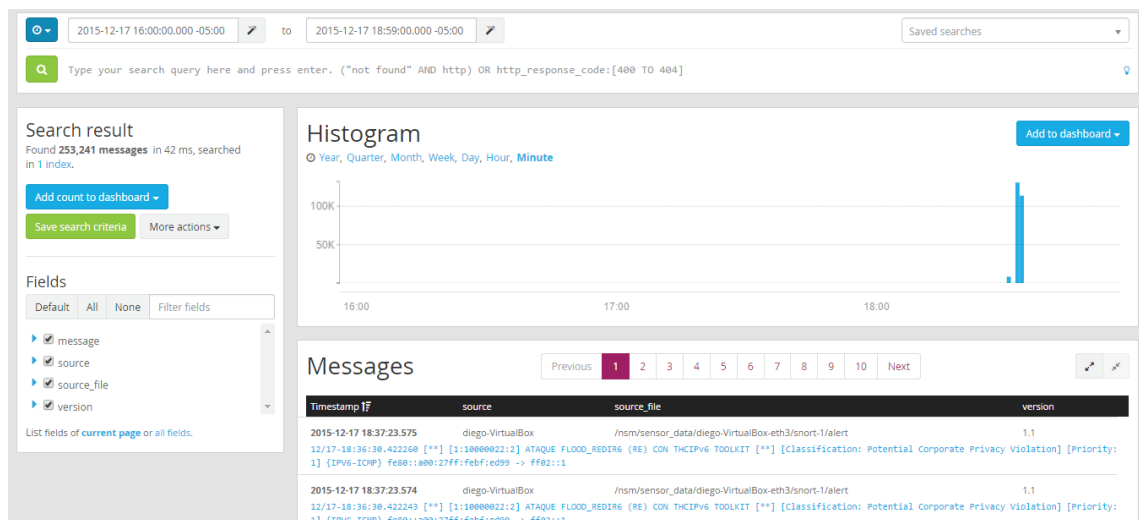
Durante el tercer intervalo de tiempo comprendido entre las 13:00 y 15:59 horas, se obtuvieron los resultados mostrados en la **Figura 30-4**



**Figura 30-4** Alertas IPv6 obtenidas en el intervalo de 13:00 a 15:59 con el Prototipo I  
Realizado por: Caiza Diego, 2016

#### 4.1.1.2.4. Intervalo 4

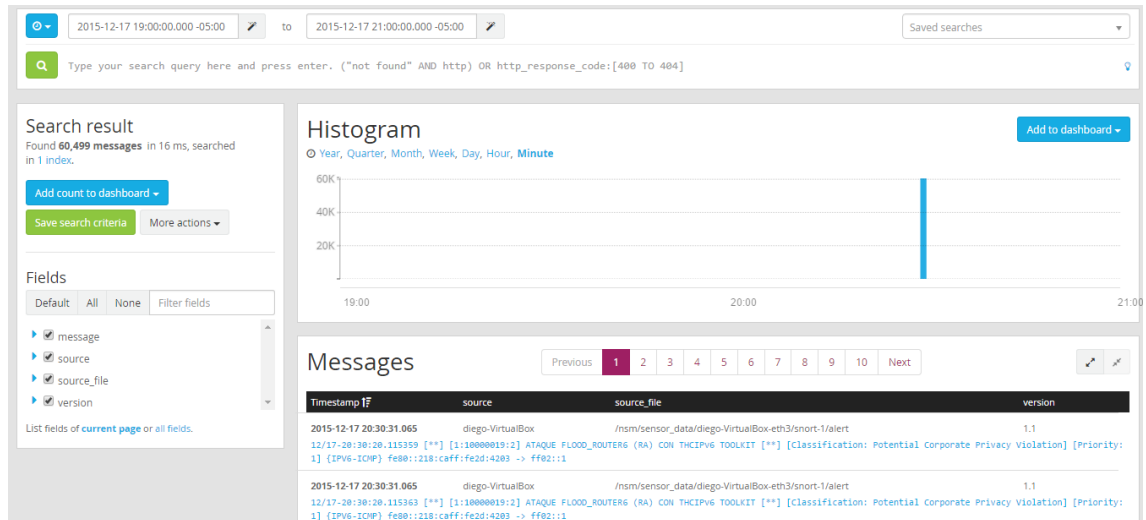
Durante el cuarto intervalo de tiempo comprendido entre las 16:00 y 18:59 horas, se obtuvieron los resultados mostrados en la **Figura 31-4**



**Figura 31-4** Alertas IPv6 obtenidas en el intervalo de 16:00 a 18:59 con el Prototipo I  
Realizado por: Caiza Diego, 2016

#### 4.1.1.2.5. Intervalo 5

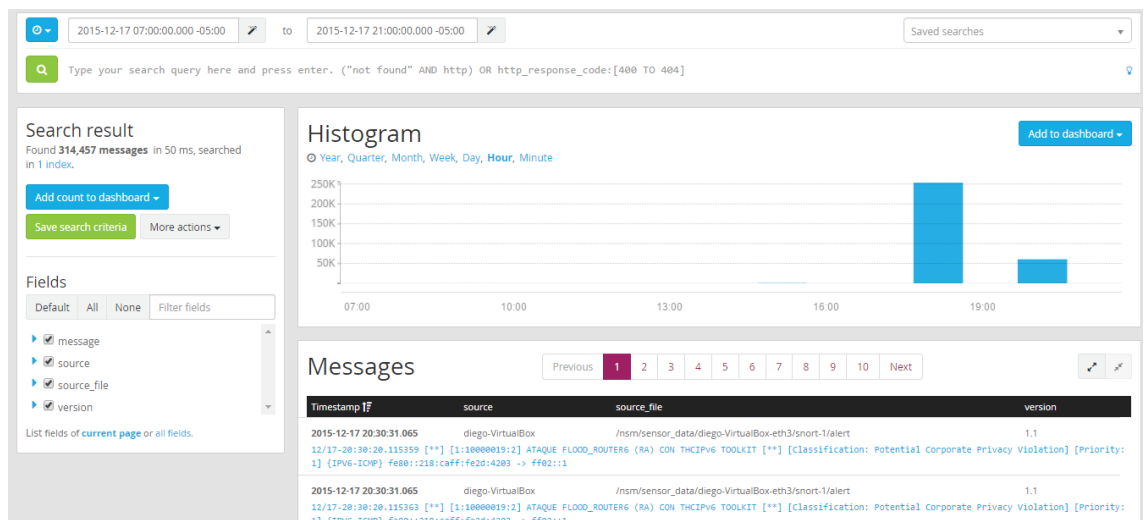
Durante el quinto intervalo de tiempo comprendido entre las 19:00 y 21:00 horas, se obtuvieron los resultados mostrados en la **Figura 32-4**



**Figura 32-4** Alertas IPv6 obtenidas en el intervalo de 19:00 a 21:00 con el Prototipo I  
Realizado por: Caiza Diego, 2016

#### 4.1.1.2.6. Resumen de Resultados

Las alertas producidas durante el periodo total de tiempo comprendido desde las 07:00 a 21:00 horas utilizando el Prototipo I, se pueden apreciar en la **Figura 33-4**



**Figura 33-4** Alertas IPv6 obtenidas en el intervalo de 07:00 a 21:00 con el Prototipo I  
Fuente: Caiza Diego, 2016

Los resultados obtenidos por este indicador una vez que se concluyó el experimento 3 se detallan en la **Tabla 3-4**, es necesario señalar que por cada alerta falsa se cuantifico

al indicador con un valor equivalente a 1, por el contrario por cada ataque verdadero realizado a manera de control se aplica un valor igual a 0.

**Tabla 3-4** Resumen de resultados del indicador No. Alertas Falsas Positivas del Prototipo I

Intervalos de tiempo	Categorización del ataque de control	Hora de ataque	No. Falsos Positivos
07:00 – 09:59	Ataque de reconocimiento	09:40	0
10:00 – 12:59	Ataque de MITM	10:35	0
13:00 – 15:59	Ataque de MITM	15:34	0
16:00 – 18:59	Ataque DDos	18:37	0
19:00 – 21:00	Ataque DDos	20:30	0
<b>Total</b>			<b>0</b>

Realizado por: Caiza Diego, 2016

El resumen final de resultados del experimento 3 se detalla en la **Tabla 4-4**

**Tabla 4-4** Resultados finales del indicador No. Alertas Falsas Positivas del Prototipo I

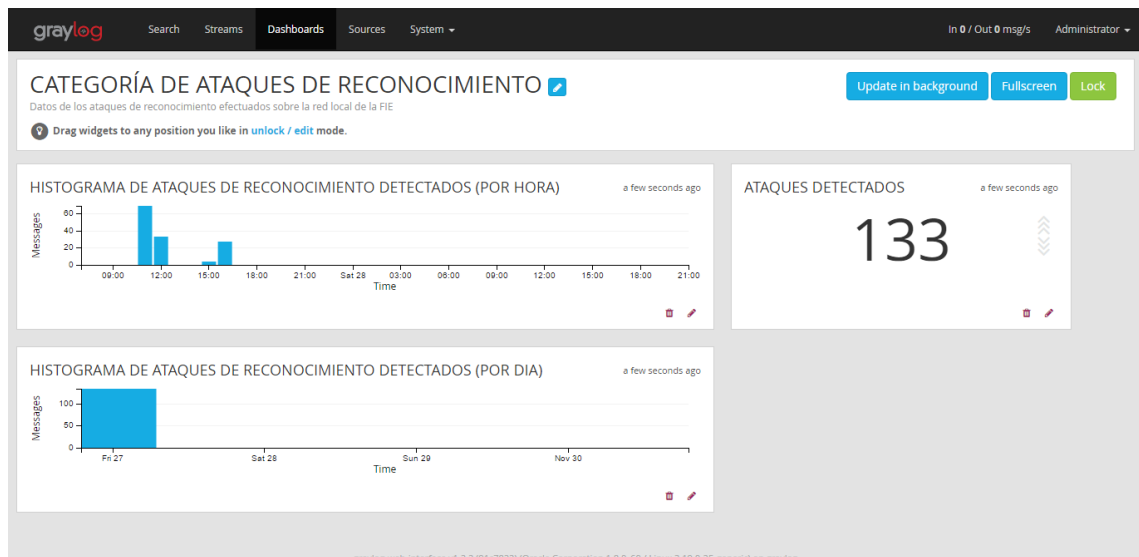
Indicador	Prototipo I
No. alertas falsas positivas	0

Realizado por: Caiza Diego, 2016

Los resultados obtenidos concluido el experimento 3 muestran la capacidad del Prototipo I para no generar alertas falsas durante el monitoreo de la VLAN de Estudiantes en la FIE. Del período comprendido desde las 07:00 hasta las 21:00 de un día normal de actividades no se detectaron alertas negativas, adicionalmente se logra deducir de estos resultados la precisión que tienen las reglas creadas para la detección de los patrones IPv6 maliciosos.

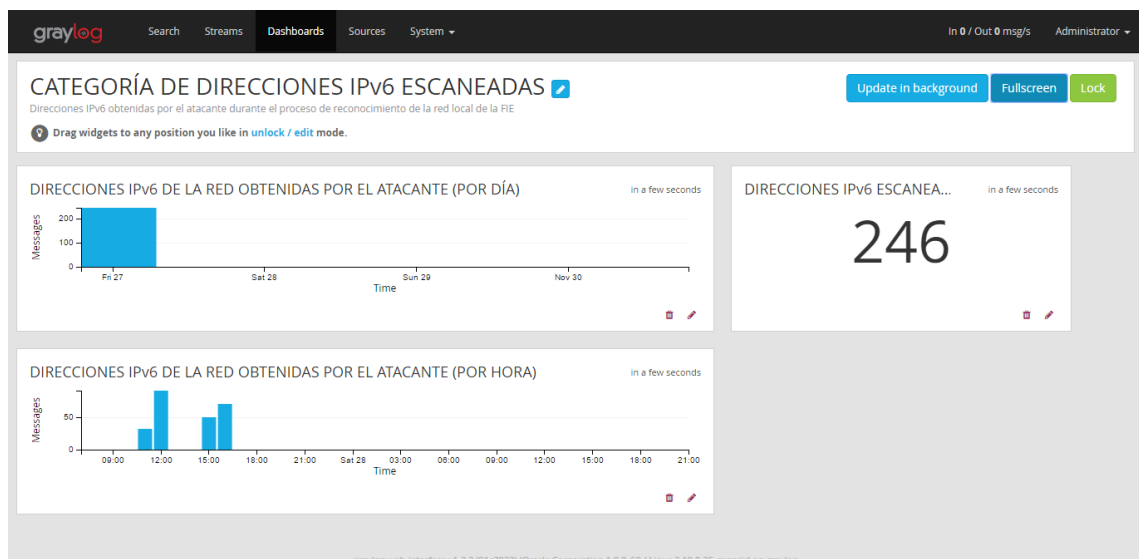
#### 4.1.1.3. Gestión de logs IPv6

Luego de realizar los experimentos de detección de número de alertas positivas y número de alertas falsas positivas, se registraron los datos estadísticos de los logs IPv6. En la **Figura 34-4** se muestran los datos estadísticos de los logs IPv6 categorizados como ataques de reconocimiento.



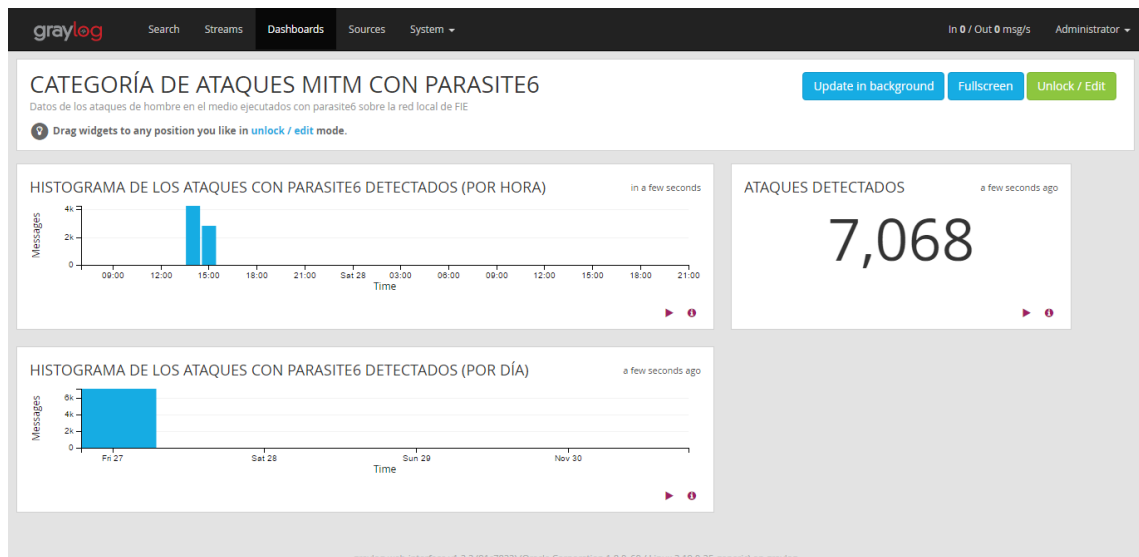
**Figura 34-4** Datos estadísticos de la categoría ataques de reconocimiento  
**Realizado por:** Caiza Diego, 2016

En la **Figura 35-4** se muestran los datos estadísticos de las direcciones IPv6 escaneadas durante los ataques de reconocimiento.



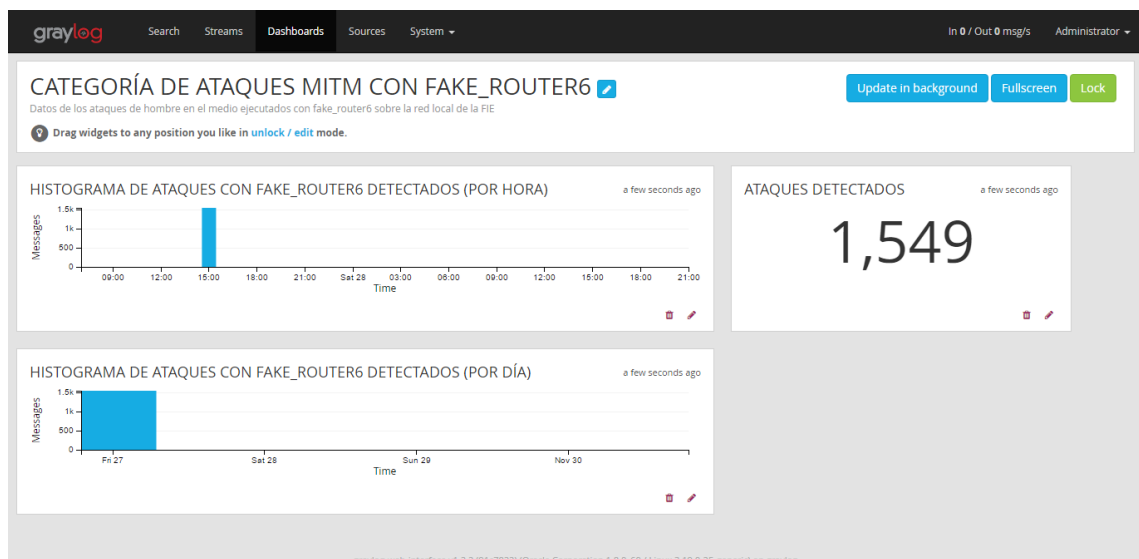
**Figura 35-4** Datos estadísticos de las direcciones IPv6 obtenidas por el atacante  
**Realizado por:** Caiza Diego, 2016

En la **Figura 36-4** se muestran los datos estadísticos de los logs IPv6 categorizados como ataques de hombre en el medio ejecutados con la herramienta parasite6.



**Figura 36-4** Datos estadísticos de ataques MITM con la herramienta parasite6  
**Realizado por:** Caiza Diego, 2016

En la **Figura 37-4** se muestran los datos estadísticos de los logs IPv6 categorizados como ataques de hombre en el medio ejecutados con la herramienta fake\_router6.



**Figura 37-4** Datos estadísticos de ataques MITM con la herramienta fake\_router6  
**Realizado por:** Caiza Diego, 2016

En la **Figura 38-4** se muestran los datos estadísticos de los de los logs IPv6 categorizados como ataques de denegación de servicios ejecutados con la herramienta flood\_advertise6.



**Figura 38-4** Datos estadísticos de denegación de servicios con flood\_advertise6  
**Realizado por:** Caiza Diego, 2016

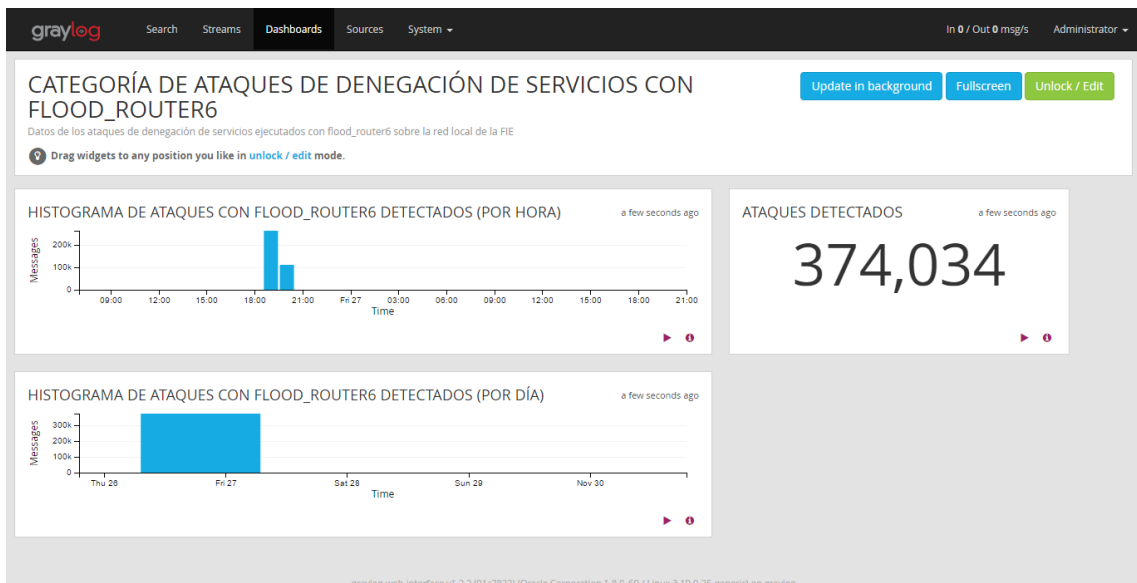
En la **Figura 39-4** se muestran los datos estadísticos de los logs IPv6 categorizados como ataques de denegación de servicios ejecutados con la herramienta flood\_solicitate6.



**Figura 39-4** Datos estadísticos de denegación de servicios con flood\_solicitate6  
**Realizado por:** Caiza Diego, 2016

En la **Figura 40-4** se muestran los datos estadísticos de los logs IPv6 categorizados como ataques de denegación de servicios ejecutados con la herramienta flood\_router6.





**Figura 40-4** Datos estadísticos de denegación de servicios con flood\_router6  
**Realizado por:** Caiza Diego, 2016

En la **Figura 41-4** se muestran los datos estadísticos de los logs IPv6 categorizados como ataques de denegación de servicios ejecutados con la herramienta flood\_rs6.



**Figura 41-4** Datos estadísticos de denegación de servicios con flood\_rs6  
**Realizado por:** Caiza Diego, 2016

En la **Figura 42-4** se muestran los datos estadísticos de los logs IPv6 categorizados como ataques de denegación de servicios ejecutados con la herramienta flood\_redir6.



**Figura 42-4** Datos estadísticos de denegación de servicios con flood\_redir6  
**Realizado por:** Caiza Diego, 2016

#### 4.1.1.3.1. Resumen

El resultado obtenido por este indicador una vez que se concluyó el experimento 5 se detallan en la **Tabla 5-4**, el Prototipo I cumple con el objetivo de gestionar los logs IPv6 de los ataques detectados.

**Tabla 5-4** Resumen de resultados del indicador Gestión de logs IPv6 del Prototipo I

Indicador	Prototipo I
Gestión de logs IPv6	SI

**Realizado por:** Caiza Diego, 2016

Los resultados obtenidos demuestran que el Prototipo I permite la presentación de las alertas o logs IPv6 generados, así como facilita su gestión a través de dashboards en la interfaz web de Graylog, muy fácil de crear y útil para efectuar el análisis en detalle de logs IPv6 recolectados.

#### 4.1.1.4. Replicación de logs IPv6

La replicación de logs tiene el objetivo de almacenar en tiempo real los logs IPv6 generados. En la **Figura 43-4** se muestra el archivo que contiene los logs IPv6 generados el cual se guarda en el módulo de Security Onion en la ruta /nsm/sensor\_data/diego-VirtualBox-eth3/snort-1.

```

alert.1450395264
File Edit Search Options Help
12/17-09:40:11.473935 [**] [1:10000010:3] DIRECCION IPv6 ESCANEADA CON THCIpV6 TOOLKIT [**] [Classification: Detection of a Network Sc
12/17-09:40:11.475666 [**] [1:10000010:3] DIRECCION IPv6 ESCANEADA CON THCIpV6 TOOLKIT [**] [Classification: Detection of a Network Sc
12/17-09:40:11.475668 [**] [1:10000010:3] DIRECCION IPv6 ESCANEADA CON THCIpV6 TOOLKIT [**] [Classification: Detection of a Network Sc
12/17-10:30:33.683774 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:30:33.683777 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:22.531328 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:22.531341 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:36.302320 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:36.302322 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:43.607430 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:43.607432 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:06.426973 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:06.426974 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:09.354647 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:09.354651 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:33:31.057837 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:35:26.713895 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:35:26.713897 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:35:26.713899 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:35:26.713901 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-15:30:13.779100 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:13.779101 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:13.779102 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:13.779103 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:13.779104 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.775702 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.775708 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776452 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776456 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776457 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776459 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi

```

**Figura 43-4** Archivo de logs IPv6 alojado en el módulo de Security Onion  
Realizado por: Caiza Diego, 2016

En la **Figura 44-4** se muestran los logs IPv6 almacenados en el servidor Graylog, en el cual se detalla la información recolectada durante los distintos ataques realizados en las pruebas.

```

2015-12-17 10:32:06.570      diego-VirtualBox
12/17-10:32:06.426973 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> fe80::9c1:83dd:d873:13f6

2015-12-17 10:31:43.670      diego-VirtualBox
12/17-10:31:43.607432 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> fe80::c54b:d32c:f451:deb2

2015-12-17 10:31:43.670      diego-VirtualBox
12/17-10:31:43.607430 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> fe80::c54b:d32c:f451:deb2

2015-12-17 10:31:36.369      diego-VirtualBox
12/17-10:31:36.302320 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> fe80::7dfe:a70c:7650:4ee8

2015-12-17 10:31:36.369      diego-VirtualBox
12/17-10:31:36.302322 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> fe80::7dfe:a70c:7650:4ee8

2015-12-17 10:31:22.569      diego-VirtualBox
12/17-10:31:22.531328 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> 2800:68:a:5200:f89e:aa48:387:28f1

2015-12-17 10:31:22.569      diego-VirtualBox
12/17-10:31:22.531341 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> 2800:68:a:5200:f89e:aa48:387:28f1

2015-12-17 10:30:33.769      diego-VirtualBox
12/17-10:30:33.683777 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> 2800:68:a:5200:fc2c:7e2e:8945:2e30

2015-12-17 10:30:33.769      diego-VirtualBox
12/17-10:30:33.683774 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> 2800:68:a:5200:fc2c:7e2e:8945:2e30

```

**Figura 44-4** Logs IPv6 alojados en el servidor Graylog  
Realizado por: Caiza Diego, 2016

Se puede verificar que ambos ficheros manejan los mismos registros en tiempo real, es decir, cumple el objetivo del indicador para el Prototipo I. El resumen final de esta comprobación se detalla en la **Tabla 6-4**

**Tabla 6-4** Resumen de resultados del indicador Replicación de logs IPv6

Indicador	Prototipo I
Replicación de logs IPv6	SI

Realizado por: Caiza Diego, 2016

#### 4.1.2. Prototipo II

Se desarrollaron las pruebas utilizando el Prototipo II en los experimentos establecidos para:

- No. Alertas positivas verdaderas
- No. Alertas falsas positivas
- Gestión de logs IPv6
- Replicación de logs IPv6

##### 4.1.2.1. No. Alertas positivas verdaderas (ataques detectados)

Los resultados obtenidos al realizar el experimento 2 se detallan en los siguientes ítems, y el detalle del tráfico malicioso capturado en el **Anexo D**.

##### 4.1.2.1.1. Prueba 1 atk6-alive6 eth0

En la prueba 1 se realizó el ataque categorizado como de reconocimiento atk6-alive6 sobre la interfaz eth0, en la **Figura 45-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 16:39:00.661      diego-VirtualBox
11/27-16:39:00.633845 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::e926:c3f:6518:9f78

2015-11-27 16:39:00.661      diego-VirtualBox
11/27-16:39:00.572498 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::78d3:3de4:f4ca:8518

2015-11-27 16:39:00.661      diego-VirtualBox
11/27-16:39:00.572615 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::78d3:3de4:f4ca:8518 -> fe80::5200:1

2015-11-27 16:39:00.461      diego-VirtualBox
11/27-16:39:00.430510 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::49e5:3439:63ca:385a

2015-11-27 16:39:00.461      diego-VirtualBox
11/27-16:39:00.393200 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::99cd:d353:8546:9651 -> fe80::5200:1

2015-11-27 16:39:00.461      diego-VirtualBox
11/27-16:39:00.430711 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::49e5:3439:63ca:385a -> fe80::5200:1

2015-11-27 16:39:00.061      diego-VirtualBox
11/27-16:38:59.973867 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::144:4368:230e:66a4 -> fe80::5200:1
```

**Figura 45-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-alive6 eth0

Realizado por: Caiza Diego, 2016

#### 4.1.2.1.2. Prueba 2 atk6-alive6 -4 172.25.0.0/21 eth0

En la prueba 2 se realizó el ataque categorizado como de reconocimiento atk6-alive6 - 4 172.25.0.0/21 sobre la interfaz eth0, en la **Figura 46-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 16:42:01.262      diego-VirtualBox
11/27-16:42:01.166457 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::28ab:78fe:a753:a582 -> fe80::5200:1

2015-11-27 16:42:01.262      diego-VirtualBox
11/27-16:42:01.166456 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::28ab:78fe:a753:a582

2015-11-27 16:42:01.161      diego-VirtualBox
11/27-16:42:01.132291 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
498:694d:6af6:71a2 -> fe80::5200:1

2015-11-27 16:42:01.161      diego-VirtualBox
11/27-16:42:01.148602 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::b801:a598:6a37:26a1 -> fe80::5200:1

2015-11-27 16:42:01.161      diego-VirtualBox
11/27-16:42:01.148599 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::b801:a598:6a37:26a1

2015-11-27 16:42:00.261      diego-VirtualBox
11/27-16:42:00.171204 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::c869:70b3:5e66:7d9f -> fe80::5200:1

2015-11-27 16:42:00.261      diego-VirtualBox
11/27-16:42:00.170074 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::c869:70b3:5e66:7d9f
```

**Figura 46-4** Alertas obtenidas al ejecutar el ataque atk6-alive6 -4 172.25.0.0/21  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.3. Prueba 3 atk6-alive6 -d eth0

En la prueba 1 se realizó el ataque categorizado como de reconocimiento atk6-alive6 - 4 172.25.0.0/21 sobre la interfaz eth0, en la **Figura 47-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 16:45:01.961      diego-VirtualBox
11/27-16:45:01.918459 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} 2800:68:a:5200:d009:de66:8cf5:704 -> fe80::5200:1

2015-11-27 16:45:01.961      diego-VirtualBox
11/27-16:45:01.917622 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> 2800:68:a:5200:d009:de66:8cf5:704

2015-11-27 16:45:01.261      diego-VirtualBox
11/27-16:45:01.151108 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::7
015:bac8:309a:9f1 -> fe80::5200:1

2015-11-27 16:45:01.261      diego-VirtualBox
11/27-16:45:01.170914 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::24eb:98c5:6ba8:41b7

2015-11-27 16:45:01.261      diego-VirtualBox
11/27-16:45:01.171115 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::24eb:98c5:6ba8:41b7 -> fe80::5200:1

2015-11-27 16:45:01.161      diego-VirtualBox
11/27-16:45:01.120529 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::7d4f:6dd9:dc0d:c95c -> fe80::5200:1

2015-11-27 16:45:01.161      diego-VirtualBox
11/27-16:45:01.120069 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::7d4f:6dd9:dc0d:c95c
```

**Figura 47-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-alive6 -d eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.4. Prueba 4 atk6-parasite6 -l eth0

En la prueba 4 se realiza el ataque MITM atk6-parasite6 –l sobre la interfaz eth0, en la **Figura 48-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 16:51:06.561      diego-VirtualBox
11/27-16:51:06.326419 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::118b:12f3:bd99:3197 -> fe80::5200:1

2015-11-27 16:51:05.462      diego-VirtualBox
11/27-16:51:05.334095 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::b516:ca19:98ca:273 -> fe80::5200:1

2015-11-27 16:51:05.462      diego-VirtualBox
11/27-16:51:05.333638 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::b516:ca19:98ca:273

2015-11-27 16:51:03.462      diego-VirtualBox
11/27-16:51:03.422328 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::4
9e5:3439:63ca:385a -> fe80::5200:1

2015-11-27 16:51:03.361      diego-VirtualBox
11/27-16:51:03.263994 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::16cc:20ff:fe85:9f47

2015-11-27 16:51:01.261      diego-VirtualBox
11/27-16:51:01.185675 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::7d4f:6dd9:dc0d:c95c -> fe80::5200:1

2015-11-27 16:51:01.261      diego-VirtualBox
11/27-16:51:01.186664 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::8
200:1 -> fe80::7d4f:6dd9:dc0d:c95c
```

**Figura 48-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.5. Prueba 5 atk6-parasite6 -l -R eth0

En la prueba 5 se realiza el ataque MITM atk6-parasite6 –l –R sobre la interfaz eth0, en la **Figura 49-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 16:57:01.961      diego-VirtualBox
11/27-16:57:01.850783 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::8
200:1 -> fe80::a00:27ff:febf:ed99

2015-11-27 16:57:01.661      diego-VirtualBox
11/27-16:57:01.627970 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::b
516:ca19:98ca:273 -> fe80::5200:1

2015-11-27 16:57:01.161      diego-VirtualBox
11/27-16:57:01.103581 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::40b3:8cd1:fc88:1c88 -> fe80::a00:27ff:febf:ed99

2015-11-27 16:57:01.161      diego-VirtualBox
11/27-16:57:01.103444 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a
00:27ff:febf:ed99 -> fe80::40b3:8cd1:fc88:1c88

2015-11-27 16:57:01.161      diego-VirtualBox
11/27-16:57:01.103584 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::40b3:8cd1:fc88:1c88 -> fe80::a00:27ff:febf:ed99

2015-11-27 16:57:01.161      diego-VirtualBox
11/27-16:57:01.103438 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a
00:27ff:febf:ed99 -> fe80::40b3:8cd1:fc88:1c88

2015-11-27 16:57:00.561      diego-VirtualBox
11/27-16:57:00.423031 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::8
200:1 -> fe80::16cc:20ff:fe85:9f47
```

**Figura 49-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -l -R eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.6. Prueba 6 atk6-parasite6 -I -F eth0

En la prueba 6 se realiza el ataque MITM atk6-parasite6 –I –F sobre la interfaz eth0, en la **Figura 50-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 17:04:02.661      diego-VirtualBox
11/27-17:04:02.518006 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> fe80::5200:1

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270597 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:fdfa:ab17:4a62:903b

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270598 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} 2800:68:a:5200:fdfa:ab17:4a62:903b -> fe80::a00:27ff:febf:ed99

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270591 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:fdfa:ab17:4a62:903b

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270598 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} 2800:68:a:5200:fdfa:ab17:4a62:903b -> fe80::a00:27ff:febf:ed99

2015-11-27 17:04:00.761      diego-VirtualBox
11/27-17:04:00.625835 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::ddf6:68f6:b486:2c80

2015-11-27 17:04:00.761      diego-VirtualBox
11/27-17:04:00.626084 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::ddf6:68f6:b486:2c80 -> fe80::5200:1
```

**Figura 50-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -I -F eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.7. Prueba 7 atk6-parasite6 -I -H eth0

En la prueba 7 se realiza el ataque MITM atk6-parasite6 –I –H sobre la interfaz eth0, en la **Figura 51-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 17:17:02.461      diego-VirtualBox
11/27-17:17:02.453235 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::dc85:3d4c:acac:c1a5

2015-11-27 17:17:02.461      diego-VirtualBox
11/27-17:17:02.453246 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::dc85:3d4c:acac:c1a5 -> fe80::5200:1

2015-11-27 17:17:00.361      diego-VirtualBox
11/27-17:17:00.324897 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::fc46:18c6:c2cf:c3f3

2015-11-27 17:17:00.361      diego-VirtualBox
11/27-17:17:00.325565 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::fc46:18c6:c2cf:c3f3 -> fe80::5200:1

2015-11-27 17:17:00.261      diego-VirtualBox
11/27-17:17:00.222252 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::3d3d:6188:99e6:d26 -> fe80::5200:1

2015-11-27 17:17:00.061      diego-VirtualBox
11/27-17:16:59.969694 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::28ab:78fe:a753:a582

2015-11-27 17:17:00.061      diego-VirtualBox
11/27-17:16:59.970084 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::28ab:78fe:a753:a582 -> fe80::5200:1
```

**Figura 51-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -I -H eth0  
Realizado por: Caiza Diego, 2016



#### 4.1.2.1.8. Prueba 8 atk6-parasite6 -I -R -F -H

En la prueba 8 se realiza el ataque MITM atk6-parasite6 -I -F -H sobre la interfaz eth0, en la **Figura 52-4** se muestran las alertas originadas por este tipo de ataque.

```
2015-11-27 17:24:03.061      diego-VirtualBox
11/27-17:24:03.002708 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::28fe:f610:210a:575c -> fe80::5200:1

2015-11-27 17:24:03.061      diego-VirtualBox
11/27-17:24:02.002494 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::28fe:f610:210a:575c

2015-11-27 17:24:02.961      diego-VirtualBox
11/27-17:24:02.867663 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a
07d:a920:1888:5010 -> fe80::5200:1

2015-11-27 17:24:00.961      diego-VirtualBox
11/27-17:24:00.889574 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::ddf6:68f6:b486:2c80 -> fe80::5200:1

2015-11-27 17:24:00.961      diego-VirtualBox
11/27-17:24:00.889344 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::ddf6:68f6:b486:2c80

2015-11-27 17:24:00.562      diego-VirtualBox
11/27-17:24:00.519446 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::dc85:3d4c:acac:c1a5

2015-11-27 17:24:00.562      diego-VirtualBox
11/27-17:24:00.519441 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::dc85:3d4c:acac:c1a5 -> fe80::5200:1
```

**Figura 52-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-parasite6 -I -R -F -H  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.9. Prueba 9 atk6-fake\_router6 eth0 2001:db8:bad::/64

En la prueba 9 se realiza el ataque MITM atk6-fake\_router6 eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 53-4** se muestran las alertas originadas.

```
2015-11-27 17:35:06.062      diego-VirtualBox
11/27-17:35:06.001019 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::2d8b:eaf:325a:c847 -> fe80::5200:1

2015-11-27 17:35:05.063      diego-VirtualBox
11/27-17:35:04.945838 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::c483:fbcd:395f:797f -> fe80::5200:1

2015-11-27 17:35:05.063      diego-VirtualBox
11/27-17:35:04.944091 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::c483:fbcd:395f:797f

2015-11-27 17:35:04.765      diego-VirtualBox
11/27-17:35:04.567014 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::c4aa:f553:1b7:82da -> fe80::5200:1

2015-11-27 17:35:04.765      diego-VirtualBox
11/27-17:35:04.567002 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::c4aa:f553:1b7:82da

2015-11-27 17:35:01.061      diego-VirtualBox
11/27-17:35:00.995063 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::2
d8b:eaf:325a:c847 -> fe80::5200:1

2015-11-27 17:35:00.661      diego-VirtualBox
11/27-17:35:00.625719 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::4
997:2001:24e2:a5a2 -> fe80::5200:1
```

**Figura 53-4** Alertas obtenidas al ejecutar atk6-fake\_router6 eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016



#### 4.1.2.1.10. Prueba 10 atk6-fake\_router6 -H eth0 2001:db8:bad::/64

En la prueba 10 se realiza el ataque MITM atk6-fake\_router6 -H eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 54-4** se muestran las alertas originadas.

2015-11-27 17:44:00.063	diego-VirtualBox	11/27-17:43:59.700589 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:bd0b:ab99:4a8a:9feb
2015-11-27 17:44:00.063	diego-VirtualBox	11/27-17:43:59.700597 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:bd0b:ab99:4a8a:9feb
2015-11-27 17:44:00.063	diego-VirtualBox	11/27-17:43:59.700593 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:bd0b:ab99:4a8a:9feb
2015-11-27 17:44:00.063	diego-VirtualBox	11/27-17:43:59.700595 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:bd0b:ab99:4a8a:9feb
2015-11-27 17:44:00.063	diego-VirtualBox	11/27-17:43:59.700602 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:bd0b:ab99:4a8a:9feb
2015-11-27 17:44:00.062	diego-VirtualBox	11/27-17:43:59.700573 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:bd0b:ab99:4a8a:9feb
2015-11-27 17:44:00.062	diego-VirtualBox	11/27-17:43:59.700586 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:bd0b:ab99:4a8a:9feb

**Figura 54-4** Alertas obtenidas al ejecutar atk6-fake\_router6 -H eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.11. Prueba 11 atk6-fake\_router6 -D eth0 2001:db8:bad::/64

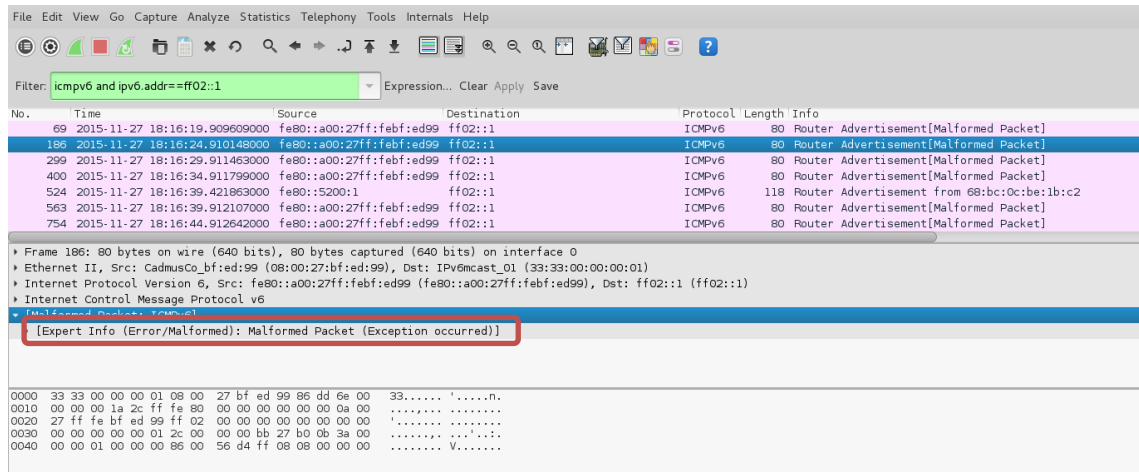
En la prueba 11 se realiza el ataque MITM atk6-fake\_router6 -D eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 55-4** se muestran las alertas originadas.

2015-11-27 18:10:24.362	diego-VirtualBox	11/27-18:10:24.315623 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::a00:27ff:febf:ed99 -> fe80::1925:2250:510a:3ed5
2015-11-27 18:10:12.963	diego-VirtualBox	11/27-18:10:12.900032 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::5c6c:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99
2015-11-27 18:10:12.963	diego-VirtualBox	11/27-18:10:12.899646 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::a00:27ff:febf:ed99 -> fe80::5c6c:e24e:3af9:dd1d
2015-11-27 18:10:12.963	diego-VirtualBox	11/27-18:10:12.900039 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::5c6c:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99
2015-11-27 18:10:12.962	diego-VirtualBox	11/27-18:10:12.899636 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::a00:27ff:febf:ed99 -> fe80::5c6c:e24e:3af9:dd1d
2015-11-27 18:10:08.161	diego-VirtualBox	11/27-18:10:07.889648 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5c6c:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99
2015-11-27 18:10:08.161	diego-VirtualBox	11/27-18:10:07.889653 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5c6c:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99

**Figura 55-4** Alertas obtenidas al ejecutar atk6-fake\_router6 -D eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.12. Prueba 12 atk6-fake\_router6 -F eth0 2001:db8:bad::/64

En la prueba 12 se realiza el ataque MITM atk6-fake\_router6 -F eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 56-4** se muestran el error “paquetes malformados” que se genera por esta herramienta desde el origen del ataque.



**Figura 56-4** Error al ejecutar atk6-fake\_router6 -F eth0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.13. Prueba 13 atk6-fake\_router6 -H -D eth0 2001:db8:bad::/64

En la prueba 13 se realiza el ataque MITM atk6-fake\_router6 -H -D eth0 2001:db8:bad::/64 sobre la interfaz eth0, en la **Figura 57-4** se muestran las alertas originadas.



**Figura 57-4** Alertas obtenidas con atk6-fake\_router6 -H -D eth0 0 2001:db8:bad::/64  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.14. Prueba 14 atk6-flood\_advertise6 eth0

En la prueba 14 se realiza el ataque de denegación de servicios atk6-flood\_advertise6 sobre la interfaz eth0, en la **Figura 58-4** se muestran las alertas originadas.

2015-12-14 18:53:12.912	diego-VirtualBox	12/14-18:53:12.777914 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:dff:fea3:dbae -> ff02::1
2015-12-14 18:53:12.912	diego-VirtualBox	12/14-18:53:12.777919 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:dff:fea3:dbae -> ff02::1
2015-12-14 18:53:12.912	diego-VirtualBox	12/14-18:53:12.777921 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:dff:fea3:dbae -> ff02::1
2015-12-14 18:53:12.912	diego-VirtualBox	12/14-18:53:12.777923 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:dff:fea3:dbae -> ff02::1
2015-12-14 18:53:12.912	diego-VirtualBox	12/14-18:53:12.777952 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:1bff:fe62:6841 -> ff02::1
2015-12-14 18:53:12.912	diego-VirtualBox	12/14-18:53:12.778092 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:cfff:fe39:2234 -> ff02::1
2015-12-14 18:53:12.691	diego-VirtualBox	12/14-18:53:12.612637 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::bc25:c519:b603:6c8e -> fe80::5200:1

**Figura 58-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_advertise6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.15. Prueba 15 atk6-flood\_solicitate6 eth0

En la prueba 15 se realiza el ataque de denegación de servicios atk6-flood\_solicitate6 sobre la interfaz eth0, en la **Figura 59-4** se muestran las alertas originadas.

2015-12-14 18:59:14.489	diego-VirtualBox	12/14-18:59:14.395160 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:30ff:feca:3cf5 -> ff02::1
2015-12-14 18:59:14.489	diego-VirtualBox	12/14-18:59:14.395175 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:b7ff:fef1:f797 -> ff02::1
2015-12-14 18:59:14.489	diego-VirtualBox	12/14-18:59:14.395176 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:b7ff:fef1:f797 -> ff02::1
2015-12-14 18:59:14.489	diego-VirtualBox	12/14-18:59:14.395023 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::218:13ff:fe29:e3af -> ff02::1
2015-12-14 18:59:14.396	diego-VirtualBox	12/14-18:59:14.292869 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::852c:31e4:1cd5:be4a -> fe80::fd98:710d:4461:5c32
2015-12-14 18:59:14.396	diego-VirtualBox	12/14-18:59:14.290347 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::852c:31e4:1cd5:be4a -> fe80::f40a:52a:2f79:bde5
2015-12-14 18:59:14.396	diego-VirtualBox	12/14-18:59:14.292874 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::f40a:52a:2f79:bde5 -> fe80::852c:31e4:1cd5:be4a

**Figura 59-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_solicitate6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.16. Prueba 16 atk6-flood\_router6 eth0

En la prueba 16 se realiza el ataque de denegación de servicios atk6-flood\_router6 sobre la interfaz eth0, en la **Figura 60-4** se muestran las alertas originadas.

```
2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546050 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:12ff:fe45:779e -> ff02::1

2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546054 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:12ff:fe45:779e -> ff02::1

2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546055 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPV6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:12ff:fe45:779e -> ff02::1

2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546029 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:c3ff:fe9f:4529 -> ff02::1

2015-12-14 20:19:11.078 diego-VirtualBox
12/14-20:19:11.027270 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe98:e5b6

2015-12-14 20:19:11.078 diego-VirtualBox
12/14-20:19:11.027273 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe98:e5b6

2015-12-14 20:19:11.078 diego-VirtualBox
12/14-20:19:11.032413 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe99:e5b6
```

**Figura 60-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_router6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.17. Prueba 17 atk6-flood\_router6 -F eth0

En la prueba 17 se realiza el ataque de denegación de servicios atk6-flood\_router6 -F sobre la interfaz eth0, en la **Figura 61-4** se muestran las alertas originadas.

```
2015-12-14 20:26:10.680 diego-VirtualBox
12/14-20:26:10.535205 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:b3ff:fed9:2bb4 -> ff02::1

2015-12-14 20:26:10.680 diego-VirtualBox
12/14-20:26:10.535206 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:b3ff:fed9:2bb4 -> ff02::1

2015-12-14 20:26:10.680 diego-VirtualBox
12/14-20:26:10.535208 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:f2ff:fe5f:f996 -> ff02::1

2015-12-14 20:26:10.680 diego-VirtualBox
12/14-20:26:10.534979 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPV6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:47ff:feee:6a09 -> ff02::1

2015-12-14 20:26:10.680 diego-VirtualBox
12/14-20:26:10.535207 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:f2ff:fe5f:f996 -> ff02::1

2015-12-14 20:26:10.680 diego-VirtualBox
12/14-20:26:10.534657 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPV6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:82ff:fe65:19 -> ff02::1

2015-12-14 20:26:10.680 diego-VirtualBox
12/14-20:26:10.534948 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPV6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:86ff:fea9:a4ae -> ff02::1

2015-12-14 20:26:09.805 diego-VirtualBox
12/14-20:26:09.572282 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe38:56ce
```

**Figura 61-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_router6 -F eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.18. Prueba 18 atk6-flood\_rs6 eth0

En la prueba 18 se realiza el ataque de denegación de servicios atk6-flood\_rs6 sobre la interfaz eth0, en la **Figura 62-4** se muestran las alertas originadas.

```
2015-12-14 19:10:04.977      diego-VirtualBox
12/14-19:10:04.862842 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::c982:1761:7aa8:67f0 -> fe80::5200:1

2015-12-14 19:10:04.977      diego-VirtualBox
12/14-19:10:04.862842 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::c982:1761:7aa8:67f0

2015-12-14 19:10:04.878      diego-VirtualBox
12/14-19:10:04.757734 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
412:373b:da56:fa6e -> fe80::5200:1

2015-12-14 19:10:03.376      diego-VirtualBox
12/14-19:10:03.300879 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::e
47b:7ac2:175a:f448 -> fe80::5200:1

2015-12-14 19:10:02.177      diego-VirtualBox
12/14-19:10:02.164794 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::c
54b:d32c:f451:deb2 -> fe80::5200:1

2015-12-14 19:10:02.077      diego-VirtualBox
12/14-19:10:01.984283 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::3
d4e:7e3a:ec4f:c769 -> fe80::5200:1

2015-12-14 19:10:01.576      diego-VirtualBox
12/14-19:10:01.475736 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
86e:71f6:b59:1e68 -> fe80::5200:1

2015-12-14 19:10:01.176      diego-VirtualBox
12/14-19:10:01.104096 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::2
1f5:35f:fff7:a46c -> fe80::5200:1
```

**Figura 62-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.19. Prueba 19 atk6-flood\_rs6 -s eth0

En la prueba 19 se realiza el ataque de denegación de servicios atk6-flood\_rs6 -s sobre la interfaz eth0, en la **Figura 63-4** se muestran las alertas originadas.

```
2015-12-14 19:14:00.876      diego-VirtualBox
12/14-19:14:00.831627 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::f40a:52a:2f79:bde5 -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876      diego-VirtualBox
12/14-19:14:00.831647 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::fd98:710d:4461:5c32 -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876      diego-VirtualBox
12/14-19:14:00.830006 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::48e4:1db2:aefe:51ef -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876      diego-VirtualBox
12/14-19:14:00.829212 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::4997:2001:24e2:a5a2 -> fe80::48e4:1db2:aefe:51ef

2015-12-14 19:14:00.876      diego-VirtualBox
12/14-19:14:00.831626 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::f40a:52a:2f79:bde5 -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876      diego-VirtualBox
12/14-19:14:00.830005 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::48e4:1db2:aefe:51ef -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876      diego-VirtualBox
12/14-19:14:00.829417 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::4997:2001:24e2:a5a2 -> fe80::2ca9:42fc:f1a0:5c7a

2015-12-14 19:14:00.176      diego-VirtualBox
12/14-19:14:00.139648 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::fd98:710d:4461:5c32 -> fe80::5200:1
```

**Figura 63-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 -s eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.20. Prueba 20 atk6-flood\_rs6 -S eth0

En la prueba 20 se realiza el ataque de denegación de servicios atk6-flood\_rs6 -S sobre la interfaz eth0, en la **Figura 64-4** se muestran las alertas originadas.

2015-12-14 19:19:04.176	diego-VirtualBox	12/14-19:19:04.108488 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::c982:1761:7aa8:67f0
2015-12-14 19:19:03.676	diego-VirtualBox	12/14-19:19:03.588202 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::6cb2:7e00:6962:6feb
2015-12-14 19:19:03.676	diego-VirtualBox	12/14-19:19:03.615265 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a0ef:e3c8:4515:7a5a -> fe80::5200:1
2015-12-14 19:19:03.676	diego-VirtualBox	12/14-19:19:03.588441 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::6cb2:7e00:6962:6feb -> fe80::5200:1
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126499 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a080:1b5e:9fe9:fc61 -> fe80::9c1:83dd:d873:13f6
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126670 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::9c1:83dd:d873:13f6 -> fe80::a080:1b5e:9fe9:fc61
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126500 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::a080:1b5e:9fe9:fc61 -> fe80::9c1:83dd:d873:13f6
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126670 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::9c1:83dd:d873:13f6 -> fe80::a080:1b5e:9fe9:fc61

**Figura 64-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 -S eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.21. Prueba 21 atk6-flood\_rs6 -s -S eth0

En la prueba 21 se realiza el ataque de denegación de servicios atk6-flood\_rs6 -s -S sobre la interfaz eth0, en la **Figura 65-4** se muestran las alertas originadas.

2015-12-14 19:21:04.978	diego-VirtualBox	12/14-19:21:04.967650 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::58e8:2b03:8dd0:cbd1
2015-12-14 19:21:03.678	diego-VirtualBox	12/14-19:21:03.617782 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::a080:1b5e:9fe9:fc61 -> fe80::5200:1
2015-12-14 19:21:03.678	diego-VirtualBox	12/14-19:21:03.617154 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::a080:1b5e:9fe9:fc61
2015-12-14 19:21:03.076	diego-VirtualBox	12/14-19:21:02.938025 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} 2800:68:a:5200:f4a6:2add:868a:1aba -> fe80::5200:1
2015-12-14 19:21:03.076	diego-VirtualBox	12/14-19:21:02.937824 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2800:68:a:5200:f4a6:2add:868a:1aba
2015-12-14 19:21:03.076	diego-VirtualBox	12/14-19:21:03.040874 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5077:ebe:261:eeb -> fe80::5200:1
2015-12-14 19:21:02.876	diego-VirtualBox	12/14-19:21:02.850028 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::c982:1761:7aa8:67f0 -> fe80::5200:1
2015-12-14 19:21:02.676	diego-VirtualBox	12/14-19:21:02.569051 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::581f:52ad:a6d1:4abc

**Figura 65-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_rs6 -s -S eth0  
Realizado por: Caiza Diego, 2016



#### 4.1.2.1.22. Prueba 22 atk6-flood\_redir6 eth0

En la prueba 22 se realiza el ataque de denegación de servicios atk6-flood\_redir6 sobre la interfaz eth0, en la **Figura 66-4** se muestran las alertas originadas.

2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.233069 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::c54b:d32c:f451:deb2 -> fe80::fd98:710d:4461:5c32
2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.233115 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::f40a:52a:2f79:bde5 -> fe80::c54b:d32c:f451:deb2
2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.223014 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::c54b:d32c:f451:deb2 -> fe80::f40a:52a:2f79:bde5
2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.233068 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::c54b:d32c:f451:deb2 -> fe80::fd98:710d:4461:5c32
2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.223014 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::c54b:d32c:f451:deb2 -> fe80::f40a:52a:2f79:bde5
2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.233070 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::fd98:710d:4461:5c32 -> fe80::c54b:d32c:f451:deb2
2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.233114 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::f40a:52a:2f79:bde5 -> fe80::c54b:d32c:f451:deb2
2015-12-14 19:30:58.276	diego-VirtualBox	12/14-19:30:58.222043 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} fe80::c54b:d32c:f451:deb2 -> fe80::2ca9:42fc:f1a0:5c7a

**Figura 66-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.23. Prueba 23 atk6-flood\_redir6 -H eth0

En la prueba 23 se realiza el ataque de denegación de servicios atk6-flood\_redir6 -H sobre la interfaz eth0, en la **Figura 67-4** se muestran las alertas originadas.

2015-12-14 19:39:01.476	diego-VirtualBox	12/14-19:39:01.452321 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fedd:b0bb
2015-12-14 19:39:00.676	diego-VirtualBox	12/14-19:39:00.559549 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> 2800:68:a:5200:c5e:4ce4:6b55:2863
2015-12-14 19:39:00.676	diego-VirtualBox	12/14-19:39:00.559422 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} 2800:68:a:5200:c5e:4ce4:6b55:2863 -> fe80::5200:1
2015-12-14 19:39:00.476	diego-VirtualBox	12/14-19:39:00.447541 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:feda:70b7
2015-12-14 19:39:00.476	diego-VirtualBox	12/14-19:39:00.436679 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fedd:80be
2015-12-14 19:39:00.476	diego-VirtualBox	12/14-19:39:00.447352 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fedd:b0bb
2015-12-14 19:39:00.276	diego-VirtualBox	12/14-19:39:00.200980 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPv6-ICMP} 2800:68:a:5200:c15d:e222:61:600e -> fe80::5200:1
2015-12-14 19:39:00.076	diego-VirtualBox	12/14-19:38:59.996932 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::9d17:f834:80a3:3894

**Figura 67-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 -H eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.24. Prueba 24 atk6-flood\_redir6 -F eth0

En la prueba 24 se realiza el ataque de denegación de servicios atk6-flood\_redir6 -F sobre la interfaz eth0, en la **Figura 68-4** se muestran las alertas originadas.

2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140118 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf
2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140125 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf
2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140109 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf
2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140116 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf
2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140120 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf
2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140117 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf
2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140121 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf
2015-12-14 19:46:00.176	diego-VirtualBox	12/14-19:46:00.140122 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe9f:31cf

**Figura 68-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 -F eth0  
Realizado por: Caiza Diego, 2016

#### 4.1.2.1.25. Prueba 25 atk6-flood\_redir6 -H -F eth0

En la prueba 25 se realiza el ataque de denegación de servicios atk6-flood\_redir6 -H -F sobre la interfaz eth0, en la **Figura 69-4** se muestran las alertas originadas.

2015-12-14 19:51:00.276	diego-VirtualBox	12/14-19:51:00.230808 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe56:2b7
2015-12-14 19:51:00.276	diego-VirtualBox	12/14-19:51:00.240602 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe3e:62ce
2015-12-14 19:51:00.276	diego-VirtualBox	12/14-19:51:00.240603 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe3e:62ce
2015-12-14 19:51:00.276	diego-VirtualBox	12/14-19:51:00.240606 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe3e:62ce
2015-12-14 19:51:00.276	diego-VirtualBox	12/14-19:51:00.240607 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe3e:62ce
2015-12-14 19:51:00.276	diego-VirtualBox	12/14-19:51:00.241637 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe3e:62ce
2015-12-14 19:51:00.276	diego-VirtualBox	12/14-19:51:00.238942 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPv6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe3e:82ce

**Figura 69-4** Alertas IPv6 obtenidas al ejecutar el ataque atk6-flood\_redir6 -H -F eth0  
Realizado por: Caiza Diego, 2016



#### 4.1.2.1.26. Resumen de resultados

Los resultados obtenidos por este indicador una vez que se concluyó el experimento 2 se detallan en la **Tabla 7-4**, es necesario señalar que por cada ataque detectado se cuantificó al indicador con un valor equivalente a 1, por el contrario por cada ataque que no es detectado se aplicó un valor igual a 0.

**Tabla 7-4** Resultados del indicador No. Alertas Positivas del Prototipo II

<b>Pruebas Ejecutadas</b>	<b>Prototipo II</b>
Prueba 1	0
Prueba 2	0
Prueba 3	0
Prueba 4	0
Prueba 5	0
Prueba 6	0
Prueba 7	0
Prueba 8	0
Prueba 9	0
Prueba 10	0
Prueba 11	0
Prueba 12	0
Prueba 13	0
Prueba 14	1
Prueba 15	1
Prueba 16	1
Prueba 17	1
Prueba 18	0
Prueba 19	0
Prueba 20	0
Prueba 21	0
Prueba 22	0
Prueba 23	0
Prueba 24	0
Prueba 25	0
<b>Total</b>	<b>4</b>

Realizado por: Caiza Diego, 2016

El resumen final del experimento 2 se detalla en la **Tabla 8-4**

**Tabla 8-4** Resumen de resultados del indicador No. Alertas Positivas del Prototipo II

Indicador	Prototipo II
No. alertas positivas	4

Realizado por: Caiza Diego, 2016

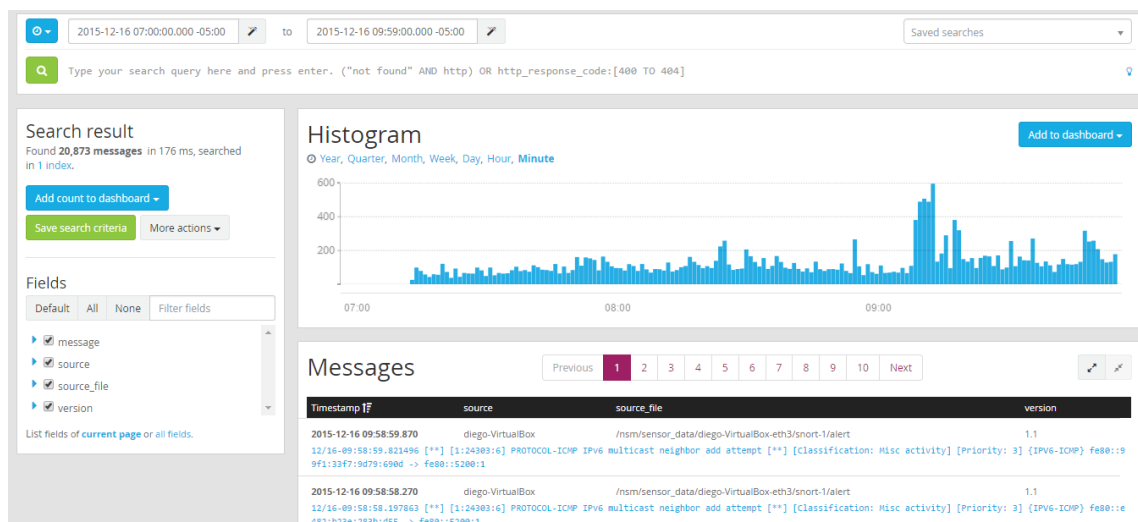
Los resultados obtenidos concluido el experimento 2 muestran la efectividad del Prototipo II durante la fase de detección de patrones de tráfico IPv6 anormal en la VLAN de Estudiantes. De un total de 25 ataques generados se detectaron 4 es decir el Prototipo I tiene un 16% de efectividad para este experimento, se debe señalar que en la Prueba 12 el ataque `atk6-fake_router6 -F eth0 2001:db8:bad::/64` tiene un error en su ejecución ya que crea paquetes mal formados, razón por la cual se hace imposible su detección.

#### 4.1.2.2. No. Alertas falsas positivas

Los resultados obtenidos al realizar el experimento 4 se detallan en los siguientes ítems:

##### 4.1.2.2.1. Intervalo 1

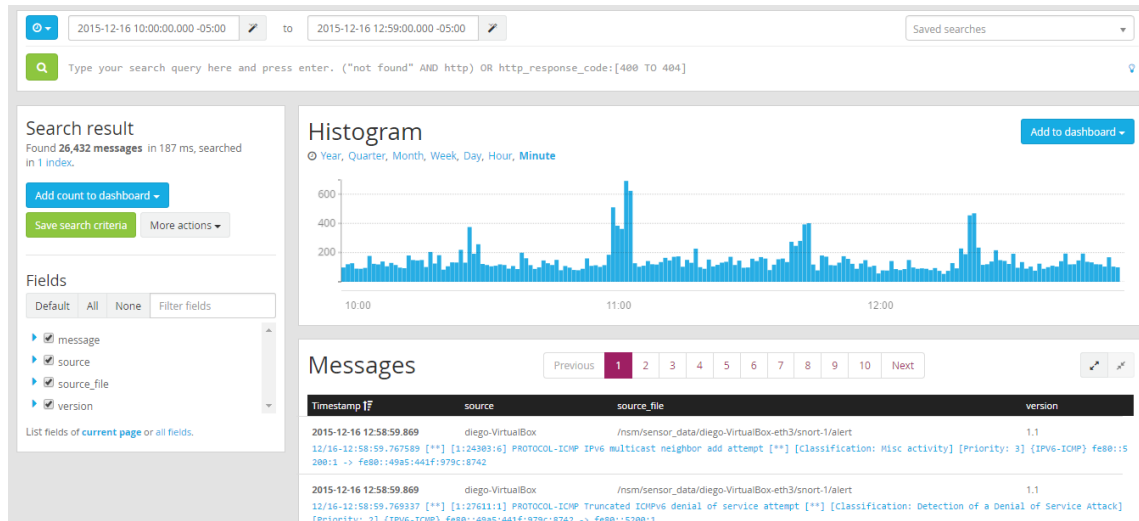
Durante el primer intervalo de tiempo comprendido entre las 07:00 y 09:59 horas, se obtuvieron los resultados mostrados en la **Figura 70-4**



**Figura 70-4** Alertas IPv6 obtenidas en el intervalo de 07:00 a 09:59 con el Prototipo II  
Realizado por: Caiza Diego, 2016

#### 4.1.2.2. Intervalo 2

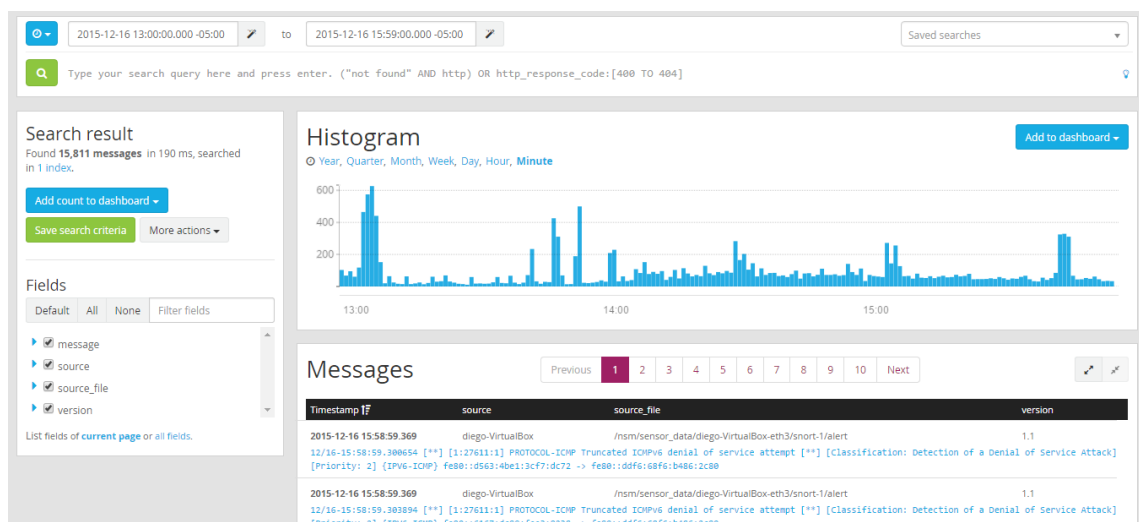
Durante el segundo intervalo de tiempo comprendido entre las 10:00 y 12:59 horas, se obtuvieron los resultados mostrados en la **Figura 71-4**



**Figura 71-4** Alertas IPv6 obtenidas en el intervalo de 10:00 a 12:59 con el Prototipo II  
Realizado por: Caiza Diego, 2016

#### 4.1.2.2.3. Intervalo 3

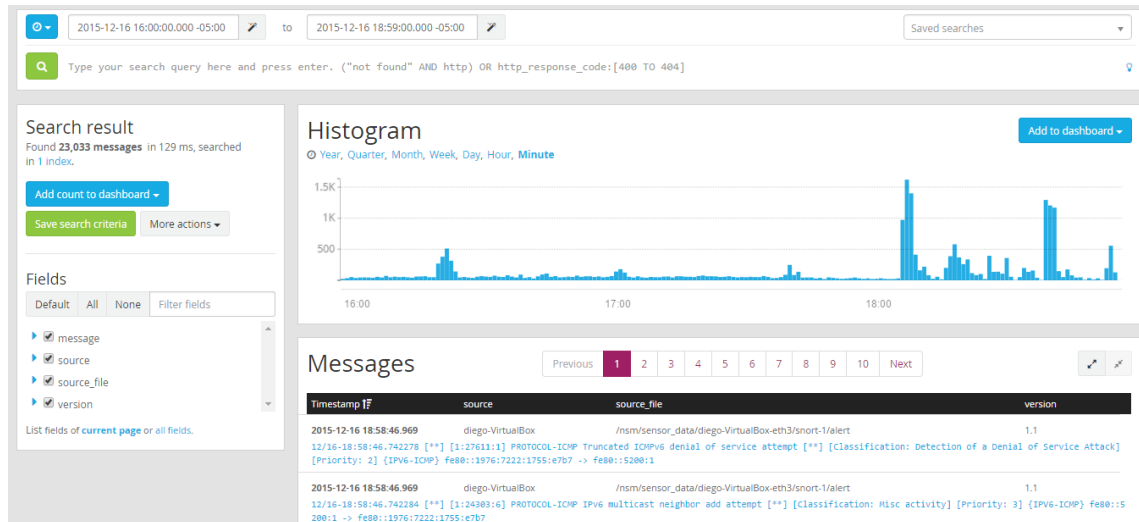
Durante el tercer intervalo de tiempo comprendido entre las 13:00 y 15:59 horas, se obtuvieron los resultados mostrados en la **Figura 72-4**



**Figura 72-4** Alertas IPv6 obtenidas en el intervalo de 13:00 a 15:59 con el Prototipo II  
Realizado por: Caiza Diego, 2016

#### 4.1.2.2.4. Intervalo 4

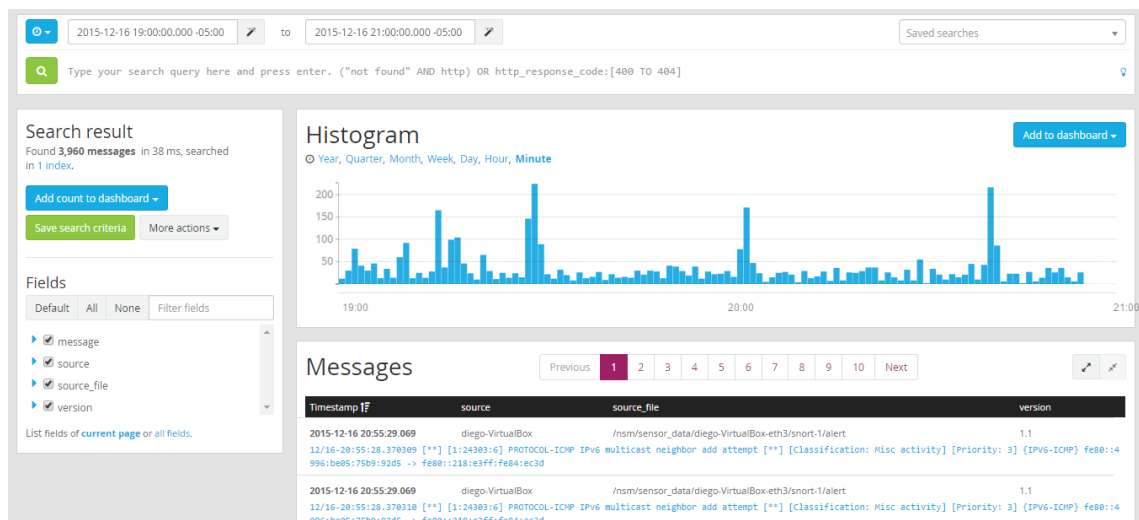
Durante el cuarto intervalo de tiempo comprendido entre las 16:00 y 18:59 horas, se obtuvieron los resultados mostrados en la **Figura 73-4**



**Figura 73-4** Alertas IPv6 obtenidas en el intervalo de 16:00 a 18:59 con el Prototipo II  
Realizado por: Caiza Diego, 2016

#### 4.1.2.2.5. Intervalo 5

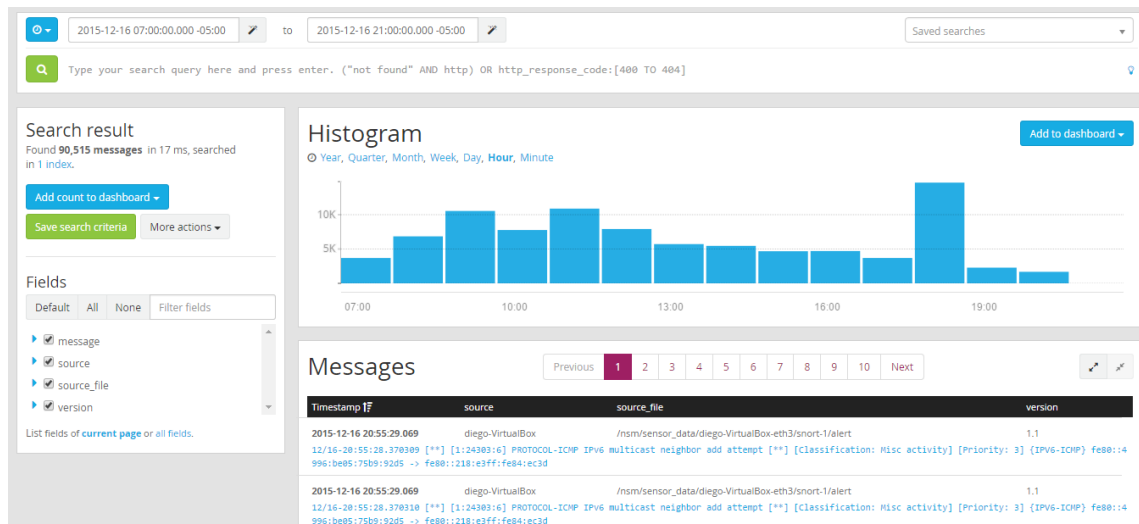
Durante el quinto intervalo de tiempo comprendido entre las 19:00 y 21:00 horas, se obtuvieron los resultados mostrados en la **Figura 74-4**



**Figura 74-4** Alertas IPv6 obtenidas en el intervalo de 19:00 a 21:00 con el Prototipo II  
Realizado por: Caiza Diego, 2016

#### 4.1.2.2.6. Resumen de resultados

Las alertas producidas durante el periodo total de tiempo comprendido desde las 07:00 a 21:00 horas utilizando el Prototipo II, se pueden apreciar en la **Figura 75-4**



**Figura 75-4** Alertas IPv6 obtenidas en el intervalo de 07:00 a 21:00 con el Prototipo II  
Fuente: Caiza Diego, 2016

Los resultados obtenidos por este indicador una vez que se concluyó el experimento 4 se detallan en la **Tabla 3-4**, es necesario señalar que por cada alerta falsa se cuantifico al indicador con un valor equivalente a 1, por el contrario por cada ataque verdadero realizado a manera de control se aplica un valor igual a 0.

**Tabla 9-4** Resumen de resultados del indicador No. Alertas Falsas Positivas del Prototipo II

Intervalos de tiempo	Categorización del ataque de control	Hora de ataque	No. Falsos Positivos
07:00 – 09:59	Ataque de reconocimiento	09:35	20873
10:00 – 12:59	Ataque de MITM	10:30	26432
13:00 – 15:59	Ataque de MITM	15:30	15811
16:00 – 18:59	Ataque DDos	18:35	13819
19:00 – 21:00	Ataque DDos	20:30	3960
<b>Total</b>			<b>80895</b>

Realizado por: Caiza Diego, 2016

Los resultados finales se detallan en la **Tabla 10-4**

**Tabla 10-4** Resultados finales del indicador No. Alertas Falsas Positivas del Prototipo II

Indicador	Prototipo II
No. alertas falsas positivas	80895

Realizado por: Caiza Diego, 2016

Los resultados obtenidos concluido el experimento 4 muestran la capacidad del Prototipo II para no generar alertas falsas durante el monitoreo de la VLAN de Estudiantes en la FIE. Del período comprendido desde las 07:00 hasta las 21:00 de un día normal de actividades (día anterior al del experimento 3) se detectaron 80895 alertas negativas, generando un problema de ineficiencia del prototipo debido a que está generando alarmas ante ataques inexistentes.

#### 4.1.2.3. Gestión de logs IPv6

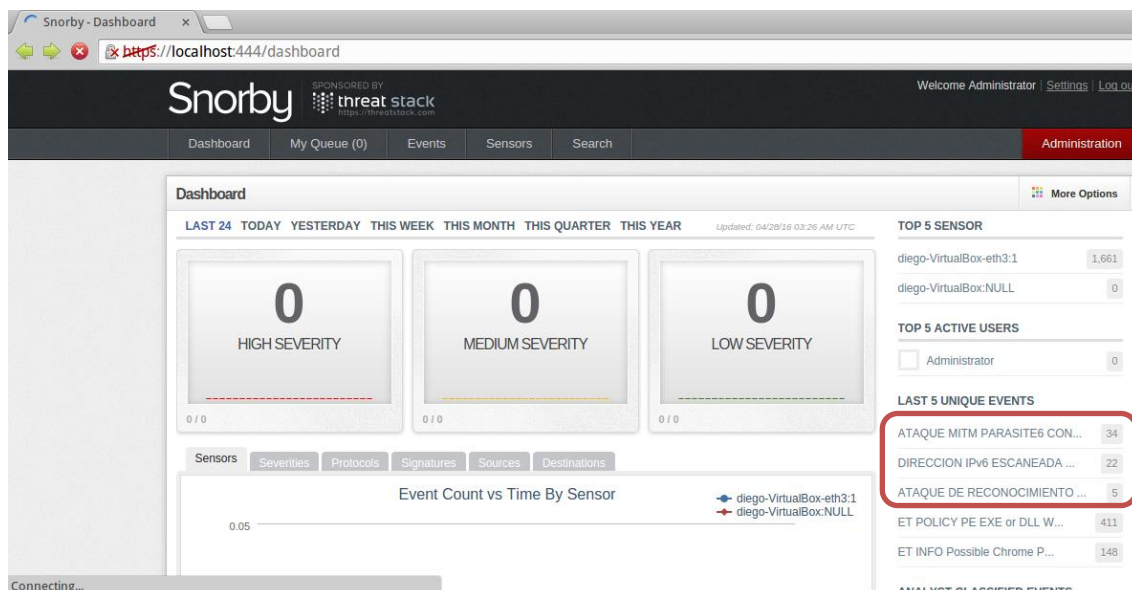
Luego de realizar los experimentos de detección de número de alertas positivas y número de alertas falsas positivas, se registraron los datos estadísticos de los logs IPv6.

En la **Figura 76-4** se muestra los resultados de la recolección de los logs IPv6 por el gestor Sguil de Security Onion.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	diego-VirtualBox-eth3-1	1.989	2015-12-16 15:58:40	0.0.0.0		0.0.0.0		0	ET POLICY Python-urllib/ Suspicious User Agent
RT	2	diego-VirtualBox-eth3-1	1.1140	2015-12-16 17:19:42	0.0.0.0		0.0.0.0		0	ET CHAT Google IM traffic Jabber client sign-on
RT	1	diego-VirtualBox-eth3-1	1.1171	2015-12-16 17:33:48	0.0.0.0		0.0.0.0		0	GPL CHAT Google Talk Logon
RT	1	diego-VirtualBox-eth3-1	1.1173	2015-12-16 17:33:48	0.0.0.0		0.0.0.0		0	ET CHAT Google Talk (Jabber) Client Login
RT	47	diego-VirtualBox-eth3-1	1.1180	2015-12-16 17:36:54	0.0.0.0		0.0.0.0		0	ET POLICY GNU/Linux APT User-Agent Outbound likely related to pack...
RT	50	diego-VirtualBox-eth3-1	1.1354	2015-12-16 19:59:57	0.0.0.0		0.0.0.0		0	ET INFO PDF Using CCITTFax Filter
RT	1	diego-VirtualBox-eth3-1	1.1447	2015-12-16 20:50:48	0.0.0.0		0.0.0.0		0	ET P2P ThunderNetwork UDP Traffic
RT	5	diego-VirtualBox-eth3-1	1.1601	2015-12-17 14:30:14	0.0.0.0		0.0.0.0		0	ATAQUE DE RECONOCIMIENTO IPv6 CON THCIIP6 TOOLKIT
RT	22	diego-VirtualBox-eth3-1	1.1606	2015-12-17 14:30:14	0.0.0.0		0.0.0.0		0	DIRECCION IPv6 ESCANEADA CON THCIIP6 TOOLKIT
RT	34	diego-VirtualBox-eth3-1	1.1628	2015-12-17 15:30:43	0.0.0.0		0.0.0.0		0	ATAQUE MITM PARASITE6 CON THCIIP6 TOOLKIT

**Figura 76-4** Sguil gestor interno de Security Onion no compatible para IPv6  
Realizado por: Caiza Diego, 2016

En la **Figura 77-4** se muestra los resultados de la recolección de los logs IPv6 por el gestor Snorby de Security Onion.



**Figura 77-4** Snorby gestor interno de Security Onion no compatible para IPv6  
**Realizado por:** Caiza Diego, 2016

Los resultados obtenidos por este indicador una vez que se concluyó el experimento 4 se detallan en la **Tabla 11-4**, es necesario señalar que se cuantifico al indicador con un valor equivalente a 1 si se cumplió con el objetivo de gestionar los logs IPv6 de los ataques detectados, por el contrario se aplicó un valor igual a 0 sino se cumple esta premisa.

**Tabla 11-4** Resumen de resultados indicador Gestión de logs IPv6 del Prototipo II

Indicador	Prototipo II
Replicación de logs IPv6	NO

**Fuente:** Caiza Diego, 2016

Los resultados obtenidos demuestran que el Prototipo II no permite la presentación y mucho menos la gestión de las alertas o logs IPv6 generados, lo cual limita claramente el uso del prototipo.

#### 4.1.2.4. Replicación de logs IPv6

La replicación de logs tiene el objetivo de almacenar en tiempo real los logs IPv6 generados. En la **Figura 78-4** se muestra el archivo que contienen estos registros almacenados en la distribución Security Onion bajo la ruta `/nsm/sensor_data/diego-VirtualBox-eth3/snort-1`.

```

alert.1450395264
File Edit Search Options Help
12/17-09:40:11.473935 [**] [1:10000010:3] DIRECCION IPv6 ESCANEADA CON THCIpV6 TOOLKIT [**] [Classification: Detection of a Network Sc
12/17-09:40:11.475666 [**] [1:10000010:3] DIRECCION IPv6 ESCANEADA CON THCIpV6 TOOLKIT [**] [Classification: Detection of a Network Sc
12/17-09:40:11.475668 [**] [1:10000010:3] DIRECCION IPv6 ESCANEADA CON THCIpV6 TOOLKIT [**] [Classification: Detection of a Network Sc
12/17-10:30:33.683774 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:30:33.683777 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:22.531328 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:22.531341 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:36.302320 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:36.302322 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:43.607430 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:31:43.607432 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:06.426973 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:06.426974 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:09.354647 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:32:09.354651 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:33:31.057838 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:33:31.057839 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:35:26.713895 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-10:35:26.713897 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy
12/17-15:30:13.779100 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:13.779102 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:13.779103 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:13.779104 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.775702 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.775708 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776452 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776456 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776457 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi
12/17-15:30:18.776459 [**] [1:10000033:2] ATAQUE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Vi

```

**Figura 78-4** Archivo de logs IPv6 alojado en Security Onion

Realizado por: Caiza Diego, 2016

El Prototipo II solo almacena los logs IPv6 en la distribución Security Onion debido a que su estructura no está acoplada al módulo del servidor Graylog. El resumen final se detalla en la **Tabla 12-4**

**Tabla 12-4** Resumen de resultados del indicador Replicación de logs IPv6

Indicador	Prototipo II
Replicación de logs IPv6	NO

Realizado por: Caiza Diego, 2016

## 4.2. Análisis y comparación de resultados

Luego de realizar los experimentos estipulados con los Prototipos desarrollados, se procede a realizar el análisis y comparación de los resultados obtenidos en cada uno de ellos:

### 4.2.1. No. Alertas positivas verdaderas (ataques detectados)

Se comparan los resultados obtenidos con el Prototipo I y con el Prototipo II, los cuales se muestran en la **Tabla 13-4**

**Tabla 13-4** Resultados del indicador No. Alertas Positivas

Pruebas Ejecutadas	Prototipo I	Prototipo II
Prueba 1	1	0
Prueba 2	1	0



Prueba 3	1	0
Prueba 4	1	0
Prueba 5	1	0
Prueba 6	1	0
Prueba 7	1	0
Prueba 8	1	0
Prueba 9	1	0
Prueba 10	1	0
Prueba 11	1	0
Prueba 12	0	0
Prueba 13	1	0
Prueba 14	1	1
Prueba 15	1	1
Prueba 16	1	1
Prueba 17	1	1
Prueba 18	1	0
Prueba 19	1	0
Prueba 20	1	0
Prueba 21	1	0
Prueba 22	1	0
Prueba 23	1	0
Prueba 24	1	0
Prueba 25	1	0
<b>Total</b>	<b>24</b>	<b>4</b>

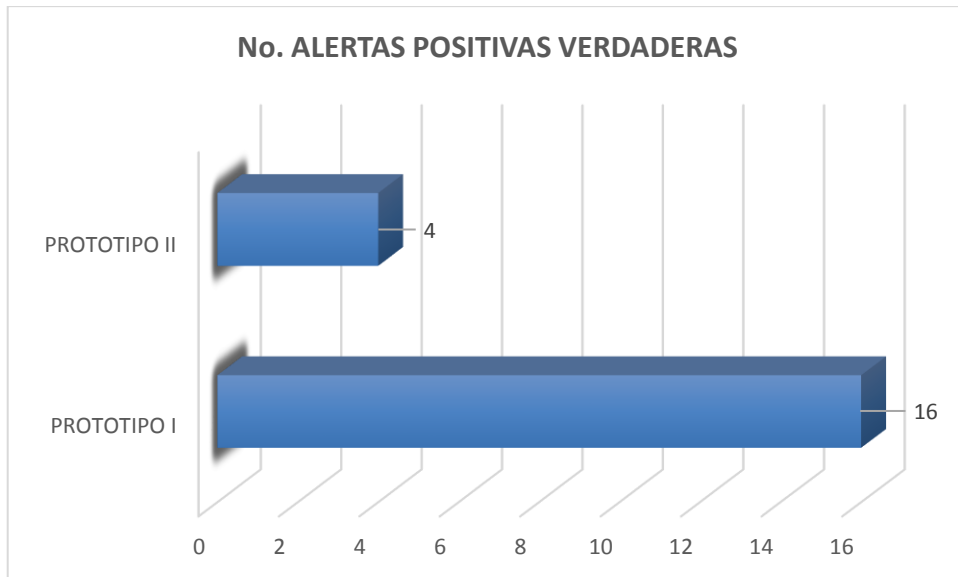
Realizado por: Caiza Diego, 2016

Los resultados finales obtenidos por este indicador una vez que se concluyó el experimento 1 y 2 se detallan en la **Tabla 14-4** y se observan en el **Gráfico 1-4**

**Tabla 14-4** Resultados del indicador No. Alertas Positivas del Prototipo I y II

<b>Indicador</b>	<b>Prototipo I</b>	<b>Prototipo II</b>
No. alertas positivas	24	4

Realizado por: Caiza Diego, 2016



**Gráfico 1-4** Comparación del indicador Número de Alertas Positivas  
Realizado por: Caiza Diego, 2016

De acuerdo a los resultados obtenidos al monitorear el tráfico de la red se determina que el Prototipo I detecta un número mayor de ataques IPv6 en contraste de los resultados obtenidos al monitorear el tráfico de red con el Prototipo II.

#### **4.2.2. No. Alertas falsas positivas**

Se comparan los resultados obtenidos con el Prototipo I y con el Prototipo II, los cuales se muestran en la **Tabla 15-4**

**Tabla 15-4** Resultados del indicador No. Falsos Positivos

Intervalos de tiempo	Prototipo I	Prototipo II
1° Intervalo	0	20873
2° Intervalo	0	26432
3° Intervalo	0	15811
4° Intervalo	0	13819
5° Intervalo	0	3960
<b>Total</b>	<b>0</b>	<b>80895</b>

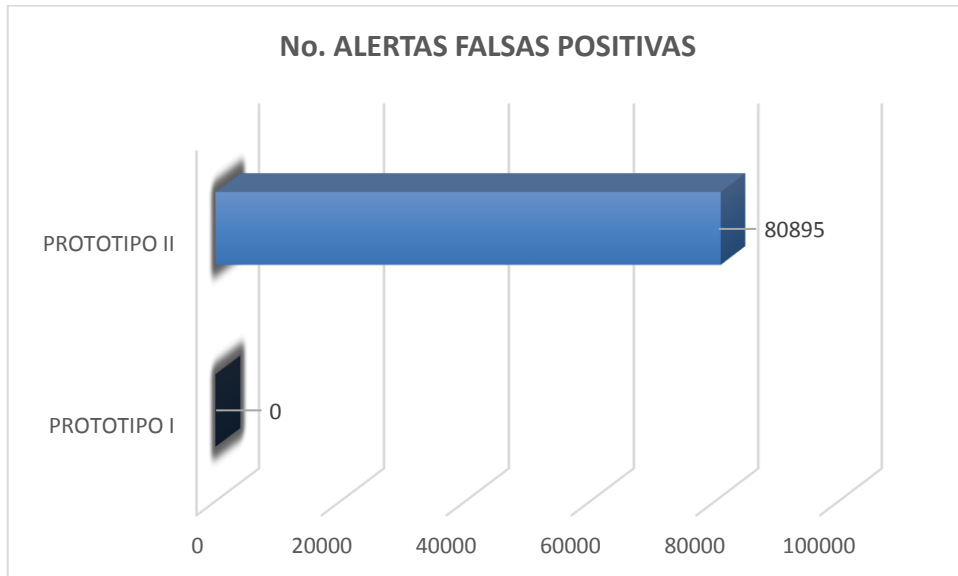
Realizado por: Caiza Diego, 2016

Los resultados finales obtenidos por este indicador una vez que se concluyó el experimento 3 y 4 se detallan en la **Tabla 16-4** y se observan en el **Gráfico 2-4**

**Tabla 16-4** Resultados del indicador No. Alertas Falsas Positivas del Prototipo I y II

Indicador	Prototipo I	Prototipo II
No. alertas falsas positivas	0	80895

Realizado por: Caiza Diego, 2016



**Gráfico 2-4** Comparación del indicador Número de Alertas Falsas Positivas  
Realizado por: Caiza Diego, 2016

De acuerdo a los resultados obtenidos al monitorear el tráfico de la red se determina que con el Prototipo I, el registro de alertas falsas es nulo en contraste de los resultados obtenidos al monitorear el tráfico de red con el Prototipo II.

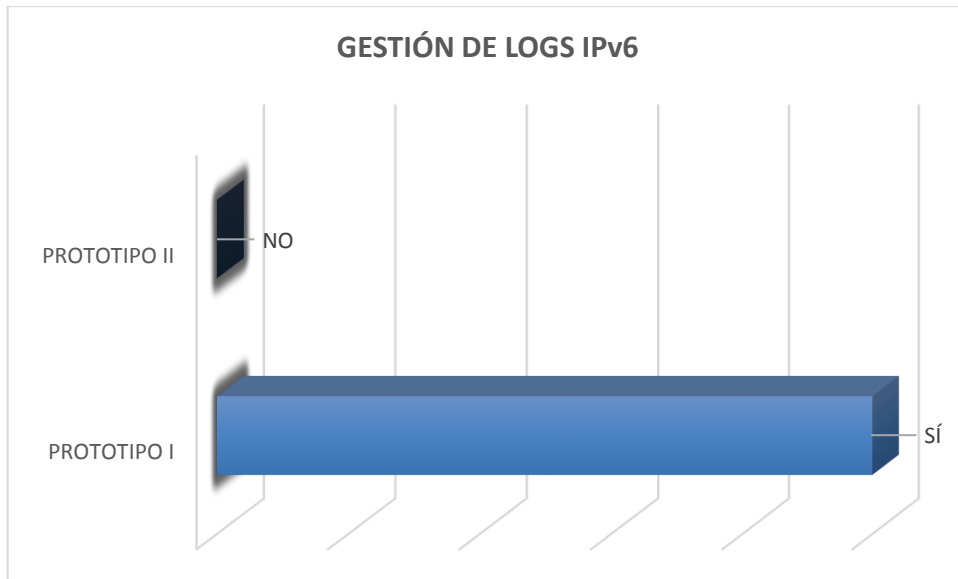
#### 4.2.3. Gestión de logs IPv6

Los resultados finales obtenidos por este indicador una vez que se concluyó el experimento 5 y 6 se detallan en la **Tabla 17-4** y se observan en el **Gráfico 3-4**

**Tabla 17-4** Resultados del indicador Gestión de logs IPv6 del Prototipo I y II

Indicador	Prototipo I	Prototipo II
Gestión de logs IPv6	SI	NO

Realizado por: Caiza Diego, 2016



**Gráfico 3-4** Comparación del indicador Gestión de logs IPv6  
Realizado por: Caiza Diego, 2016

De acuerdo a los resultados obtenidos al monitorear el tráfico de la red se determina que el Prototipo I si cumple con la premisa de gestionar los logs IPv6, a diferencia de los resultados obtenidos al monitorear el tráfico de red con el Prototipo II.

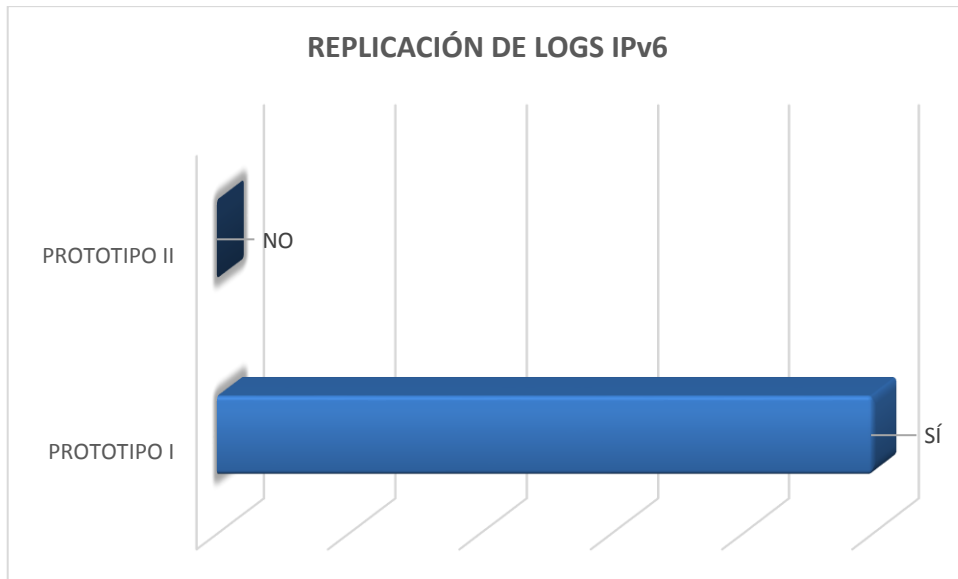
#### **4.2.4. Replicación de logs IPv6**

Los resultados finales obtenidos por este indicador una vez que se verificaron y compararon los ficheros de almacenamiento de logs del Prototipo I y Prototipo II se detallan en la **Tabla 18-4** y se observan en el **Gráfico 4-4**

**Tabla 18-4** Resultados del indicador Replicación de logs IPv6 del Prototipo I y II

<b>Indicador</b>	<b>Prototipo I</b>	<b>Prototipo II</b>
Gestión de logs IPv6	SI	NO

Realizado por: Caiza Diego, 2016



**Gráfico 4-4** Comparación del indicador Replicación de logs IPv6  
Realizado por: Caiza Diego, 2016

De acuerdo a los resultados obtenidos al monitorear el tráfico de la red se determina que el Prototipo I si cumple con el objetivo de replicar los logs IPv6 generados, a diferencia de los resultados obtenidos al monitorear el tráfico de red con el Prototipo II.

### 4.3. Prueba de hipótesis

#### 4.3.1. Ambiente de pruebas

Para la comprobación de la hipótesis se compara los resultados del Prototipo I y del Prototipo II, para los siguientes indicadores de la variable dependiente definida:

- Gestión de Logs IPv6
- No. Alertas Positivas Verdaderas
- No. Alertas Falsas Positivas
- Replicación de logs IPv6

#### 4.3.2. Escala de calificación

Para realizar la comparación de los resultados obtenidos se utilizará la escala de Likert para cada uno de los indicadores.

#### 4.3.2.1. *Indicador 1: No. Alertas positivas verdaderas*

Para medir el Indicador 1: No. Alertas positivas, se utilizará la escala mostrada en la **Tabla 19-4**

**Tabla 19-4** Tabla de escalas para el Indicador 1: No. Alertas positivas

<b>Número de detecciones</b>	<b>Valor</b>
>20	4
14-20	3
7-13	2
0-6	1

Realizado por: Caiza Diego, 2016

#### 4.3.2.2. *Indicador 2: No. Alertas falsas positivas*

Para medir el Indicador 2: No. Alertas Falsas Positivas, se utilizará la escala mostrada en la **Tabla 20-4**

**Tabla 20-4** Tabla de escalas para el Indicador 2: No. Alertas Falsas Positivas

<b>Número de alertas</b>	<b>Valor</b>
0-100	4
101-150	3
150-200	2
>200	1

Realizado por: Caiza Diego, 2016

#### 4.3.2.3. *Indicador 3: Gestión de logs IPv6*

Para medir el Indicador 3: Gestión de logs IPv6, se utilizará la escala mostrada en la **Tabla 21-4**

**Tabla 21-4** Tabla de escalas para el Indicador 3: Gestión de logs IPv6

<b>Gestión alertas</b>	<b>Valor</b>
SI	4
NO	1

Realizado por: Caiza Diego, 2016

#### 4.3.2.4. Indicador 4: Replicación de logs IPv6

Para medir el Indicador 4: Replicación de logs IPv6, se utilizará la escala mostrada en la **Tabla 22-4**

**Tabla 22-4** Tabla de escalas para el Indicador 4: Replicación de logs IPv6

Replicación de logs IPv6	Valor
SI	4
NO	1

Realizado por: Caiza Diego, 2016

#### 4.3.3. Ponderación de los indicadores

Los resultados obtenidos en las pruebas para cada Indicador en el punto 4.3.1 son cuantificados con las escalas definidas en el punto 4.3.2.

##### 4.3.3.1. Indicador 1: No. Alertas positivas verdaderas

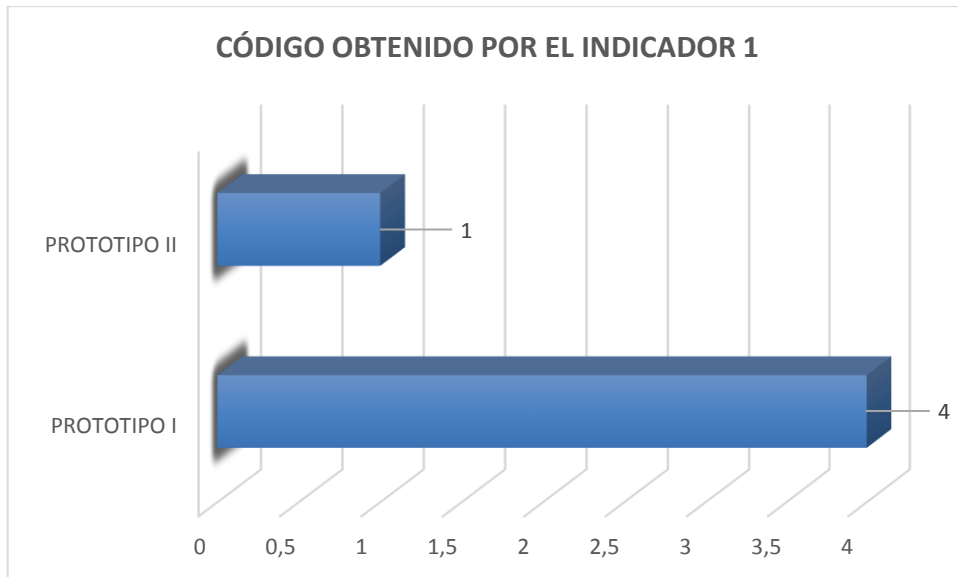
Utilizando los valores promedios del Indicador 1: No. Alertas positivas, con cada Prototipo se cuantifica los resultados de acuerdo a la escala definida, con lo que se obtiene los valores mostrados en la **Tabla 23-4**

**Tabla 23-4** Códigos del Indicador 1: No. Alertas positivas

No.	Indicador	Valor promedio		Código obtenido (de acuerdo a la escala)	
		Prototipo I	Prototipo II	Prototipo I	Prototipo II
1	No. Alertas positivas	24	4	4	1

Realizado por: Caiza Diego, 2016

En el **Gráfico 5-4** se muestran los códigos obtenidos (de acuerdo a la escala) del Indicador.



**Gráfico 5-4** Resultados obtenidos (de acuerdo a la escala) del Indicador 1:  
No. Alertas Positivas Verdaderas  
Realizado por: Caiza Diego, 2016

#### 4.3.3.2. Indicador 2: No. Alertas falsas positivas

Utilizando los valores promedios del Indicador 2: No. Alertas Falsas Positivas, con cada Prototipo se cuantifica los resultados de acuerdo a la escala definida, con lo que se obtiene los valores mostrados en la **Tabla 24-4**

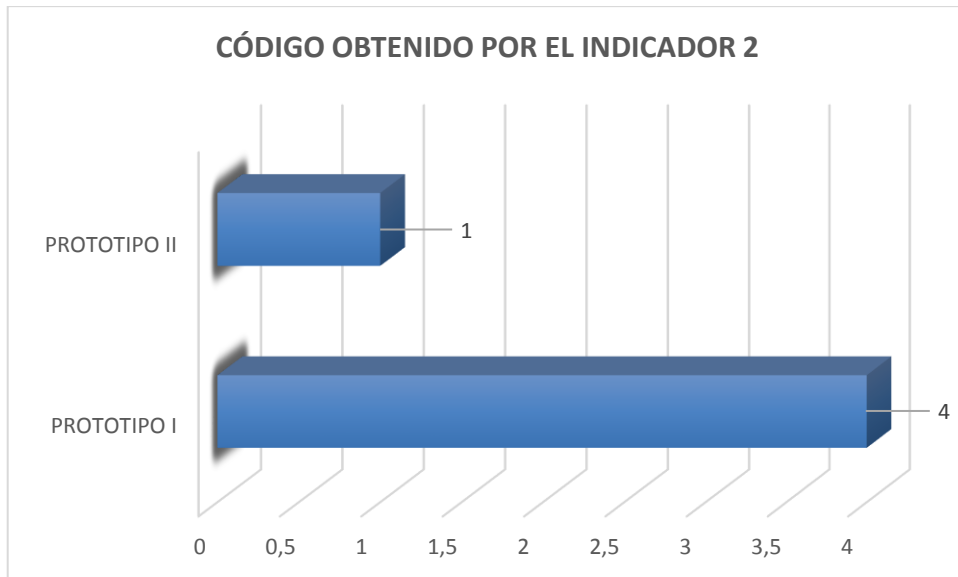
**Tabla 24-4** Códigos del Indicador 2: No. Alertas Falsas Positivas

No.	Indicador	Valor promedio		Código obtenido (de acuerdo a la escala)	
		Prototipo I	Prototipo II	Prototipo I	Prototipo II
2	No. Falsos Positivos	0	80895	4	1

Realizado por: Caiza Diego, 2016

En el **Gráfico 6-4** se muestran los códigos obtenidos (de acuerdo a la escala) del Indicador.





**Gráfico 6-4** Resultados obtenidos (de acuerdo a la escala) del Indicador 2:  
No. Alertas Falsas Positivas  
Realizado por: Caiza Diego, 2016

#### 4.3.3.3. Indicador 3: Gestión de logs IPv6

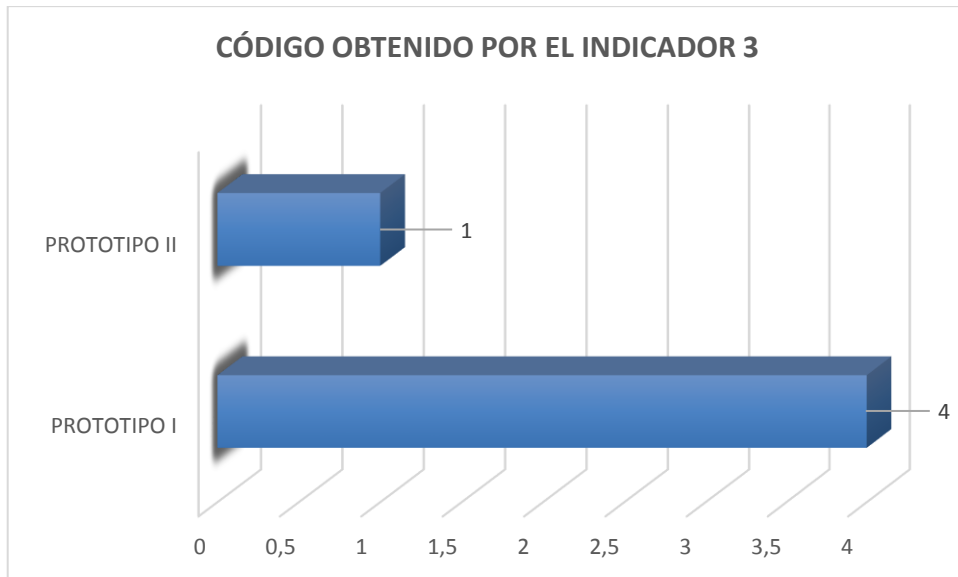
Utilizando los valores promedios del Indicador 3: Gestión de logs IPv6, con cada Prototipo se cuantifica los resultados de acuerdo a la escala definida, con lo que se obtiene los valores mostrados en la **Tabla 25-4**

**Tabla 25-4** Códigos del Indicador 3: Gestión de logs IPv6

No.	Indicador	Valor promedio		Código obtenido (de acuerdo a la escala)	
		Prototipo I	Prototipo II	Prototipo I	Prototipo II
		3	Gestión de logs IPv6	SI	NO

Realizado por: Caiza Diego, 2016

En la **¡Error! No se encuentra el origen de la referencia.-4** se muestran los códigos obtenidos (de acuerdo a la escala) del Indicador.



**Gráfico 7-4** Resultados obtenidos (de acuerdo a la escala) del Indicador 3: Gestión de logs IPv6

Realizado por: Caiza Diego, 2016

#### 4.3.3.4. Indicador 4: Replicación de logs IPv6

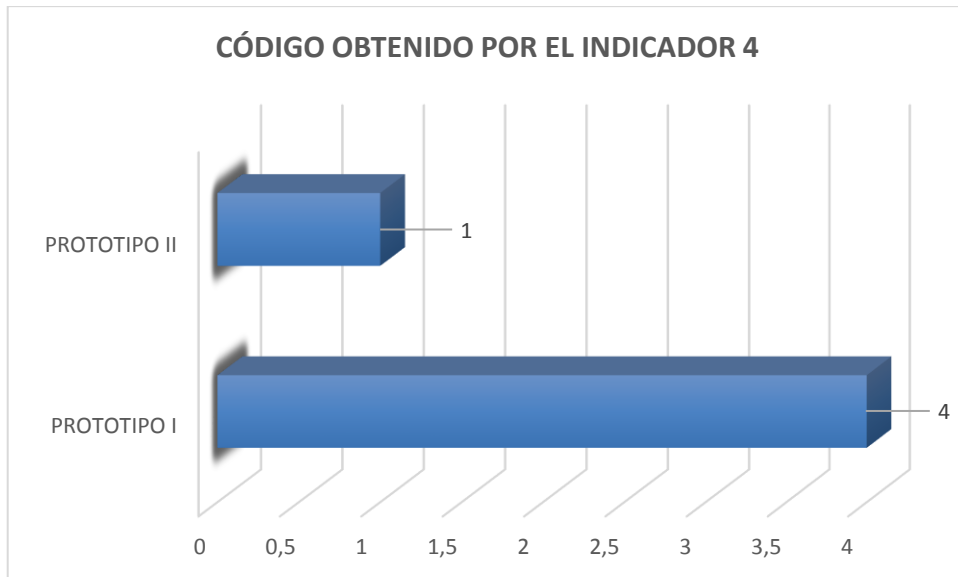
Utilizando los valores promedios del Indicador 4: Replicación de logs IPv6, con cada Prototipo se cuantifica los resultados de acuerdo a la escala definida, con lo que se obtiene los valores mostrados en la **Tabla 26-4**

**Tabla 26-4** Códigos del Indicador 4: Replicación de logs IPv6

No.	Indicador	Valor promedio		Código obtenido (de acuerdo a la escala)	
		Prototipo I	Prototipo II	Prototipo I	Prototipo II
4	Replicación de Logs IPv6	SI	NO	4	1

Realizado por: Caiza Diego, 2016

En el **Gráfico 8-4** se muestran los códigos obtenidos (de acuerdo a la escala) del Indicador.



**Gráfico 8-4** Resultados obtenidos (de acuerdo a la escala) del Indicador 4: Copia de seguridad de logs IPv6

Realizado por: Caiza Diego, 2016

#### 4.3.4. Comprobación de la hipótesis

La hipótesis definida en la presente investigación es **“La implementación de un Prototipo como sistema detector de intrusos con soporte del protocolo IPv6 desarrollado con herramientas open source servirá para mejorar el nivel de seguridad dentro de la red local”**.

Para la demostración de la hipótesis se utilizará la estadística descriptiva y la estadística inferencial.

##### 4.3.4.1. Estadística descriptiva

Para la comprobación de la hipótesis se utilizará la estadística descriptiva como punto de partida de la investigación en la que se cuantifican los resultados obtenidos en las pruebas realizadas de cada uno de los indicadores definidos utilizando la escala de Likert, como se muestra en la **Tabla 27-4**

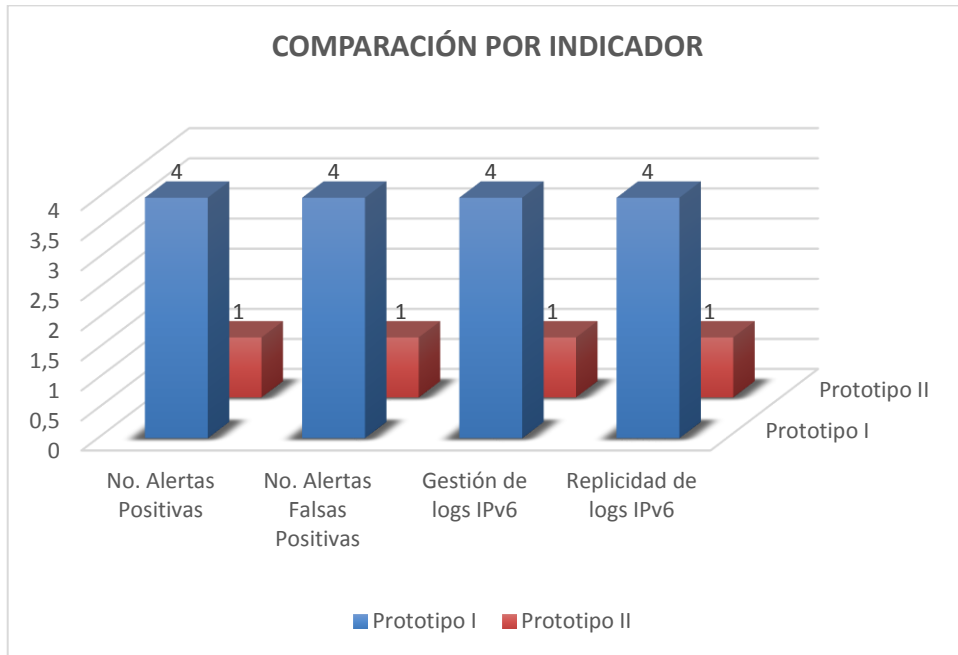
**Tabla 27-4** Resultados de indicadores

No.	Indicadores	Prototipo I	Prototipo II
1	No. Alertas Positivas	4	1
2	No. Alertas Falsas Positivas	4	1
3	Gestión de logs IPv6	4	1

<b>4</b>	Replicación de logs IPv6	<b>4</b>	<b>1</b>
<b>TOTAL</b>		<b>16</b>	<b>4</b>

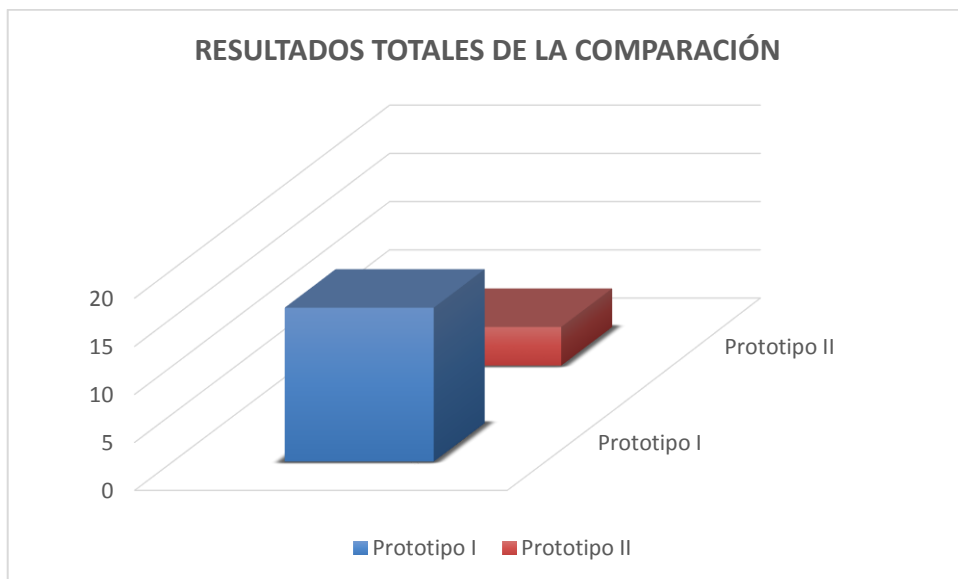
Realizado por: Caiza Diego, 2016

En el **Gráfico 9-4** se muestran los resultados de la comparación realizada por cada uno de los indicadores.



**Gráfico 9-4** Resultados de la comparación por Indicador  
Realizado por: Caiza Diego, 2016

En el **Gráfico 10-4** se muestran los resultados totales de la comparación realizada por cada Prototipo.



**Gráfico 10-4** Resultados totales de la comparación  
Fuente: Caiza Diego, 2016

Se concluye que la implementación del Prototipo I como “**Sistema detector de intrusos con soporte del protocolo IPv6 desarrollado con herramientas open source**” mejora un 300% el nivel de seguridad de la red local, en comparación con el Prototipo II.

#### 4.3.4.2. *Estadística inferencial*

Para la comprobación de la hipótesis de investigación con la estadística inferencial se inicia proporcionando valores a la variable independiente  $X$ :

$X =$  Seguridad en la red local

$X_1 =$  Mejora el nivel de Seguridad en la red local

$X_2 =$  No mejora el nivel la Seguridad en la red local

Una aplicación importante de la distribución Chi cuadrado es el empleo de datos muestrales para probar la independencia de dos variables

Para la prueba de hipótesis planteada se utilizó la prueba de Chi cuadrado o  $X^2$ , que es una prueba no paramétrica a través de la cual se mide la relación entre la variable dependiente e independiente.

Además, se considera la hipótesis nula  $H_0$  y la hipótesis de investigación  $H_i$ .

- **$H_i$ : La implementación de un Prototipo como sistema detector de intrusos con soporte del protocolo IPv6 desarrollado con herramientas open source servirá para mejorar el nivel de seguridad dentro de la red local.**
- **$H_0$ : La implementación de un Prototipo como sistema detector de intrusos con soporte del protocolo IPv6 desarrollado con herramientas open source NO servirá para mejorar el nivel de seguridad dentro de la red local.**

La tabla de contingencia creada para el cálculo de Chi cuadrado, se muestra en la **Tabla 28-4**, en la que se ubican las frecuencias observadas de cada Indicador.

**Tabla 28-4** Tabla de contingencia de frecuencias observadas

V. Independiente \ V. Dependiente	Indicadores	Prototipo I	Prototipo II	Total
<b>Mejora el nivel seguridad</b>	No. Alertas Positivas	4	0	4
	No. Alertas Falsas Positivas	4	0	4
	Gestión de logs IPv6	4	0	4
	Replicación de logs IPv6	4	0	4
<b>No mejora el nivel seguridad</b>	No. Alertas Positivas	0	1	1
	No. Alertas Falsas Positivas	0	1	1
	Gestión de logs IPv6	0	1	1
	Replicación de logs IPv6	0	1	1
<b>TOTAL</b>		<b>16</b>	<b>4</b>	<b>20</b>

Realizado por: Caiza Diego, 2016

La tabla de contingencia de frecuencias esperadas son los valores que se esperaría encontrar si las variables no estuvieran relacionadas. Chi cuadrado parte del supuesto de “no relación entre las variables” y se evaluará si es cierto o no, analizando si sus frecuencias observadas son diferentes de lo que pudiera esperarse en caso de ausencia de correlación.

La frecuencia esperada de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas.

$$f_e = \frac{(total\_fila) * (total\_columna)}{N}$$

**Donde:**

*N*: Número total de frecuencias observadas.

Aplicando la fórmula a los valores de la Tabla se obtiene la tabla de contingencia de valores esperados, como se muestra en la **Tabla 29-4**

**Tabla 29-4** Tabla de contingencia de frecuencias esperadas

V. Dependiente \ V. Independiente	Indicadores	Prototipo I	Prototipo II	Total
<b>Mejora el nivel seguridad</b>	No. Alertas Positivas	3,20	0,80	4
	No. Alertas Falsas Positivas	3,20	0,80	4

	Gestión de logs IPv6	3,20	0,80	<b>4</b>
	Replicación de logs IPv6	3,20	0,80	<b>4</b>
<b>No mejora el nivel seguridad</b>	No. Alertas Positivas	0,80	0,20	<b>1</b>
	No. Alertas Falsas Positivas	0,80	0,20	<b>1</b>
	Gestión de logs IPv6	0,80	0,20	<b>1</b>
	Replicación de logs IPv6	0,80	0,20	<b>1</b>
<b>TOTAL</b>		<b>16</b>	<b>4</b>	<b>20</b>

Realizado por: Caiza Diego, 2016

Una vez obtenida la tabla de frecuencias esperadas, se aplica la siguiente fórmula de Chi cuadrado.

$$x^2 = \sum \frac{(o - E)^2}{E}$$

Donde:

**O**: Frecuencia observada en cada celda

**E**: Frecuencia esperada en cada celda

En la **Tabla 30-4** se calcula el valor de  $X^2$

**Tabla 30-4** Cálculo de  $X^2$

	<b>Indicadores</b>	<b>O</b>	<b>E</b>	<b>O - E</b>	<b>(O - E)<sup>2</sup></b>	<b><math>\frac{(O - E)^2}{E}</math></b>
<b>Prototipo I</b>	Mejora/ No. Alertas Positivas por el Prototipo I	4	3,2	0,80	0,64	0,20
	Mejora/No. Alertas Falsas Positivas por el Prototipo I	4	3,2	0,80	0,64	0,20
	Mejora/Gestión de logs IPv6 por el Prototipo I	4	3,2	0,80	0,64	0,20
	Mejora/Replicación de logs IPv6 por el Prototipo I	4	3,2	0,80	0,64	0,20
<b>Prototipo II</b>	Mejora/ No. Alertas Positivas por el Prototipo II	0	0,8	-0,80	0,64	0,80
	Mejora/No. Alertas Falsas Positivas por el Prototipo II	0	0,8	-0,80	0,64	0,80
	Mejora/Gestión de logs IPv6 por el Prototipo II	0	0,8	-0,80	0,64	0,80
	Mejora/Replicación de logs IPv6 por el Prototipo II	0	0,8	-0,80	0,64	0,80
<b>Prototipo I</b>	No Mejora/ No. Alertas Positivas por el Prototipo I	0	0,8	-0,80	0,64	0,80
	No Mejora/No. Alertas Falsas Positivas por el Prototipo I	0	0,8	-0,80	0,64	0,80
	No Mejora/Gestión de logs IPv6 por el Prototipo I	0	0,8	-0,80	0,64	0,80
	No Mejora/Replicación de logs IPv6 por el Prototipo I	0	0,8	-0,80	0,64	0,80

<b>Prototipo II</b>	No Mejora/ No. Alertas Positivas por el Prototipo II	1	0,2	0,80	0,64	3,20	
	No Mejora/No. Alertas Falsas Positivas por el Prototipo II	1	0,2	0,80	0,64	3,20	
	No Mejora/Gestión de logs IPv6 por el Prototipo II	1	0,2	0,80	0,64	3,20	
	No Mejora/Replicación de logs IPv6 por el Prototipo II	1	0,2	0,80	0,64	3,20	
	$X^2$						<b>20,00</b>

Realizado por: Caiza Diego, 2016

## Interpretación

Para determinar si el valor de  $X^2$  es o no significativo, se debe determinar los grados de libertad mediante la siguiente fórmula.

$$GI = (f - 1)(c - 1)$$

**Donde:**

*f*: Número de filas de la tabla de contingencia

*c*: Número de columnas de la tabla de contingencia

Por lo tanto:

$$GI = (8 - 1)(2 - 1) = 7$$

De acuerdo la tabla de distribución  $X^2$  que se muestra en la **Tabla 31-4** y eligiendo como nivel de significancia de  $\alpha = 1\% = 0.01$  para obtener un nivel de confianza del 99%, se obtiene como punto crítico de  $X^2$  para 7 grados de libertad  $X^2_{critico} = 18.4753$ .



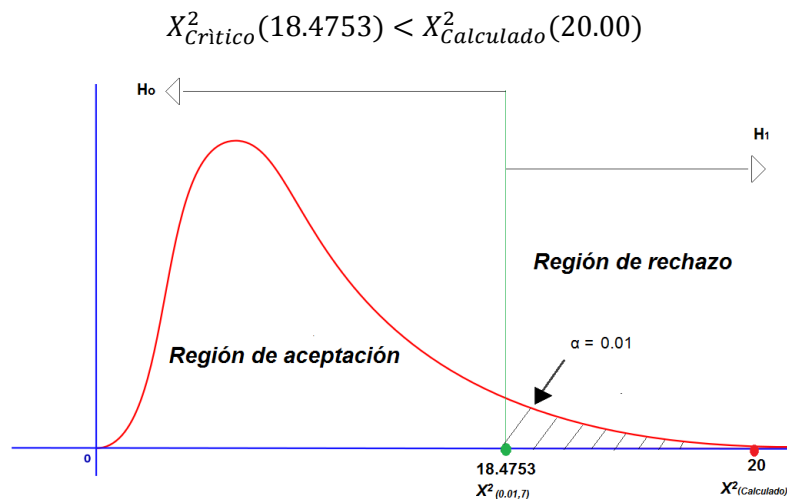
**Tabla 31-4** Tabla de distribución de  $\chi^2$

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, v = Grados de Libertad

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Fuente: [http://labrad.fisica.edu.uy/docs/tabla\\_chi\\_cuadrado.pdf](http://labrad.fisica.edu.uy/docs/tabla_chi_cuadrado.pdf)

El valor  $\chi^2$  calculado  $\chi^2_{Calculado}$  en esta investigación es de 20.00 que es superior al valor de la tabla de distribución de 18.4753, como se muestra en el **Gráfico 11-4**



Fuente: Caiza Diego, 2016

Por lo que el valor calculado de  $\chi^2$  se encuentra en el sector de rechazo de la hipótesis nula  $H_0$ , y se acepta la hipótesis de investigación que es significativa, con un nivel de significancia de  $\alpha = 1\% = 0.01$  para obtener un nivel de confianza del 99%.

## CONCLUSIONES

- Se analizó el soporte IPv6 que prestan los tres principales sistemas detectores de intrusos open source para mostrar actividad anormal en la red local y se prefirió optar por Snort como el motor detector más adecuado debido a las características de: arquitectura, fiabilidad y constante actualización que brinda su software.
- Durante el transcurso de la investigación se utilizó la distribución Linux Security Onion basada en Ubuntu por ser una distribución especializada en sistemas detectores de intrusos. Sus principales características son su colección interna de herramientas de seguridad (incluidos Snort, Suricata y Bro) y su colección de gestores de registros (Sguil, Squert, ELSA, Xplico, pero ninguno cuenta con soporte de direccionamiento IPv6).
- Se acopló el servidor de logs open source Graylog, debido a la falta de soporte de los gestores internos de Security Onion. El cual permite la recepción de los denominados colectores distribuidos en la red local, además almacena los logs en su base de datos interna, gestiona los registros y permite el análisis en un solo sistema centralizado.
- Se analizó tres tipos de herramientas especializadas en ejecutar pruebas de intrusiones sobre dominios locales (THCIPv6, SI6 Networks' IPv6 Toolkit, Evil Foca) y se escogió la suite THCIPv6 por ser la más completa dentro del mundo de la seguridad IPv6.
- Dentro de la investigación se identificó y clasificó en tres tipos de ataques: de reconocimiento, de denegación de servicio y de hombre en el medio. La ejecución de cualquiera de las herramientas de la suite THCIPv6 altera el comportamiento normal de una red y a la vez generan patrones de tráfico IPv6 anormales, definidos en la investigación como ataques IPv6.
- Se crearon nuevas reglas, específicas para detectar los patrones de tráfico IPv6 generados por la suite, como consecuencia de que las reglas que componen el paquete oficial de Snort no cumplieron con la premisa de identificar este tipo de tráfico.

- Se utilizó la herramienta Wireshark, la cual permitió efectuar en el momento de la ejecución de la suite THCIPv6 un análisis byte a byte de todos los paquetes de datos inyectados en la red, con el objetivo de distinguir los tipos de rastros y diseñar reglas personalizadas para la detección.
- El lenguaje propio que utiliza Snort para la creación de reglas es flexible y potente, evitando posteriores coincidencias de patrones negativos que generen falsas alarmas.
- Las reglas creadas en la investigación se basaron en la coincidencia de los parámetros de los mensajes de control ICMPv6 del tráfico detectado como anormal.
- Las pruebas se efectuaron en el mismo escenario que es la infraestructura de la red de la FIE (Facultad de Informática y Electrónica) de la ESPOCH, específicamente se trabajó con la VLAN de Estudiantes aprovechando el tráfico nativo bajo IPv6.
- Los resultados obtenidos durante las pruebas al monitorear el tráfico de la red determinan, que el Prototipo I detecta un número mayor de ataques, el registro de alertas falsas es nulo, además permite la gestión y análisis de los logs IPv6 y cumple con el objetivo de replicar en tiempo real los logs IPv6 generados, en contraste de los resultados obtenidos al monitorear el tráfico de red con el Prototipo II.
- El Prototipo I es adaptable a cualquier Red Lan que tenga soporte del protocolo IPv6, independientemente de la infraestructura que posea, con lo cual se cumple la premisa de escalabilidad.

## RECOMENDACIONES

- Se recomienda dar continuidad al análisis de patrones anormales de tráfico IPv6 con el objetivo de incrementar el número de alertas de detección.
- Durante la fase de implementación del sistema detector completo es importante sincronizar la zona horaria de los servidores, caso contrario existirán problemas con el envío de logs desde el colector hacia el servidor Graylog. Por lo que se sugiere se realice una sincronización manual de ser necesario.
- Se recomienda durante la fase de desarrollo de pruebas de denegación de servicios realizarlos en una hora apropiada para evitar problemas con las máquinas activas, debido a que genera un problema con los recursos del computador (si se trabaja con el sistema operativo Windows 7) y adicionalmente compromete la disponibilidad de la red.
- En un ambiente de producción se recomienda realizar un hardening tanto de Security Onion como de Graylog, es decir eliminar aplicaciones así como servicios innecesarios, asegurar usuarios, endurecer el sistema de acceso remoto, endurecer servicios, actualizar periódicamente, con el objetivo de reducir las vulnerabilidades de los sistemas.

## BIBLIOGRAFÍA

- ALLEN, J.** (2015). *A Performance Comparison of Intrusion Detection*. Obtenido de <https://www.sans.org/reading-room/whitepapers/detection/ipv6-open-source-ids-35957>
- ALONSO, C.** (2012). *El Lado Del Mal*. Obtenido de <http://www.elladodelmal.com/2012/10/hacking-en-redes-de-datos-ipv6.html>
- ALONSO, C.** (2012). *El Lado Del Mal*. Obtenido de <http://www.elladodelmal.com/2012/11/hacking-en-redes-de-datos-ipv6-neighbor.html>
- AMOL RAWAL, S. G.** (2014). *Study of IPv6 security Vulnerabilities*. (Technical Report: T.R. 2014-001). The Center for Convergence and Emerging Network Technologies, School of information Studies Syracuse University.
- CISCO.** (2016). *Snort*. Obtenido de <https://www.snort.org/>
- DEERING, S., & HINDEN, R.** (1998). *RFC 2460*. Obtenido de <https://www.ietf.org/rfc/rfc2460.txt>
- ELEVEN PATHS.** (2013). *Eleven Paths*. Obtenido de <http://blog.elevenpaths.com/2013/08/white-paperpractical-hacking-in-ipv6.html>
- ELEVENTH PATHS.** (2013). *Eleventh Paths*. Obtenido de <https://www.elevenpaths.com/es/labstools/evil-focasp/index.html>
- GONT, F.** (2012). *Si6 Networks*. Obtenido de <http://www.si6networks.com/tools/ipv6toolkit/index.html>
- GONT, F.** (2013). *Si6 Networks*. Obtenido de <http://www.es.hackingipv6networks.com/trainings/hacking-ipv6-networks>

- GONT, F.** (2014). *Techtarget*. Obtenido de <http://searchdatacenter.techtarget.com/es/cronica/Mitos-sobre-la-seguridad-en-IPv6-desmontando-falsas-ideas>
- GONZÁLEZ, E.** (2012). *Estudio IPv6*. Universitat Oberta de Catalunya, Catalunya, España.
- GRAYLOG INC.** (2016). *Graylog*. Obtenido de <https://www.graylog.org/>
- GU, L.** (2014). A Light-Weight Penetration Test Tool for IPv6 Threats. *Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 49-52). Taipei:IEEE
- JERONIMO, J.** (2016). *Blog de tecnología e ingeniería del software*. Obtenido de <http://javierjeronimo.es/2015/03/23/graylog-arquitectura-tolerante-a-fallos-y-escalable/>
- JIMENEZ, M.** (2012). *Hackplayers*. Obtenido de <http://www.hackplayers.com/2012/10/comprometiendo-ipv6.html>
- MARTINEZ, J.** (2012). *Consulintel*. Obtenido de: <http://www.consulintel.es/html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf>
- NETWORK INFORMATION CENTER MEXICO SC.** (2013). *IPv6MX*. Obtenido de <http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6>
- OISF.** (2015). *Suricata IDS*. Obtenido de <http://suricata-ids.org/>
- RODRIGUEZ, C.** (2013). *Ipv6nuevastecredes*. Obtenido de <https://ipv6nuevastecredes.wikispaces.com/wiki/members>
- SAAD, R., RAMADASS, S., & MANICKAM, S.** (2013). A study on detecting ICMPv6 flooding attack based on IDS. *Australian Journal of Basic and Applied Sciences*, (Vol. 7, Issue 2, pp. 175-181).

**SCHÜTTE, M.** (2013). Design and Implementation of an IPv6 Plugin for the Snort Intrusion Detection System. *Magdeburger Journal zur Sicherheitsforschung*, (Vol. 2, pp. 409-452).

**SECURITY ONION SOLUTIONS.** (2015). *Security Onion*. Obtenido de <https://security-onion-solutions.github.io/security-onion/>

**SECURITY ONION SOLUTIONS.** (2015). *Security Onion*. Obtenido de <https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion>

**SUMIT, K., & RAVREET, K.** (2013). IPv6 Network Security using Snort. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, (Vol. 2, No 8, pp. 17-22).

**THE HACKERS CHOICE .** (2015). *THC*. Obtenido de <https://www.thc.org/thc-ipv6/>

**UNIVERSIDAD DE ALMERÍA.** (2013). *Administración de sistemas operativos*. Obtenido de [http://www.adminso.es/index.php/Snort-CABECERA\\_DE\\_UNA\\_REGLA](http://www.adminso.es/index.php/Snort-CABECERA_DE_UNA_REGLA)

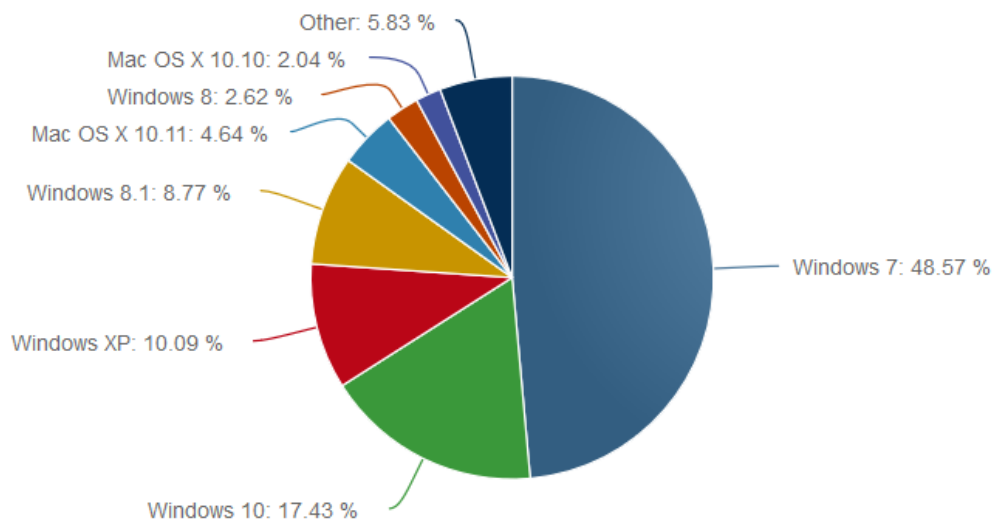
**VEATO, V.** (2014). *Redes Locales y Globales*. Obtenido de <https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/7-icmp-en-ipv6>

## ANEXOS

### Anexo A: Sistemas Operativos mas usados en el mercado actual

Netmarketshare (<https://www.netmarketshare.com>) es un portal que incluye datos sobre la distribución y el reparto del mercado de navegadores, sistemas operativos y buscadores en ordenadores personales, tabletas y teléfonos móviles. A partir de diferentes fuentes, el portal representa a casi todos los países del mundo y proporciona datos mensuales sobre el reparto de los mercados de navegadores, buscadores, pantallas y su resolución, principales ISPs y sistemas operativos.

#### Desktop Operating System Market Share Juny, 2016



OPERATING SYSTEM	TOTAL MARKET SHARE
<input checked="" type="checkbox"/> Windows 7	48.57%
<input checked="" type="checkbox"/> Windows 10	17.43%
<input checked="" type="checkbox"/> Windows XP	10.09%
<input checked="" type="checkbox"/> Windows 8.1	8.77%
<input checked="" type="checkbox"/> Mac OS X 10.11	4.64%
<input checked="" type="checkbox"/> Windows 8	2.62%
<input checked="" type="checkbox"/> Mac OS X 10.10	2.04%
<input checked="" type="checkbox"/> Linux	1.79%
<input checked="" type="checkbox"/> Windows Vista	1.35%
<input checked="" type="checkbox"/> Mac OS X 10.9	0.83%
<input checked="" type="checkbox"/> Windows NT	0.73%
<input checked="" type="checkbox"/> Mac OS X 10.7	0.35%
<input checked="" type="checkbox"/> Mac OS X 10.8	0.31%
<input checked="" type="checkbox"/> Mac OS X 10.6	0.30%
<input checked="" type="checkbox"/> Windows 3.1	0.10%
<input checked="" type="checkbox"/> Mac OS X 10.5	0.04%
<input checked="" type="checkbox"/> Windows 2000	0.02%
<input checked="" type="checkbox"/> Mac OS X 10.4	0.01%
<input checked="" type="checkbox"/> Mac OS X (no version reported)	0.00%
<input checked="" type="checkbox"/> FreeBSD	0.00%

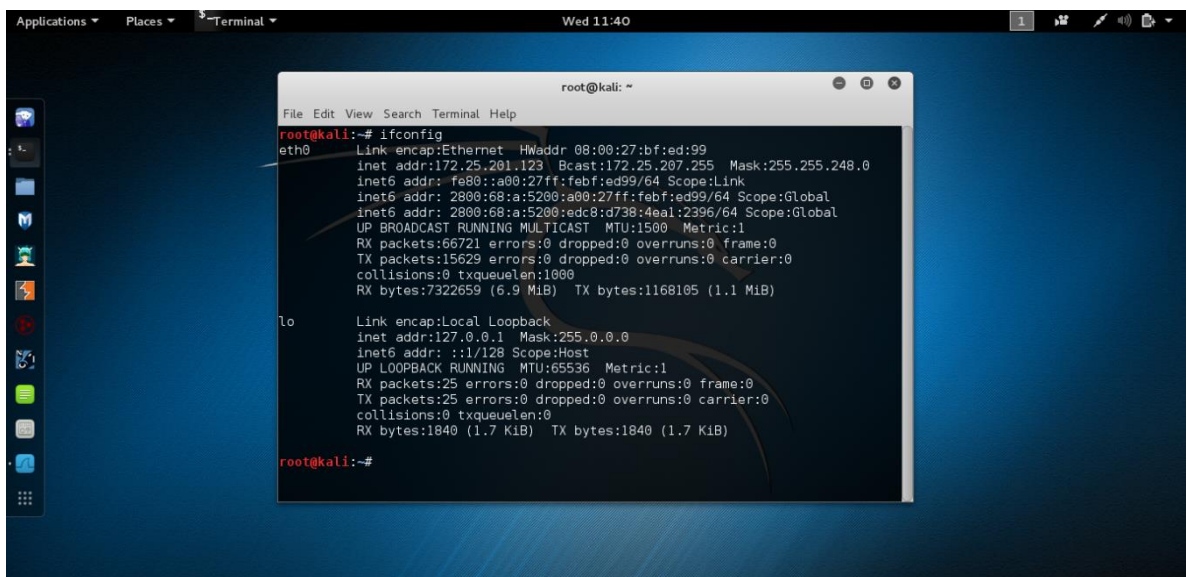


## Anexo B: Instalación y configuración de la máquina atacante

La manera más sencilla de instalar Kali Linux 2.0 para realizar las pruebas establecidas es descargar el archivo Kali-Linux-2.0.0-vbox-amd64.7z desde su dirección oficial <http://images.kali.org/Kali-Linux-2.0.0-vbox-amd64.7z>

Para montar la imagen en Virtual Box se accede al menú Archivo ▶ Importar servicio virtualizado, se selecciona el archivo Kali-Linux-2.0.0-vbox-amd64.ova, se opta por las características y recursos por defecto, se importa el servicio y la máquina queda instalada.

Las credenciales para acceder a Kali son user: root y password: toor. Dentro del sistema operativo ya se encuentran instaladas la suite de herramientas de THCIpV6 listas para utilizar.



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bf:ed:99
          inet addr:172.25.201.123  Bcast:172.25.207.255  Mask:255.255.248.0
          inet6 addr: fe80::a00:27ff:febf:ed99/64  Scope:Link
          inet6 addr: 2800:68:a:5200:a00:27ff:febf:ed99/64  Scope:Global
          inet6 addr: 2800:68:a:5200:edc8:d730:4ea1:2396/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66721 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15629 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7322659 (6.9 MiB)  TX bytes:1168105 (1.1 MiB)

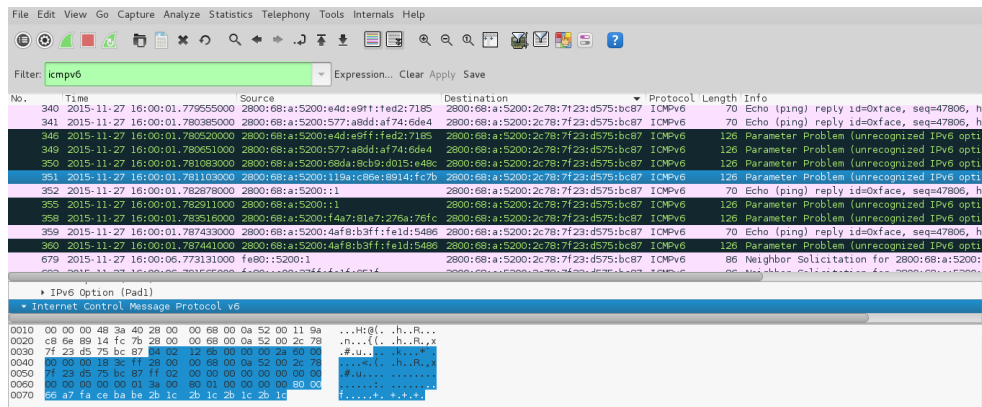
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1840 (1.7 KiB)  TX bytes:1840 (1.7 KiB)

root@kali:~#
```

## Anexo C: Experimento 1 desde la Kali Linux

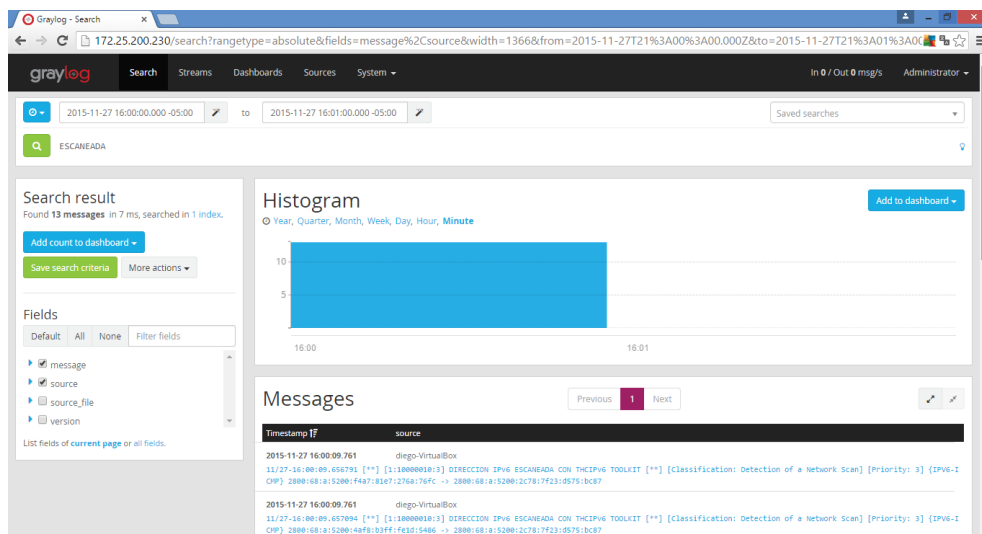
En las imágenes siguientes se muestran las capturas del tráfico malicioso generado por cada ataque desde Kali Linux y las capturas de las alertas generadas por cada ataque.

### Prueba 1 atk6-alive6 eth0



The screenshot shows a Wireshark capture of network traffic on the eth0 interface. The filter is set to 'icmpv6'. The packet list pane shows several ICMPv6 Echo (ping) requests and responses, as well as Parameter Problem messages. The packet details pane shows the structure of an ICMPv6 Echo request, including the IPv6 Option (Pad) and the Internet Control Message Protocol v6 header.

No.	Time	Source	Destination	Protocol	Length	Info
340	2015-11-27 16:00:01.779555000	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, h...
341	2015-11-27 16:00:01.780385000	2800:68:a:5200:577:a8dd:af74:6d64	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, h...
346	2015-11-27 16:00:01.780620000	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti...
349	2015-11-27 16:00:01.780651000	2800:68:a:5200:577:a8dd:af74:6d64	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti...
350	2015-11-27 16:00:01.781083000	2800:68:a:5200:68d:a8cb:d015:e48c	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti...
351	2015-11-27 16:00:01.781103000	2800:68:a:5200:119a:c96a:8914:fc7b	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti...
352	2015-11-27 16:00:01.782878000	2800:68:a:5200::1	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, h...
355	2015-11-27 16:00:01.782911000	2800:68:a:5200::1	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti...
359	2015-11-27 16:00:01.783169000	2800:68:a:5200:14d7:91a7:276a:76fc	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti...
359	2015-11-27 16:00:01.787433000	2800:68:a:5200:4af8:b3ff:fe1d:5486	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, h...
360	2015-11-27 16:00:01.787441000	2800:68:a:5200:4af8:b3ff:fe1d:5486	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti...
679	2015-11-27 16:00:06.779131000	fe80::5200:1	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200...



The screenshot shows the Graylog search interface. The search criteria are set to 'ESCANEAADA' for the time range 2015-11-27 16:00:00.000-05:00. The search results show 13 messages. A histogram shows the distribution of messages over time, with a peak at 16:01. The messages list shows two entries for the detection of a network scan.

Search result  
Found 13 messages in 7 ms, searched in 1 index.

Fields  
message  
source  
source\_file  
version

Histogram  
Year, Quarter, Month, Week, Day, Hour, Minute

Messages  
Previous 1 Next

Timestamp	source
2015-11-27 16:00:09.761	dego-virtualbox
11/27-16:00:09.656792 [**] [1:10000001:3] DIRECTION IPv6 ESCANEAADA CON THCPV6 TOOLKIT [**] [Classification: Detection of a Network Scan] [Priority: 3] (IPv6-I CWP) 2800:68:a:5200:f487:8167:276a:76fc -> 2800:68:a:5200:2c78:7f23:d575:bc87	
2015-11-27 16:00:09.761	dego-virtualbox
11/27-16:00:09.657894 [**] [1:10000001:3] DIRECTION IPv6 ESCANEAADA CON THCPV6 TOOLKIT [**] [Classification: Detection of a Network Scan] [Priority: 3] (IPv6-I CWP) 2800:68:a:5200:4af8:b3ff:fe1d:5486 -> 2800:68:a:5200:2c78:7f23:d575:bc87	

## Prueba 2 atk6-alive6 -4 172.25.0.0/21 eth0

Wireshark capture showing ICMPv6 traffic. The filter is set to `icmpv6`. The capture shows several Echo (ping) requests and responses, as well as Parameter Problem messages. The source IP is `2800:68:a:5200:e4d:e9ff:fed2:7185` and the destination is `2800:68:a:5200:2c78:7f23:d575:bc87`. The protocol is ICMPv6 and the length is 70 bytes. The info field shows `Echo (ping) reply id=0xface, seq=47806, h`.

No.	Time	Source	Destination	Protocol	Length	Info
228	2015-11-27 16:06:46.883912000	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, h
229	2015-11-27 16:06:46.883922000	2800:68:a:5200:119a:c86e:8914:fc7b	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
230	2015-11-27 16:06:46.883925000	2800:68:a:5200:1db6:49cc:f2a9:9160	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
231	2015-11-27 16:06:46.883927000	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
232	2015-11-27 16:06:46.883929000	2800:68:a:5200:68d4:5bc9:d015:4d8c	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
233	2015-11-27 16:06:46.883930000	2800:68:a:5200:14a7:81e7:276a:76fc	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
234	2015-11-27 16:06:46.883932000	2800:68:a:5200:11	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, h
235	2015-11-27 16:06:46.884133000	2800:68:a:5200:2c78:7f23:d575:bc87	ff02::192:168:1:1	ICMPv6	70	Echo (ping) request id=0xface, seq=47806, s
236	2015-11-27 16:06:46.884269000	2800:68:a:5200:2c78:7f23:d575:bc87	ff02::192:168:1:1	ICMPv6	78	Echo (ping) request id=0xface, seq=47806, s
237	2015-11-27 16:06:46.884415000	2800:68:a:5200:11	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
238	2015-11-27 16:06:46.884510000	2800:68:a:5200:2c78:7f23:d575:bc87	ff02::c0a8:101	ICMPv6	70	Echo (ping) request id=0xface, seq=47806, s
239	2015-11-27 16:06:46.884652000	2800:68:a:5200:2c78:7f23:d575:bc87	ff02::c0a8:101	ICMPv6	78	Echo (ping) request id=0xface, seq=47806, s

Graylog search results for the query `source=2800:68:a:5200:e4d:e9ff:fed2:7185`. The search found 43 messages in 7 ms. The results show a list of messages with details such as source, destination, and classification. The classification is `DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]` and the priority is 3. The source IP is `2800:68:a:5200:e4d:e9ff:fed2:7185` and the destination is `2800:68:a:5200:2c78:7f23:d575:bc87`.

Time	Source	Destination	Classification	Priority
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3
2015-11-27 16:06:55.161	2800:68:a:5200:e4d:e9ff:fed2:7185	2800:68:a:5200:2c78:7f23:d575:bc87	DIRECCION IPV6 ESCANEADA CON THCIPIV6 TOOLKIT [**]	3

## Prueba 3 atk6-alive6 -d eth0

Wireshark capture showing ICMPv6 traffic. The filter is set to `icmpv6`. The capture shows several Neighbor Solicitation and Neighbor Advertisement messages, as well as Echo (ping) requests and responses. The source IP is `2800:68:a:5200:119a:c86e:8914:fc7b` and the destination is `2800:68:a:5200:2c78:7f23:d575:bc87`. The protocol is ICMPv6 and the length is 126 bytes. The info field shows `Neighbor Solicitation for 2800:68:a:5200:2c`.

No.	Time	Source	Destination	Protocol	Length	Info
281	2015-11-27 16:14:08.36619000	2800:68:a:5200:119a:c86e:8914:fc7b	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
282	2015-11-27 16:14:08.36627000	2800:68:a:5200:1db6:49cc:f2a9:9160	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
283	2015-11-27 16:14:08.36629000	2800:68:a:5200:68d4:5bc9:d015:4d8c	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
284	2015-11-27 16:14:08.361661000	2800:68:a:5200:4c19:34bf:4e7b:918b	ff02::1:ff75:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200:
285	2015-11-27 16:14:08.361685000	2800:68:a:5200:2c78:7f23:d575:bc87	2800:68:a:5200:4c19:34bf:4e7b:918b	ICMPv6	86	Neighbor Advertisement 2800:68:a:5200:2c
286	2015-11-27 16:14:08.361701000	2800:68:a:5200:14a7:81e7:276a:76fc	ff02::1:ff75:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200:
287	2015-11-27 16:14:08.361708000	2800:68:a:5200:2c78:7f23:d575:bc87	2800:68:a:5200:14a7:81e7:276a:76fc	ICMPv6	86	Neighbor Advertisement 2800:68:a:5200:2c
288	2015-11-27 16:14:08.361718000	2800:68:a:5200:11	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, f
289	2015-11-27 16:14:08.361724000	2800:68:a:5200:4af8:b3ff:fed1:5496	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
290	2015-11-27 16:14:08.361730000	2800:68:a:5200:2c78:7f23:d575:bc87	ff02::1:ff75:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200:
291	2015-11-27 16:14:08.361730000	2800:68:a:5200:2c78:7f23:d575:bc87	2800:68:a:5200:4af8:b3ff:fed1:5496	ICMPv6	86	Neighbor Advertisement 2800:68:a:5200:2c
292	2015-11-27 16:14:08.362129000	2800:68:a:5200:4c19:34bf:4e7b:918b	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti

Graylog - Search

172.25.200.230/search?rangetype=relative&fields=message%2Csource&width=1366&relative=300&q=ESCANEDA#fields=message%2Csource

graylog Search Streams Dashboards Sources System In 0 / Out 0 msgs Administrator

**Search result**  
Found 15 messages in 6 ms, searched in 1 index.

Add count to dashboard Save search criteria More actions

**Fields**  
Default All None Filter fields  
message source source\_file version  
List fields of current page or all fields.

2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212944 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:108e:49cc:f2a5:9180 -> 2800:68:a:5200:2c78:7f23:0575:bc87
2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212947 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:108e:49cc:f2a5:9180 -> 2800:68:a:5200:2c78:7f23:0575:bc87
2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212945 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:119a:c86e:8934:fc70 -> 2800:68:a:5200:2c78:7f23:0575:bc87
2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212943 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:108e:49cc:f2a5:9180 -> 2800:68:a:5200:2c78:7f23:0575:bc87
2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212956 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:e4d:9fff:f6d2:7185 -> 2800:68:a:5200:2c78:7f23:0575:bc87
2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212945 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:119a:c86e:8934:fc70 -> 2800:68:a:5200:2c78:7f23:0575:bc87
2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212943 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:108e:49cc:f2a5:9180 -> 2800:68:a:5200:2c78:7f23:0575:bc87
2015-11-27 16:14:16.261	diego-VirtualBox	11/27-16:14:16.212956 [**] [1:18000010:3] DIRECTION IPV6 ESCANEDA CON THCPV6 TOOLKIT [**] [Classification: detection of a Network Scan] [Priority: 3] [IPV6-I CMP] 2800:68:a:5200:e4d:9fff:f6d2:7185 -> 2800:68:a:5200:2c78:7f23:0575:bc87

Previous 1 Next

## Prueba 4 atk6-parasite6 -l eth0

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmpv6 and ipv6.addr==fe80:a00:27ff:febf:ed99 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
43679	2015-11-27 14:06:59.354520000	fe80:c98e:2ec7:369b:cf33	fe80:a00:27ff:febf:ed99	ICMPv6	86	Neighbor Advertisement fe80:c98e:2ec7:369b:cf33
43682	2015-11-27 14:06:59.365893000	fe80:a00:27ff:febf:ed99	2800:68:a:5200:7d3b:5cBc:ce24:2cd6	ICMPv6	1294	Redirect Is at 68:bc:0c:be:1b:c2
43710	2015-11-27 14:06:59.381456000	fe80:a00:27ff:febf:ed99	fe80:a4c4:903a:1e5f:c46a	ICMPv6	86	Neighbor Advertisement fe80:a00:27ff:febf:ed99
43749	2015-11-27 14:06:59.456143000	fe80:9492:a655:cda5:a9b6	fe80:a00:27ff:febf:ed99	ICMPv6	86	Neighbor Advertisement fe80:9492:a655:cda5:a9b6
43750	2015-11-27 14:06:59.456227000	fe80:a4c4:903a:1e5f:c46a	fe80:a00:27ff:febf:ed99	ICMPv6	86	Neighbor Advertisement fe80:a4c4:903a:1e5f:c46a
43751	2015-11-27 14:06:59.456300000	fe80:a00:27ff:febf:ed99	fe80:589e:71f6:b59:1e68	ICMPv6	86	Neighbor Advertisement fe80:a00:27ff:febf:ed99
43752	2015-11-27 14:06:59.457440000	fe80:a00:27ff:febf:ed99	fe80:9492:a655:cda5:a9b6	ICMPv6	86	Neighbor Advertisement fe80:a00:27ff:febf:ed99
43754	2015-11-27 14:06:59.458298000	fe80:589e:71f6:b59:1e68	fe80:a00:27ff:febf:ed99	ICMPv6	86	Neighbor Advertisement fe80:589e:71f6:b59:1e68
43757	2015-11-27 14:06:59.472785000	fe80:a00:27ff:febf:ed99	fe80:201e:bf6d:787c:5041	ICMPv6	86	Neighbor Advertisement fe80:a00:27ff:febf:ed99
43759	2015-11-27 14:06:59.473553000	fe80:201e:bf6d:787c:5041	fe80:a00:27ff:febf:ed99	ICMPv6	86	Neighbor Advertisement fe80:201e:bf6d:787c:5041

Frame 43682: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: QuantaCo\_24:01:9e (08:9e:01:24:01:9e)  
 Internet Protocol Version 6, Src: fe80:a00:27ff:febf:ed99, Dst: 2800:68:a:5200:7d3b:5cBc:ce24:2cd6 (2800:68:a:5200:7d3b:5cBc:ce24:2cd6)  
 Internet Control Message Protocol v6  
 Type: Redirect (137)

```

0030  5c bc ce 24 2c d6 39 00 ef 16 00 00 00 00 fe 80
0040  00 00 00 00 00 00 00 00 00 00 52 00 01 2a 0c
0050  28 80 f0 00 00 1a fa ce b0 c0 00 00 2d da 02 01
0060  68 bc ce 1b c2 04 95 00 00 00 00 00 00 60 00
0070  00 00 04 b9 06 40 28 00 00 68 00 00 00 52 00
0080  5c bc ce 24 2c d6 2a 03 28 80 f0 00 00 1a fa ce
0090  b0 c0 00 00 2d da dd 72 01 bb 89 bd c2 e4 b1 22
00a0  15 11 27 14 06 59 45 62 27 00 00 00 00 00 00
  
```

Graylog - Search

172.25.200.230/search?width=1366&from=2015-11-27T19:3A07%3A00%00&page=15&sortOrder=desc&q=&rangetype=absolute&fields=message%2Csource&

graylog Search Streams Dashboards Sources System In 0 / Out 0 msgs Administrator

**Search result**  
Found 1,469 messages in 4 ms, searched in 1 index.

Add count to dashboard Save search criteria More actions

**Fields**  
Default All None Filter fields  
message source source\_file version  
List fields of current page or all fields.

2015-11-27 14:07:01.862	diego-VirtualBox	11/27-14:07:01.774295 [**] [1:18000025:1] ATAKU HITH PARASITES CON THCPV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80:a00:27ff:febf:ed99 -> fe80:cd73:9371:132b:c06
2015-11-27 14:07:00.861	diego-VirtualBox	11/27-14:07:00.763339 [**] [1:18000025:1] ATAKU HITH PARASITES CON THCPV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80:a00:27ff:febf:ed99 -> 2800:68:a:5200:7d3b:5cBc:ce24:2cd6
2015-11-27 14:07:00.861	diego-VirtualBox	11/27-14:07:00.763337 [**] [1:18000025:1] ATAKU HITH PARASITES CON THCPV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80:a00:27ff:febf:ed99 -> 2800:68:a:5200:7d3b:5cBc:ce24:2cd6
2015-11-27 14:07:00.861	diego-VirtualBox	11/27-14:07:00.770336 [**] [1:18000025:1] ATAKU HITH PARASITES CON THCPV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80:a00:27ff:febf:ed99 -> 2800:68:a:5200:9c6:1f25:622e:297f
2015-11-27 14:07:00.861	diego-VirtualBox	11/27-14:07:00.770334 [**] [1:18000025:1] ATAKU HITH PARASITES CON THCPV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80:a00:27ff:febf:ed99 -> 2800:68:a:5200:9c6:1f25:622e:297f
2015-11-27 14:07:00.861	diego-VirtualBox	11/27-14:07:00.763342 [**] [1:18000025:1] ATAKU HITH PARASITES CON THCPV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80:a00:27ff:febf:ed99 -> 2800:68:a:5200:7d3b:5cBc:ce24:2cd6
2015-11-27 14:07:00.861	diego-VirtualBox	11/27-14:07:00.763341 [**] [1:18000025:1] ATAKU HITH PARASITES CON THCPV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80:a00:27ff:febf:ed99 -> 2800:68:a:5200:7d3b:5cBc:ce24:2cd6

Previous 10 11 12 13 14 15 Next

## Prueba 5 atk6-parasite6 -I -R eth0

Wireshark capture showing ICMPv6 Redirect packets. The filter is `icmpv6.type==137 and ipv6.addr==2800:68:a:5200:31`. The packets are from source `fe80::a00:27ff:febf:ed99` to destination `2800:68:a:5200:3b:bc7a:6d72:93cb`. The info field indicates "Redirect is at 68:bc:0c:be:1b:c2".

No.	Time	Source	Destination	Protocol	Length	Info
18425	2015-11-27 14:22:50.393748000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	214	Redirect is at 68:bc:0c:be:1b:c2
18428	2015-11-27 14:22:50.393781000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
18551	2015-11-27 14:22:50.698061000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	358	Redirect is at 68:bc:0c:be:1b:c2
19404	2015-11-27 14:22:51.842115000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	214	Redirect is at 68:bc:0c:be:1b:c2
19407	2015-11-27 14:22:51.842220000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	198	Redirect is at 68:bc:0c:be:1b:c2
19410	2015-11-27 14:22:51.842304000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
20670	2015-11-27 14:22:53.312762000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
20734	2015-11-27 14:22:53.393370000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	462	Redirect is at 68:bc:0c:be:1b:c2
25631	2015-11-27 14:23:00.795327000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	574	Redirect is at 68:bc:0c:be:1b:c2
26439	2015-11-27 14:23:01.060319000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2

List of network events from a virtual machine. The events are categorized as "Potential Corporate Privacy Violation" with a priority of 1. The events are related to ICMPv6 Redirect packets.

- 2015-11-27 14:23:01.261 diego-VirtualBox  
11/27-14:23:01.163597 [\*\*] [1:10800025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb
- 2015-11-27 14:23:01.261 diego-VirtualBox  
11/27-14:23:01.163596 [\*\*] [1:10800025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb
- 2015-11-27 14:22:59.661 diego-VirtualBox  
11/27-14:22:59.613284 [\*\*] [1:10800025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb
- 2015-11-27 14:22:59.661 diego-VirtualBox  
11/27-14:22:59.613286 [\*\*] [1:10800025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb
- 2015-11-27 14:22:59.661 diego-VirtualBox  
11/27-14:22:59.613283 [\*\*] [1:10800025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb
- 2015-11-27 14:22:59.661 diego-VirtualBox  
11/27-14:22:59.613286 [\*\*] [1:10800025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb
- 2015-11-27 14:22:59.461 diego-VirtualBox  
11/27-14:22:59.442786 [\*\*] [1:10800025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> fe80::c080:571e:f880:af86

## Prueba 6 atk6-parasite6 -I -F eth0

Wireshark capture showing ICMPv6 Redirect packets. The filter is `icmpv6.type==137`. The packets are from source `fe80::a00:27ff:febf:ed99` to destination `2800:68:a:5200:41e:f9b6:e2f8:8719`. The info field indicates "Redirect is at 68:bc:0c:be:1b:c2".

No.	Time	Source	Destination	Protocol	Length	Info
20520	2015-11-27 14:31:02.862218000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	310	Redirect is at 68:bc:0c:be:1b:c2
20536	2015-11-27 14:31:02.967138000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3b:bc7a:6d72:93cb	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
21602	2015-11-27 14:31:04.376765000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:41e:f9b6:e2f8:8719	ICMPv6	1294	Redirect is at 68:bc:0c:be:1b:c2
21657	2015-11-27 14:31:04.441135000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:41e:f9b6:e2f8:8719	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
21669	2015-11-27 14:31:04.480116000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:41e:f9b6:e2f8:8719	ICMPv6	470	Redirect is at 68:bc:0c:be:1b:c2
21700	2015-11-27 14:31:04.496719000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:41e:f9b6:e2f8:8719	ICMPv6	1294	Redirect is at 68:bc:0c:be:1b:c2
21716	2015-11-27 14:31:04.517264000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:41e:f9b6:e2f8:8719	ICMPv6	350	Redirect is at 68:bc:0c:be:1b:c2
21719	2015-11-27 14:31:04.517348000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:41e:f9b6:e2f8:8719	ICMPv6	1294	Redirect is at 68:bc:0c:be:1b:c2
21762	2015-11-27 14:31:04.618999000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:c4d4:331f:7366:8b77	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2
21777	2015-11-27 14:31:04.631002000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:c4d4:331f:7366:8b77	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2

2015-11-27 14:31:12.361	diego-VirtualBox	11/27-14:31:12.292879 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:41e:f9b6:e2f8:8719
2015-11-27 14:31:12.361	diego-VirtualBox	11/27-14:31:12.292649 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:41e:f9b6:e2f8:8719
2015-11-27 14:31:12.361	diego-VirtualBox	11/27-14:31:12.292650 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:41e:f9b6:e2f8:8719
2015-11-27 14:31:12.361	diego-VirtualBox	11/27-14:31:12.292883 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:41e:f9b6:e2f8:8719
2015-11-27 14:31:12.161	diego-VirtualBox	11/27-14:31:12.152671 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:41e:f9b6:e2f8:8719
2015-11-27 14:31:12.161	diego-VirtualBox	11/27-14:31:12.152669 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:41e:f9b6:e2f8:8719
2015-11-27 14:31:10.761	diego-VirtualBox	11/27-14:31:10.657065 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb
2015-11-27 14:31:10.761	diego-VirtualBox	11/27-14:31:10.657064 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3b:bc7a:6d72:93cb

## Prueba 7 atk6-parasite6 -l -H eth0

Filter: icmpv6.type==137

No.	Time	Source	Destination	Protocol	Length	Info
286920	2015-11-27 14:41:57.141469000	fe80::a00:27ff:febf:ed99	fe80::21:c8:100f:43af:69:1	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
286931	2015-11-27 14:41:57.141526000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:3095:56f6:500b:7f90	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
287538	2015-11-27 14:41:57.394866000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:508a:6e08:4c9d:37cc	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
287740	2015-11-27 14:41:57.498434000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:7947:fc3b:6f:5ca8	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
289019	2015-11-27 14:41:57.922790000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:b026:9f41:5a14:6c6b	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
289299	2015-11-27 14:41:57.968825000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:508a:6e08:4c9d:37cc	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
289631	2015-11-27 14:41:58.080990000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:c4f4:b699:8db9:7fd1	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
290025	2015-11-27 14:41:58.218750000	fe80::a00:27ff:febf:ed99	fe80::bc25:c519:b033:0c8e	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
290720	2015-11-27 14:41:58.403527000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:6d7e:5c8b:d4ad:7a39	ICMPv6	206	Redirect is at 68:bc:0c:be:1b:c2
291064	2015-11-27 14:41:58.486920000	fe80::a00:27ff:febf:ed99	fe80::5412:373b:da56:fa6e	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2

Frame 287538: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: Hewlett\_2b:f1:8f (2c:27:d7:2b:f1:8f)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99, Dst: 2800:68:a:5200:508a:6e08:4c9d:37cc (2800:68:a:5200:508a:6e08:4c9d:37cc)  
 Internet Control Message Protocol v6

Type: Redirect (137)  
 Code: 0  
 Flags: 0x00000000  
 Reserved: 0x00000000  
 Target Address: n.L..Z..5e.....  
 Source Address: .....R.....  
 Destination Address: .....  
 Hop Limit: .....  
 ICMPv6 Options (len 0):  
 Type: 0, Length: 0, Reserved: 0, Data: ..h..R.P.  
 Type: 0, Length: 0, Reserved: 0, Data: n.L..Z..5e.....  
 Type: 0, Length: 0, Reserved: 0, Data: ..e0..8

2015-11-27 14:42:01.761	diego-VirtualBox	11/27-14:42:01.728173 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:508a:6e08:4c9d:37cc
2015-11-27 14:42:01.761	diego-VirtualBox	11/27-14:42:01.728125 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:508a:6e08:4c9d:37cc
2015-11-27 14:42:01.761	diego-VirtualBox	11/27-14:42:01.728172 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:508a:6e08:4c9d:37cc
2015-11-27 14:42:00.261	diego-VirtualBox	11/27-14:42:00.219616 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3095:56f6:500b:7f90
2015-11-27 14:42:00.261	diego-VirtualBox	11/27-14:42:00.218427 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3095:56f6:500b:7f90
2015-11-27 14:42:00.261	diego-VirtualBox	11/27-14:42:00.219619 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3095:56f6:500b:7f90
2015-11-27 14:42:00.261	diego-VirtualBox	11/27-14:42:00.218430 [**] [1:10000025:1] ATAQUE MITM PARASITE6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:3095:56f6:500b:7f90



## Prueba 8 atk6-parasite6 -I -R -F -H

The image shows a Wireshark capture of ICMPv6 Redirect messages. The filter is set to `icmpv6.type==137`. The packet list shows several Redirect messages from source `fe80::a00:27ff:febf:ed99` to destination `2800:68:a:5200:6d7e:5c8b:d4ad:7a39`. The packet details pane shows the structure of an ICMPv6 Redirect message (Type: Redirect (137)).

Below the capture, a list of events is displayed, each with a red border:

- 2015-11-27 14:54:09.561 diego-VirtualBox  
11/27-14:54:09.482585 [\*\*] [1:10000025:1] ATAKUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:6d7e:5c8b:d4ad:7a39
- 2015-11-27 14:54:09.561 diego-VirtualBox  
11/27-14:54:09.482584 [\*\*] [1:10000025:1] ATAKUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:6d7e:5c8b:d4ad:7a39
- 2015-11-27 14:54:09.461 diego-VirtualBox  
11/27-14:54:09.386233 [\*\*] [1:10000025:1] ATAKUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:6d7e:5c8b:d4ad:7a39
- 2015-11-27 14:54:08.362 diego-VirtualBox  
11/27-14:54:08.270788 [\*\*] [1:10000025:1] ATAKUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:6d7e:5c8b:d4ad:7a39
- 2015-11-27 14:54:08.362 diego-VirtualBox  
11/27-14:54:08.270788 [\*\*] [1:10000025:1] ATAKUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:6d7e:5c8b:d4ad:7a39
- 2015-11-27 14:54:07.261 diego-VirtualBox  
11/27-14:54:07.221075 [\*\*] [1:10000025:1] ATAKUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:6d7e:5c8b:d4ad:7a39
- 2015-11-27 14:54:07.261 diego-VirtualBox  
11/27-14:54:07.221077 [\*\*] [1:10000025:1] ATAKUE MITM PARASITE6 CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:6d7e:5c8b:d4ad:7a39

## Prueba 9 atk6-fake\_router6 eth0 2001:db8:bad::/64

The image shows a Wireshark capture of ICMPv6 messages. The filter is set to `icmpv6`. The packet list shows several Router Advertisement messages from source `fe80::a00:27ff:febf:ed99` to destination `ff02::1`. The packet details pane shows the structure of an ICMPv6 Router Advertisement message (Type: Router Advertisement (134)).

2015-11-27 15:21:48.661	diego-VirtualBox
11/27-15:21:48.605271 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:21:48.661	diego-VirtualBox
11/27-15:21:48.605264 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:21:48.661	diego-VirtualBox
11/27-15:21:48.605266 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:21:48.661	diego-VirtualBox
11/27-15:21:48.605270 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:21:48.661	diego-VirtualBox
11/27-15:21:48.605268 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:21:48.661	diego-VirtualBox
11/27-15:21:43.599426 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	

## Prueba 10 atk6-fake\_router6 -H eth0 2001:db8:bad::/64

The screenshot shows a Wireshark capture of network traffic. The filter is set to `icmpv6.type==134 and ipv6.dst==ff02::1`. The packet list shows several ICMPv6 Router Advertisement messages from source `fe80::a00:27ff:febf:ed99` to destination `ff02::1`. The selected packet (No. 29626) is expanded to show the packet structure:

- Frame 29626: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0
- Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
- Type: Router Advertisement (134)

The packet bytes pane shows the raw hex and ASCII representation of the ICMPv6 message.

2015-11-27 15:29:58.863	diego-VirtualBox
11/27-15:29:58.757720 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:29:58.863	diego-VirtualBox
11/27-15:29:58.757721 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:29:58.863	diego-VirtualBox
11/27-15:29:58.757725 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:29:58.863	diego-VirtualBox
11/27-15:29:58.757718 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:29:58.863	diego-VirtualBox
11/27-15:29:58.757715 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:29:58.863	diego-VirtualBox
11/27-15:29:58.757722 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:29:58.863	diego-VirtualBox
11/27-15:29:58.757723 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	
2015-11-27 15:29:53.861	diego-VirtualBox
11/27-15:29:53.757607 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1	



## Prueba 11 atk6-fake\_router6 -D eth0 2001:db8:bad::/64

Filter: icmpv6

No.	Time	Source	Destination	Protocol	Length	Info
4	2015-11-27 15:37:36.972788000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
6	2015-11-27 15:37:36.995779000	fe80::594e:eabf:792:b15a	fe80::a00:27ff:febf:ed99	ICMPv6	86	Neighbor Solicitation for fe80::a00:27ff:febf:ed99 from 0c:
7	2015-11-27 15:37:36.995866000	fe80::a00:27ff:febf:ed99	fe80::594e:eabf:792:b15a	ICMPv6	78	Neighbor Advertisement fe80::a00:27ff:febf:ed99 (sol)
65	2015-11-27 15:37:37.517830000	fe80::a00:27ff:febf:ed99	fe80::201e:bf6d:787c:5041	ICMPv6	86	Neighbor Solicitation for fe80::201e:bf6d:787c:5041 from 08:
66	2015-11-27 15:37:37.518420000	fe80::201e:bf6d:787c:5041	fe80::a00:27ff:febf:ed99	ICMPv6	86	Neighbor Advertisement fe80::201e:bf6d:787c:5041 (sol, ovr)
99	2015-11-27 15:37:37.715945000	fe80::3d4e:7e3a:ec4f:c769	fe80::a00:27ff:febf:ed99	ICMPv6	86	Neighbor Solicitation for fe80::a00:27ff:febf:ed99 from 2c:
100	2015-11-27 15:37:37.715981000	fe80::a00:27ff:febf:ed99	fe80::3d4e:7e3a:ec4f:c769	ICMPv6	78	Neighbor Advertisement fe80::a00:27ff:febf:ed99 (sol)
115	2015-11-27 15:37:37.902081000	fe80::a00:27ff:febf:ed99	fe80::118b:12f3:bd99:3197	ICMPv6	86	Neighbor Solicitation for fe80::118b:12f3:bd99:3197 from 08:
116	2015-11-27 15:37:37.903485000	fe80::118b:12f3:bd99:3197	fe80::a00:27ff:febf:ed99	ICMPv6	86	Neighbor Advertisement fe80::118b:12f3:bd99:3197 (sol, ovr)
120	2015-11-27 15:37:37.961073000	fe80::8023:a8b9:246a:e841	fe80::a00:27ff:febf:ed99	ICMPv6	86	Neighbor Solicitation for fe80::a00:27ff:febf:ed99 from 00:

Frame 4: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Router Advertisement (134)

```

2015-11-27 15:37:34.861      diego-VirtualBox
11/27-15:37:34.773888 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:37:29.861      diego-VirtualBox
11/27-15:37:29.772994 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:37:24.861      diego-VirtualBox
11/27-15:37:24.771817 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:37:19.862      diego-VirtualBox
11/27-15:37:19.772952 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:37:09.861      diego-VirtualBox
11/27-15:37:09.769879 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:37:04.861      diego-VirtualBox
11/27-15:37:04.769757 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:36:59.861      diego-VirtualBox
11/27-15:36:59.768135 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:36:54.861      diego-VirtualBox
11/27-15:36:54.767200 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

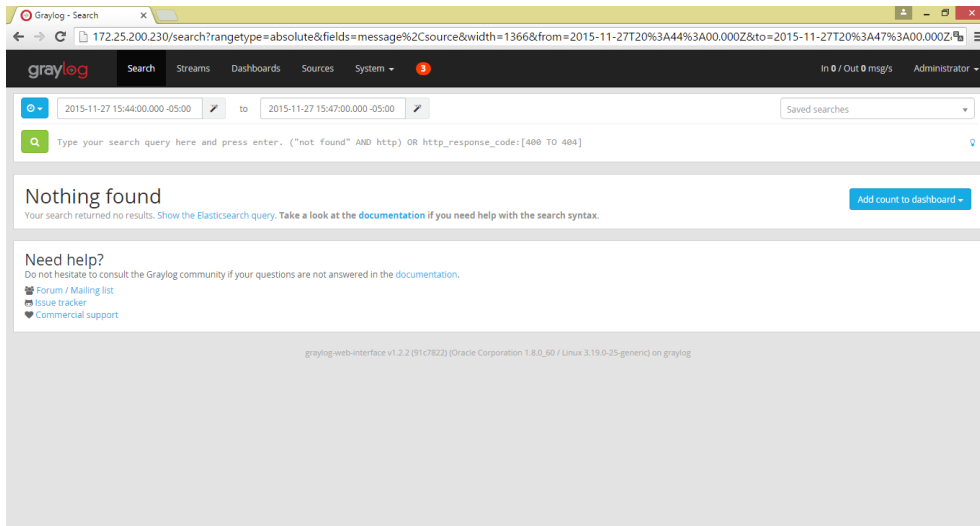
2015-11-27 15:36:49.861      diego-VirtualBox
11/27-15:36:49.766374 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {I
PV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1
  
```

## Prueba 12 atk6-fake\_router6 -F eth0 2001:db8:bad::/64

Filter: icmpv6.type==134 and ipv6.dst==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
728	2015-11-27 15:44:57.259217000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
1092	2015-11-27 15:45:02.260219000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
1500	2015-11-27 15:45:07.260918000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
1851	2015-11-27 15:45:12.262063000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
2209	2015-11-27 15:45:17.262388000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
2513	2015-11-27 15:45:22.262535000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
2897	2015-11-27 15:45:27.262848000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]

Frame 2513: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Malformed Packet: ICMPv6  
 [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]



## Prueba 13 atk6-fake\_router6 -H -D eth0 2001:db8:bad::/64

The screenshot shows a Wireshark capture of network traffic. The filter is `icmpv6.type==134 and ipv6.dst==ff02::1`. The packet list shows several ICMPv6 Router Advertisement (Type 134) packets. The selected packet (No. 3668) is expanded to show the packet bytes and the packet details pane.

**Packet Details:**

- Frame 3668: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface 0
- Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
  - Type: Router Advertisement (134)

**Packet Bytes:**

```

05f0 86 00 c5 59 ff 08 08 00 00 00 00 00 00 04 0c ...Y.....
0600 05 01 00 00 00 00 05 de 04 40 c0 11 11 11 11 .....(8)
0610 04 04 04 04 00 00 00 20 01 0d b8 06 ad 00 00 .....(8)
0620 00 00 00 00 00 00 00 01 01 08 00 27 bf ed 99 .....
0630 18 03 00 04 00 00 11 11 00 00 00 00 00 00 06 .....
0640 00 00 00 00 00 00 00 18 03 03 08 00 00 11 11 .....
0650 20 00 00 00 00 00 00 00 00 00 00 00 00 00 0c .....

```

**Log Output:**

```

2015-11-27 15:52:14.362 diego-VirtualBox
11/27-15:52:14.272842 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:52:09.361 diego-VirtualBox
11/27-15:52:09.270652 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:52:04.361 diego-VirtualBox
11/27-15:52:04.270037 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:51:59.361 diego-VirtualBox
11/27-15:51:59.270417 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:51:54.362 diego-VirtualBox
11/27-15:51:54.269971 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:51:49.361 diego-VirtualBox
11/27-15:51:49.269174 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:51:44.361 diego-VirtualBox
11/27-15:51:44.269255 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-27 15:51:39.362 diego-VirtualBox
11/27-15:51:39.265225 [**] [1:10000033:2] ATAUQE FAKE-ROUTER6 CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1

```

## Prueba 14 atk6-flood\_advertise6 eth0

Wireshark interface showing a capture of ICMPv6 Neighbor Advertisement messages. The filter is set to 'icmpv6'. The packet list shows several advertisements from various source addresses to the destination ff02::1. The selected packet (No. 2094) is expanded to show the Ethernet II header, Internet Protocol Version 6 header, and the Neighbor Advertisement message structure. The message details include the type (Neighbor Advertisement (136)), code (0), and the target address (ff02::1).

Log output showing multiple entries for 'diego-VirtualBox' with the message: '11/26-17:02:46.454837 [\*\*] [1:10000018:1] ATAUQUE FLOOD\_ADVERTISE6 (NA) CON THCHIP6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::218:fff:fe64:cb3 -> ff02::1'. One entry is highlighted with a red box.

## Prueba 15 atk6-flood\_solicitate6 eth0

Wireshark interface showing a capture of ICMPv6 Neighbor Solicitation messages. The filter is set to 'icmpv6'. The packet list shows several solicitations from various source addresses to the destination ff02::1. The selected packet (No. 35033) is expanded to show the Ethernet II header, Internet Protocol Version 6 header, and the Neighbor Solicitation message structure. The message details include the type (Neighbor Solicitation (135)), code (0), and the target address (ff02::1).

```

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918916 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:7c7f:feb2:2adb -> ff02::1

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918937 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:acff:fe8e:3e70 -> ff02::1

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918940 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:acff:fe8e:3e70 -> ff02::1

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918942 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:7c7f:feb2:2adb -> ff02::1

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918994 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:d4ff:fe6e:7fcc -> ff02::1

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918996 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:d4ff:fe6e:7fcc -> ff02::1

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918914 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:7c7f:feb2:2adb -> ff02::1

2015-11-26 17:11:30.001      diego-VirtualBox
11/26-17:11:09.918917 [**] [1:10000020:2] ATAQUE FLOOD_SOLICITATE6 (NS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:acff:fe8e:3e70 -> ff02::1

```

## Prueba 16 atk6-flood\_router6 eth0

The screenshot shows a Wireshark capture of network traffic. The filter is set to 'icmpv6'. The packet list pane shows several ICMPv6 Router Advertisement messages. The selected packet (No. 202171) is expanded to show the 'Internet Control Message Protocol v6' details. The details pane shows the type as 'Router Advertisement (134)' and the code as '0'. The raw packet bytes are displayed in hexadecimal and ASCII format.

```

2015-11-26 19:46:29.999      diego-VirtualBox
11/26-19:46:12.743461 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:1fff:fe1c:458a -> ff02::1

2015-11-26 19:46:29.999      diego-VirtualBox
11/26-19:46:12.743455 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:1fff:fe1c:458a -> ff02::1

2015-11-26 19:46:29.999      diego-VirtualBox
11/26-19:46:12.743460 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:1fff:fe1c:458a -> ff02::1

2015-11-26 19:46:29.999      diego-VirtualBox
11/26-19:46:12.743462 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:1fff:fe1c:458a -> ff02::1

2015-11-26 19:46:29.999      diego-VirtualBox
11/26-19:46:12.743464 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:1fff:fe1c:458a -> ff02::1

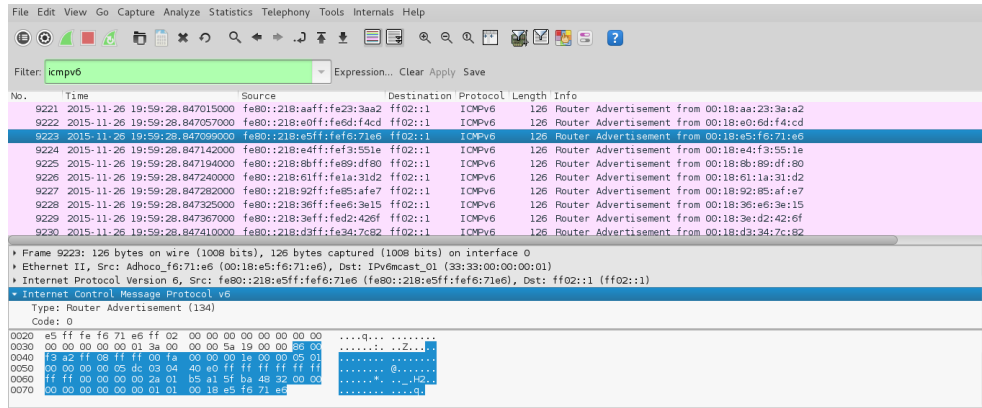
2015-11-26 19:46:29.999      diego-VirtualBox
11/26-19:46:12.743479 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:9fff:feab:b526 -> ff02::1

2015-11-26 19:46:29.999      diego-VirtualBox
11/26-19:46:12.743482 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:9fff:feab:b526 -> ff02::1

2015-11-26 19:46:29.997      diego-VirtualBox
11/26-19:46:12.743400 [**] [1:10000019:2] ATAQUE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:4dff:fe16:a6c4 -> ff02::1

```

## Prueba 17 atk6-flood\_router6 -F eth0



Filter: icmpv6

No.	Time	Source	Destination	Protocol	Length	Info
9221	2015-11-26 19:59:28.847015000	fe80::218:aaff:fe23:3aa2	ff02::1	ICMPv6	126	Router Advertisement from 00:18:aa:23:3a:a2
9222	2015-11-26 19:59:28.847057000	fe80::218:e0ff:fedf:44cd	ff02::1	ICMPv6	126	Router Advertisement from 00:18:e0:6d:f4:cd
9223	2015-11-26 19:59:28.847099000	fe80::218:e5ff:fe6f:71e6	ff02::1	ICMPv6	126	Router Advertisement from 00:18:e5:6f:71:e6
9224	2015-11-26 19:59:28.847142000	fe80::218:e4ff:fe3:551e	ff02::1	ICMPv6	126	Router Advertisement from 00:18:e4:f3:55:1e
9225	2015-11-26 19:59:28.847194000	fe80::218:ebff:fe89:d180	ff02::1	ICMPv6	126	Router Advertisement from 00:18:eb:89:d1:80
9226	2015-11-26 19:59:28.847240000	fe80::218:61ff:fe1a:31d2	ff02::1	ICMPv6	126	Router Advertisement from 00:18:61:1a:31:d2
9227	2015-11-26 19:59:28.847282000	fe80::218:92ff:fe85:afe7	ff02::1	ICMPv6	126	Router Advertisement from 00:18:92:85:af:e7
9228	2015-11-26 19:59:28.847325000	fe80::218:36ff:fe6:3e15	ff02::1	ICMPv6	126	Router Advertisement from 00:18:36:e6:3e:15
9229	2015-11-26 19:59:28.847367000	fe80::218:3eff:fed2:426f	ff02::1	ICMPv6	126	Router Advertisement from 00:18:3e:d2:42:6f
9230	2015-11-26 19:59:28.847410000	fe80::218:d3ff:fe34:7c82	ff02::1	ICMPv6	126	Router Advertisement from 00:18:d3:34:7c:82

Frame 9223: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0  
 Ethernet II, Src: Adhoco\_f6:71:e6 (00:18:e5:6f:71:e6), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::218:e5ff:fe6f:71e6 (fe80::218:e5ff:fe6f:71e6), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Router Advertisement (134)  
 Code: 0  
 0020 e5 ff fe 6f 71 e6 ff 02 00 00 00 00 00 00 00 00 .....q.....  
 0030 00 00 00 00 01 3a 00 00 00 5a 19 00 00 38 00 .....Z.....  
 0040 f3 a2 ff 08 ff ff 00 f8 00 00 00 18 00 00 05 01 .....  
 0050 00 00 00 00 02 00 04 40 40 ff ff ff ff ff ff .....  
 0060 ff ff 00 00 00 2a 01 b5 a1 9f ba 48 32 00 00 .....H.....  
 0070 00 00 00 00 00 01 01 00 18 e5 6f 71 e6 .....d.....

```

2015-11-26 19:59:40.078 diego-VirtualBox
11/26-19:59:35:277935 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:e0ff:fedf:44cd -> ff02::1

2015-11-26 19:59:40.078 diego-VirtualBox
11/26-19:59:35:277936 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:e0ff:fedf:44cd -> ff02::1

2015-11-26 19:59:40.078 diego-VirtualBox
11/26-19:59:35:277938 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:e0ff:fedf:44cd -> ff02::1

2015-11-26 19:59:40.078 diego-VirtualBox
11/26-19:59:35:277949 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:e0ff:fedf:44cd -> ff02::1

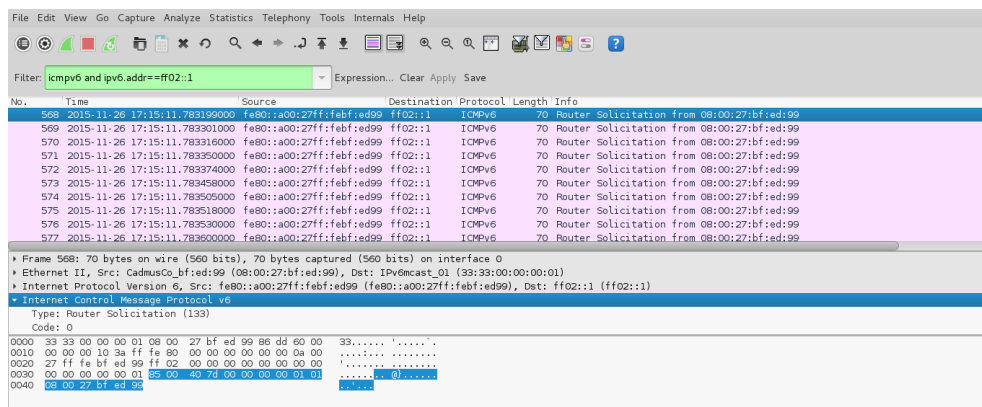
2015-11-26 19:59:40.078 diego-VirtualBox
11/26-19:59:35:277952 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:e0ff:fedf:44cd -> ff02::1

2015-11-26 19:59:40.078 diego-VirtualBox
11/26-19:59:35:277957 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:e5ff:fe6f:71e6 -> ff02::1

2015-11-26 19:59:40.014 diego-VirtualBox
11/26-19:59:35:277721 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:40ff:fe8e:5804 -> ff02::1

2015-11-26 19:59:40.014 diego-VirtualBox
11/26-19:59:35:277758 [**] [1:10000019:2] ATAUQE FLOOD_ROUTER6 (RA) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::218:40ff:fe8e:5804 -> ff02::1
  
```

## Prueba 18 atk6-flood\_rs6 eth0



Filter: icmpv6 and ipv6.addr==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
568	2015-11-26 17:15:11.783199000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
569	2015-11-26 17:15:11.783301000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
570	2015-11-26 17:15:11.783316000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
571	2015-11-26 17:15:11.783350000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
572	2015-11-26 17:15:11.783374000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
573	2015-11-26 17:15:11.783458000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
574	2015-11-26 17:15:11.783505000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
575	2015-11-26 17:15:11.783518000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
576	2015-11-26 17:15:11.783530000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
577	2015-11-26 17:15:11.783500000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99

Frame 568: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Router Solicitation (133)  
 Code: 0  
 0000 33 33 00 00 00 01 08 00 27 bf ed 99 86 dd 60 00 33.....'  
 0010 00 00 00 10 3a ff fe 00 00 00 00 00 00 0a 00 .....  
 0020 27 ff fe bf ed 99 ff 02 00 00 00 00 00 00 00 .....  
 0030 00 00 00 00 01 33 00 40 7d 00 00 00 01 01 .....  
 0040 08 00 27 bf ed 99 .....8.....

```

2015-11-26 17:15:20.335      diego-VirtualBox
11/26-17:15:19.853366 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> ff02::1

2015-11-26 17:15:20.335      diego-VirtualBox
11/26-17:15:19.853371 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> ff02::1

2015-11-26 17:15:20.335      diego-VirtualBox
11/26-17:15:19.853373 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> ff02::1

2015-11-26 17:15:20.335      diego-VirtualBox
11/26-17:15:19.853386 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> ff02::1

2015-11-26 17:15:20.335      diego-VirtualBox
11/26-17:15:19.853385 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> ff02::1

2015-11-26 17:15:20.065      diego-VirtualBox
11/26-17:15:19.853193 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:feb7:ed99 -> ff02::1

```

## Prueba 19 atk6-flood\_rs6 -s eth0

The screenshot shows a Wireshark capture of network traffic. The filter is set to 'icmpv6'. The packet list pane shows several ICMPv6 Router Solicitation packets (type 133) from various source addresses to the destination ff02::1. The packet details pane for packet 7316 shows the structure of the Router Solicitation message, including the code (0) and the ICMPv6 header fields.

No.	Time	Source	Destination	Protocol	Length	Info
7314	2015-11-26 17:20:15.867540000	fe80::a00:27ff:fec4:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7315	2015-11-26 17:20:15.867579000	fe80::a00:27ff:fec5:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7316	2015-11-26 17:20:15.867619000	fe80::a00:27ff:fec6:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7317	2015-11-26 17:20:15.867658000	fe80::a00:27ff:fec7:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7318	2015-11-26 17:20:15.867720000	fe80::a00:27ff:fec8:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7319	2015-11-26 17:20:15.867781000	fe80::a00:27ff:fec9:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7320	2015-11-26 17:20:15.867800000	fe80::a00:27ff:feca:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7321	2015-11-26 17:20:15.867839000	fe80::a00:27ff:fecb:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7322	2015-11-26 17:20:15.867878000	fe80::a00:27ff:fecd:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
7323	2015-11-26 17:20:15.867917000	fe80::a00:27ff:fecd:a389	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99

Packet 7316 details:

- Frame 7316: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
- Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::a00:27ff:fec6:a389 (fe80::a00:27ff:fec6:a389), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
  - Type: Router Solicitation (133)
  - Code: 0

Hex dump of packet 7316:

```

0000 33 33 00 00 00 01 08 00 27 bf ed 99 86 dd 60 00 33.....'.....
0010 00 00 00 10 3a ff fe 00 00 00 00 00 00 0a 00 .....
0020 27 ff fe c6 a3 89 ff 02 00 00 00 00 00 00 00 00 27 ff fe c6 a3 89 ff 02 00 00 00 00 00 00 00
0030 00 00 00 00 00 01 33 33 00 00 00 00 00 00 01 01 .....33.....
0040 08 00 27 bf ed 99 .....

```

```

2015-11-26 17:20:23.594      diego-VirtualBox
11/26-17:20:23.395928 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:fec6:a389 -> ff02::1

2015-11-26 17:20:23.594      diego-VirtualBox
11/26-17:20:23.395930 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:fec6:a389 -> ff02::1

2015-11-26 17:20:23.594      diego-VirtualBox
11/26-17:20:23.395924 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:fec6:a389 -> ff02::1

2015-11-26 17:20:23.593      diego-VirtualBox
11/26-17:20:23.395836 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:fec6:a389 -> ff02::1

2015-11-26 17:20:23.593      diego-VirtualBox
11/26-17:20:23.395834 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:fec6:a389 -> ff02::1

2015-11-26 17:20:23.593      diego-VirtualBox
11/26-17:20:23.395835 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:fec6:a389 -> ff02::1

2015-11-26 17:20:23.593      diego-VirtualBox
11/26-17:20:23.395837 [**] [1:10000021:2] ATAQUE FLOOD_RS6 (RS) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{IPV6-ICMP} fe80::a00:27ff:fec6:a389 -> ff02::1

```

## Prueba 20 atk6-flood\_rs6 -S eth0

Wireshark capture showing ICMPv6 Router Solicitation messages. The filter is 'icmpv6 and ipv6.addr==ff02::1'. The capture shows multiple packets from various source addresses to the destination ff02::1. The selected packet (No. 539) is expanded to show the Ethernet II header, Internet Protocol Version 6 header, and Internet Control Message Protocol (ICMPv6) header, which is a Router Solicitation (133) with code 0. The packet bytes are shown in hexadecimal and ASCII.

Security logs showing repeated events for '2015-11-26 17:25:23.487' from 'diego-VirtualBox'. Each event is classified as 'Potential Corporate Privacy Violation' with a priority of 1. The event details include: '11/26-17:25:23.131103 [\*\*] [1:10800021:2] ATAUKE FLOOD\_RS6 (RS) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> ff02::1'. One instance of this log entry is highlighted with a red border.

## Prueba 21 atk6-flood\_rs6 -s -S eth0

Wireshark capture showing ICMPv6 Router Solicitation messages. The filter is 'icmpv6 and ipv6.addr==ff02::1'. The capture shows multiple packets from various source addresses to the destination ff02::1. The selected packet (No. 326) is expanded to show the Ethernet II header, Internet Protocol Version 6 header, and Internet Control Message Protocol (ICMPv6) header, which is a Router Solicitation (133) with code 0. The packet bytes are shown in hexadecimal and ASCII.



2015-11-26 17:31:14.000	diego-VirtualBox	11/26-17:31:13.693853 [**] [1:10000021:2] ATAUQE FLOOD_R56 (R5) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:b4f4 -> ff02::1
2015-11-26 17:31:14.000	diego-VirtualBox	11/26-17:31:13.693851 [**] [1:10000021:2] ATAUQE FLOOD_R56 (R5) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:b4f4 -> ff02::1
2015-11-26 17:31:14.000	diego-VirtualBox	11/26-17:31:13.693854 [**] [1:10000021:2] ATAUQE FLOOD_R56 (R5) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:b4f4 -> ff02::1
2015-11-26 17:31:14.000	diego-VirtualBox	11/26-17:31:13.693846 [**] [1:10000021:2] ATAUQE FLOOD_R56 (R5) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:b4f4 -> ff02::1
2015-11-26 17:31:14.000	diego-VirtualBox	11/26-17:31:13.693862 [**] [1:10000021:2] ATAUQE FLOOD_R56 (R5) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:b4f4 -> ff02::1
2015-11-26 17:31:14.000	diego-VirtualBox	11/26-17:31:13.693861 [**] [1:10000021:2] ATAUQE FLOOD_R56 (R5) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:b4f4 -> ff02::1

## Prueba 22 atk6-flood\_redir6 eth0

The screenshot shows a Wireshark capture of network traffic. The filter is set to 'icmpv6 and ipv6.addr==ff02::1'. The packet list shows several ICMPv6 Redirect messages (No. 645-654) from source fe80::a00:27ff:feb0:ed99 to destination ff02::1. The packet details for packet 645 show: Ethernet II, Src: CadmusCo\_bf:ed:99:08:00:27:bf:ed:99, Dst: Ipv6cast\_01 (33:33:00:00:00:01), Internet Protocol Version 6, Src: fe80::a00:27ff:feb0:ed99, Dst: ff02::1 (ff02::1), and Internet Control Message Protocol v6, Type: Redirect (137). The packet bytes show the ICMPv6 Redirect structure with fields like destination address and flags.

2015-11-26 17:37:09.501	diego-VirtualBox	11/26-17:37:09.245845 [**] [1:10000022:2] ATAUQE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:ed99 -> ff02::1
2015-11-26 17:37:09.501	diego-VirtualBox	11/26-17:37:09.245846 [**] [1:10000022:2] ATAUQE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:ed99 -> ff02::1
2015-11-26 17:37:09.501	diego-VirtualBox	11/26-17:37:09.245848 [**] [1:10000022:2] ATAUQE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:ed99 -> ff02::1
2015-11-26 17:37:09.501	diego-VirtualBox	11/26-17:37:09.245850 [**] [1:10000022:2] ATAUQE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:ed99 -> ff02::1
2015-11-26 17:37:09.501	diego-VirtualBox	11/26-17:37:09.245852 [**] [1:10000022:2] ATAUQE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:ed99 -> ff02::1
2015-11-26 17:37:09.501	diego-VirtualBox	11/26-17:37:09.245875 [**] [1:10000022:2] ATAUQE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:ed99 -> ff02::1
2015-11-26 17:37:09.501	diego-VirtualBox	11/26-17:37:09.245877 [**] [1:10000022:2] ATAUQE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:feb0:ed99 -> ff02::1



## Prueba 23 atk6-flood\_redir6 -H eth0

Filter: icmpv6 and ipv6.addr==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
827	2015-11-26 17:44:01.029459000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 68:bc:0c:be:1b:c2
1098	2015-11-26 17:44:05.026474000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 68:bc:0c:be:1b:c2
1459	2015-11-26 17:44:07.961015000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:f8:25:a8:09
1460	2015-11-26 17:44:07.961105000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:f9:25:a8:09
1461	2015-11-26 17:44:07.961123000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:fa:25:a8:09
1462	2015-11-26 17:44:07.961139000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:fb:25:a8:09
1463	2015-11-26 17:44:07.961223000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:fc:25:a8:09
1464	2015-11-26 17:44:07.961273000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:fd:25:a8:09
1465	2015-11-26 17:44:07.961321000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:fe:25:a8:09

Frame 1465: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Redirect (137)

- 2015-11-26 17:44:17.761 diego-VirtualBox  
 11/26-17:44:17.758359 [\*\*] [1:1000002:2] ATAKE FLOOD\_REDIRE (RE) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1
- 2015-11-26 17:44:17.761 diego-VirtualBox  
 11/26-17:44:17.758381 [\*\*] [1:1000002:2] ATAKE FLOOD\_REDIRE (RE) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1
- 2015-11-26 17:44:17.761 diego-VirtualBox  
 11/26-17:44:17.758382 [\*\*] [1:1000002:2] ATAKE FLOOD\_REDIRE (RE) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1
- 2015-11-26 17:44:17.761 diego-VirtualBox  
 11/26-17:44:17.759261 [\*\*] [1:1000002:2] ATAKE FLOOD\_REDIRE (RE) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1
- 2015-11-26 17:44:17.761 diego-VirtualBox  
 11/26-17:44:17.759264 [\*\*] [1:1000002:2] ATAKE FLOOD\_REDIRE (RE) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1
- 2015-11-26 17:44:17.761 diego-VirtualBox  
 11/26-17:44:17.759266 [\*\*] [1:1000002:2] ATAKE FLOOD\_REDIRE (RE) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1
- 2015-11-26 17:44:17.761 diego-VirtualBox  
 11/26-17:44:17.752552 [\*\*] [1:1000002:2] ATAKE FLOOD\_REDIRE (RE) CON THCIpV6 TOOLKIT [\*\*] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

## Prueba 24 atk6-flood\_redir6 -F eth0

Filter: icmpv6 and ipv6.addr==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
1304	2015-11-26 17:49:20.848070000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:cf:f6:65:3f
1305	2015-11-26 17:49:20.848178000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d0:f6:65:3f
1306	2015-11-26 17:49:20.848280000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d1:f6:65:3f
1307	2015-11-26 17:49:20.848292000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d2:f6:65:3f
1308	2015-11-26 17:49:20.848395000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d3:f6:65:3f
1309	2015-11-26 17:49:20.848353000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d4:f6:65:3f
1310	2015-11-26 17:49:20.848404000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d5:f6:65:3f
1311	2015-11-26 17:49:20.848455000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d6:f6:65:3f
1312	2015-11-26 17:49:20.848476000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:d7:f6:65:3f

Frame 1304: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Redirect (137)

```

2015-11-26 17:49:28.393      diego-VirtualBox
11/26-17:49:28.136655 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 17:49:28.393      diego-VirtualBox
11/26-17:49:28.136658 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 17:49:28.393      diego-VirtualBox
11/26-17:49:28.136652 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 17:49:28.393      diego-VirtualBox
11/26-17:49:28.136653 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 17:49:28.393      diego-VirtualBox
11/26-17:49:28.136658 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 17:49:28.393      diego-VirtualBox
11/26-17:49:28.136657 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 17:49:28.393      diego-VirtualBox
11/26-17:49:28.136638 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

```

## Prueba 25 atk6-flood\_redir6 -H -F eth0

The screenshot shows a Wireshark capture of an ICMPv6 flood attack. The filter is set to 'icmpv6 and ipv6.addr==ff02::1'. The packet list shows multiple ICMPv6 Redirect packets from source fe80::a00:27ff:febf:ed99 to destination ff02::1. The packet details pane shows the structure of an ICMPv6 Redirect packet (Type: Redirect (137)), including fields for Code, Redirected Address, and Next Hop Address.

No.	Time	Source	Destination	Protocol	Length	Info
420	2015-11-26 19:39:00.657608000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:22:75:23:0d
421	2015-11-26 19:39:00.657650000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:23:75:23:0d
422	2015-11-26 19:39:00.657657000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:24:75:23:0d
423	2015-11-26 19:39:00.657675000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:25:75:23:0d
424	2015-11-26 19:39:00.657690000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:26:75:23:0d
425	2015-11-26 19:39:00.657763000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:27:75:23:0d
426	2015-11-26 19:39:00.657810000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:28:75:23:0d
427	2015-11-26 19:39:00.657825000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:29:75:23:0d
428	2015-11-26 19:39:00.657840000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:2a:75:23:0d

```

2015-11-26 19:39:10.700      diego-VirtualBox
11/26-19:39:10.666282 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 19:39:10.700      diego-VirtualBox
11/26-19:39:10.666283 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 19:39:10.700      diego-VirtualBox
11/26-19:39:10.666889 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 19:39:10.692      diego-VirtualBox
11/26-19:39:10.666281 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 19:39:10.692      diego-VirtualBox
11/26-19:39:10.666281 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

2015-11-26 19:39:10.692      diego-VirtualBox
11/26-19:39:10.666280 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

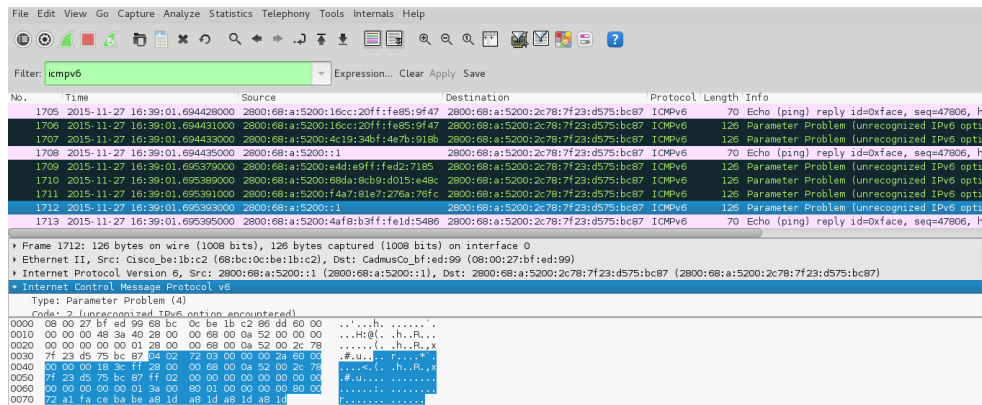
2015-11-26 19:39:10.692      diego-VirtualBox
11/26-19:39:10.666279 [**] [1:1000002:2] ATAQUE FLOOD_REDIRE6 (RE) CON THCIpV6 TOOLKIT [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] [IPV6-ICMP] fe80::a00:27ff:febf:ed99 -> ff02::1

```

## Anexo D: Experimento 2 desde la Kali Linux

En las imágenes siguientes se muestran las capturas del tráfico malicioso generado por cada ataque desde Kali Linux y las capturas de las alertas generadas por cada ataque.

### Prueba 1 atk6-alive6 eth0



## Prueba 2 atk6-alive6 -4 172.25.0.0/21 eth0

No.	Time	Source	Destination	Protocol	Length	Info
1313	2015-11-27 16:42:11.158596000	2800:68:a:5200:f4a7:81e7:276a:76fc	ff02::1:fff75:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200:2c7
1314	2015-11-27 16:42:11.158610000	2800:68:a:5200:2c78:7f23:d575:bc87	2800:68:a:5200:f4a7:81e7:276a:76fc	ICMPv6	86	Neighbor Advertisement 2800:68:a:5200:2c7
1315	2015-11-27 16:42:11.158627000	2800:68:a:5200::1	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
1316	2015-11-27 16:42:11.158637000	2800:68:a:5200:f4a7:81e7:276a:76fc	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
1317	2015-11-27 16:42:11.159316000	2800:68:a:5200:16cc:20ff:fe85:9f47	ff02::1:fff75:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200:
1318	2015-11-27 16:42:11.159324000	2800:68:a:5200:2c78:7f23:d575:bc87	2800:68:a:5200:16cc:20ff:fe85:9f47	ICMPv6	86	Neighbor Advertisement 2800:68:a:5200:2c7
1319	2015-11-27 16:42:11.159345000	2800:68:a:5200:68da:8cb9:d015:e48c	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
1320	2015-11-27 16:42:11.159348000	2800:68:a:5200:4c19:34bf:4e7b:918b	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
1321	2015-11-27 16:42:11.159350000	2800:68:a:5200:f4a7:81e7:276a:76fc	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti

Frame 1320: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0  
 Ethernet II, Src: Hewlett\_2b:f2:1a (2c:27:d7:2b:f2:1a), Dst: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99)  
 Internet Protocol Version 6, Src: 2800:68:a:5200:4c19:34bf:4e7b:918b (2800:68:a:5200:4c19:34bf:4e7b:918b), Dst: 2800:68:a:5200:2c78:7f23:d575:bc87 (2800:68:a:5200:2c78:7f23:d575:bc87)  
 Internet Control Message Protocol v6  
 Type: Parameter Problem (4)

```

0000 08 00 27 bf ed 99 2c 27 d7 2b f2 1a 86 dd 60 00  ..G...
0010 00 00 00 48 3a 40 28 00 00 68 00 0a 52 00 4c 19  ..H:(. .h.R.L.
0020 34 bf 4e 7b 91 8b 28 00 00 68 00 0a 52 00 2c 78  4.N(. .h.R,x
0030 7f 23 d5 75 bc 87 04 02 0c 68 00 00 0a 52 00 2c 78  ..G(. .h.R,x
0040 00 00 00 18 3c ff 28 00 00 68 00 0a 52 00 2c 78  ..G(. .h.R,x
0050 7f 23 d5 75 bc 87 ff 02 00 00 00 00 00 00 00 00  ..G...
0060 00 00 00 00 01 3a 00 80 01 00 00 00 00 80 00  ..G...
0070 ds a0 fa ce ba be cd id cd id cd id cd id  ..G...
  
```

```

2015-11-27 16:42:01.262      diego-VirtualBox
11/27-16:42:01.166457 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPv6-ICMP] fe80::28ab:78fe:a753:a582 -> fe80::5200:1

2015-11-27 16:42:01.262      diego-VirtualBox
11/27-16:42:01.166456 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5
200:1 -> fe80::28ab:78fe:a753:a582

2015-11-27 16:42:01.161      diego-VirtualBox
11/27-16:42:01.132291 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5
498:694d:6af6:71a2 -> fe80::5200:1

2015-11-27 16:42:01.161      diego-VirtualBox
11/27-16:42:01.148682 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPv6-ICMP] fe80::bb01:a598:6a37:26a1 -> fe80::5200:1

2015-11-27 16:42:01.161      diego-VirtualBox
11/27-16:42:01.148599 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5
200:1 -> fe80::bb01:a598:6a37:26a1

2015-11-27 16:42:00.261      diego-VirtualBox
11/27-16:42:00.171204 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPv6-ICMP] fe80::c869:70b3:5e66:7d9f -> fe80::5200:1

2015-11-27 16:42:00.261      diego-VirtualBox
11/27-16:42:00.170074 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5
200:1 -> fe80::c869:70b3:5e66:7d9f
  
```

## Prueba 3 atk6-alive6 -d eth0

No.	Time	Source	Destination	Protocol	Length	Info
546	2015-11-27 16:45:04.614090000	2800:68:a:5200::1	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
547	2015-11-27 16:45:04.614790000	2800:68:a:5200:68da:8cb9:d015:e48c	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
548	2015-11-27 16:45:04.614377000	2800:68:a:5200:4c19:34bf:4e7b:918b	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
549	2015-11-27 16:45:04.614379000	2800:68:a:5200:f4a7:81e7:276a:76fc	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
551	2015-11-27 16:45:04.616250000	2800:68:a:5200:16cc:20ff:fe85:9f47	ff02::1:fff75:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200:
552	2015-11-27 16:45:04.616273000	2800:68:a:5200:2c78:7f23:d575:bc87	2800:68:a:5200:16cc:20ff:fe85:9f47	ICMPv6	86	Neighbor Advertisement 2800:68:a:5200:2c7
553	2015-11-27 16:45:04.616543000	2800:68:a:5200:16cc:20ff:fe85:9f47	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	70	Echo (ping) reply id=0xface, seq=47806, h
554	2015-11-27 16:45:04.616550000	2800:68:a:5200:16cc:20ff:fe85:9f47	2800:68:a:5200:2c78:7f23:d575:bc87	ICMPv6	126	Parameter Problem (unrecognized IPv6 opti
555	2015-11-27 16:45:04.617396000	2800:68:a:5200:4af8:b3ff:fe1d:548e	ff02::1:fff75:bc87	ICMPv6	86	Neighbor Solicitation for 2800:68:a:5200:

Frame 554: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0  
 Ethernet II, Src: Tp-Link\_t\_85:9f:47 (14:cc:20:85:9f:47), Dst: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99)  
 Internet Protocol Version 6, Src: 2800:68:a:5200:16cc:20ff:fe85:9f47 (2800:68:a:5200:16cc:20ff:fe85:9f47), Dst: 2800:68:a:5200:2c78:7f23:d575:bc87 (2800:68:a:5200:2c78:7f23:d575:bc87)  
 Internet Control Message Protocol v6  
 Type: Parameter Problem (4)

```

0000 08 00 27 bf ed 99 14 cc 20 85 9f 47 86 dd 60 00  ..G...
0010 00 00 00 48 3a 40 28 00 00 68 00 0a 52 00 16 cc  ..H:(. .h.R..
0020 20 ff fe 85 9f 47 28 00 00 68 00 0a 52 00 2c 78  ..G(. .h.R,x
0030 7f 23 d5 75 bc 87 04 02 0c 68 00 00 0a 52 00 2c 78  ..G(. .h.R,x
0040 00 00 00 18 3c ff 28 00 00 68 00 0a 52 00 2c 78  ..G(. .h.R,x
0050 7f 23 d5 75 bc 87 ff 02 00 00 00 00 00 00 00 00  ..G...
0060 00 00 00 00 01 3a 00 80 01 00 00 00 00 80 00  ..G...
0070 e6 a0 fa ce ba be eb id eb id eb id eb id  ..G...
  
```

2015-11-27 16:45:01.961	diego-VirtualBox	11/27-16:45:01.918459 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::2800:68:a:5200:d009:de66:8cf5:704 -> fe80::5200:1
2015-11-27 16:45:01.961	diego-VirtualBox	11/27-16:45:01.917622 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> 2800:68:a:5200:d009:de66:8cf5:704
2015-11-27 16:45:01.261	diego-VirtualBox	11/27-16:45:01.151108 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::7015:bac8:309a:9f1 -> fe80::5200:1
2015-11-27 16:45:01.261	diego-VirtualBox	11/27-16:45:01.170914 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::24eb:98c5:6b8a:41b7
2015-11-27 16:45:01.261	diego-VirtualBox	11/27-16:45:01.171115 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::24eb:98c5:6b8a:41b7 -> fe80::5200:1
2015-11-27 16:45:01.161	diego-VirtualBox	11/27-16:45:01.120529 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::7d4f:6dd9:dc0d:c95c -> fe80::5200:1
2015-11-27 16:45:01.161	diego-VirtualBox	11/27-16:45:01.120069 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::7d4f:6dd9:dc0d:c95c

## Prueba 4 atk6-parasite6 -l eth0

Filter: icmpv6.type==137

No.	Time	Source	Destination	Protocol	Length	Info
4725	2015-11-27 16:51:57.558369000	fe80::a00:27ff:febf:ed99	fe80::911b:35d9:958f:edde	ICMPv6	206	Redirect
4733	2015-11-27 16:51:57.561995000	fe80::a00:27ff:febf:ed99	fe80::911b:35d9:958f:edde	ICMPv6	214	Redirect is at a0:b3:cc:f8:32:dc
4846	2015-11-27 16:51:58.100030000	fe80::a00:27ff:febf:ed99	fe80::28ab:78fe:a753:a582	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2
4951	2015-11-27 16:51:59.437885000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	1086	Redirect is at 68:bc:0c:be:1b:c2
4964	2015-11-27 16:51:59.504296000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
5013	2015-11-27 16:52:00.078761000	fe80::a00:27ff:febf:ed99	fe80::dc85:3d4c:acac:c1a5	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2
5037	2015-11-27 16:52:00.283036000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	1294	Redirect is at 68:bc:0c:be:1b:c2
5045	2015-11-27 16:52:00.390952000	fe80::a00:27ff:febf:ed99	fe80::a07d:a920:1888:5010	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2
5095	2015-11-27 16:52:01.079416000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
5242	2015-11-27 16:52:02.560277000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
5318	2015-11-27 16:52:03.094371000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2

Frame 4951: 1086 bytes captured on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: Toshiba\_03:bf:26 (b8:eb:23:03:bf:26)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: 2800:68:a:5200:fdfa:ab17:4a62:903b (2800:68:a:5200:fdfa:ab17:4a62:903b)  
 Internet Control Message Protocol v6  
 Type: Redirect (137)

```

0000  b8 eb 23 03 bf 26 08 00 27 bf ed 99 b8 eb 23 03 bf 26 08 00  ..b8..eb..23..03..bf..26..08..00..27..bf..ed..99..b8..eb..23..03..bf..26..08..00
0010  00 00 04 08 3a ff fe 80 00 00 00 00 00 00 00 0a 00  ..00..00..04..08..3a..ff..fe..80..00..00..00..00..00..00..00..00..0a..00
0020  27 ff fe bf ed 99 28 00 00 68 00 0a 52 00 fd fa  ..27..ff..fe..bf..ed..99..28..00..00..68..00..0a..52..00..fd..fa
0030  3b 17 4a 62 90 3b 08 00 00 07 00 00 00 00 fe 80  ..3b..17..4a..62..90..3b..08..00..00..07..00..00..00..00..fe..80
0040  00 00 00 00 00 00 00 00 00 00 52 00 00 01 26 07  ..00..00..00..00..00..00..00..00..00..00..52..00..00..01..26..07
0050  fe b8 40 04 08 07 00 00 00 00 00 10 00 02 01  ..fe..b8..40..04..08..07..00..00..00..00..10..00..02..01
0060  08 bc 0c be 1b c2 04 70 00 00 00 00 00 00 00 00  ..08..bc..0c..be..1b..c2..04..70..00..00..00..00..00..00..00..00
  
```

2015-11-27 16:51:06.561	diego-VirtualBox	11/27-16:51:06.326419 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::118b:12f3:bd99:3197 -> fe80::5200:1
2015-11-27 16:51:05.462	diego-VirtualBox	11/27-16:51:05.334095 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::b516:ca19:98ca:273 -> fe80::5200:1
2015-11-27 16:51:05.462	diego-VirtualBox	11/27-16:51:05.333638 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::b516:ca19:98ca:273
2015-11-27 16:51:03.462	diego-VirtualBox	11/27-16:51:03.422228 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::9e5:3439:63ca:385a -> fe80::5200:1
2015-11-27 16:51:03.361	diego-VirtualBox	11/27-16:51:03.263994 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::16cc:20ff:fe85:9f47
2015-11-27 16:51:01.261	diego-VirtualBox	11/27-16:51:01.105675 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::7d4f:6dd9:dc0d:c95c -> fe80::5200:1
2015-11-27 16:51:01.261	diego-VirtualBox	11/27-16:51:01.106664 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::7d4f:6dd9:dc0d:c95c



```

2015-11-27 17:04:02.661      diego-VirtualBox
11/27-17:04:02.518006 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> fe80::5200:1

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270597 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:fdfa:ab17:4ae2:903b

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270598 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] 2800:68:a:5200:fdfa:ab17:4ae2:903b -> fe80::a00:27ff:febf:ed99

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270591 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::a00:27ff:febf:ed99 -> 2800:68:a:5200:fdfa:ab17:4ae2:903b

2015-11-27 17:04:01.361      diego-VirtualBox
11/27-17:04:01.270598 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] 2800:68:a:5200:fdfa:ab17:4ae2:903b -> fe80::a00:27ff:febf:ed99

2015-11-27 17:04:00.761      diego-VirtualBox
11/27-17:04:00.625835 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::ddf6:68f6:b486:2c80

2015-11-27 17:04:00.761      diego-VirtualBox
11/27-17:04:00.626084 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::ddf6:68f6:b486:2c80 -> fe80::5200:1

```

## Prueba 7 atk6-parasite6 -I -H eth0

The screenshot shows a Wireshark capture of network traffic. The filter is set to 'icmpv6.type==137'. The packet list pane shows several ICMPv6 Redirect messages (type 137) from source 2800:68:a:5200:fdfa:ab17:4ae2:903b to destination fe80::a00:27ff:febf:ed99. The packet details pane shows the structure of an Internet Control Message Protocol v6 Redirect message, including fields like 'Type: Redirect (137)', 'Code: 0', and 'Destination Address: fe80::a00:27ff:febf:ed99'.

```

2015-11-27 17:02:46.1      diego-VirtualBox
11/27-17:02:46.453235 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::dc85:3d4c:acac:c1a5

2015-11-27 17:02:46.1      diego-VirtualBox
11/27-17:02:46.453246 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::dc85:3d4c:acac:c1a5 -> fe80::5200:1

2015-11-27 17:00:36.1      diego-VirtualBox
11/27-17:00:36.324897 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::fc46:18c6:c2cf:c3f3

2015-11-27 17:00:36.1      diego-VirtualBox
11/27-17:00:36.325565 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::fc46:18c6:c2cf:c3f3 -> fe80::5200:1

2015-11-27 17:00:26.1      diego-VirtualBox
11/27-17:00:26.222252 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::d3d:6188:9966:d26 -> fe80::5200:1

2015-11-27 17:00:06.1      diego-VirtualBox
11/27-17:00:06.969694 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80::128ab:78fe:a753:a582

2015-11-27 17:00:06.1      diego-VirtualBox
11/27-17:00:06.970004 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::128ab:78fe:a753:a582 -> fe80::5200:1

```



## Prueba 8 atk6-parasite6 -I -R -F -H

No.	Time	Source	Destination	Protocol	Length	Info
4725	2015-11-27 17:25:09.758812000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
5044	2015-11-27 17:25:14.335121000	fe80::a00:27ff:febf:ed99	fe80::3d3d:6188:99e6:d26	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2
5317	2015-11-27 17:25:18.282405000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:bd0b:ab99:4a8a:9f0b	ICMPv6	198	Redirect is at 68:bc:0c:be:1b:c2
5358	2015-11-27 17:25:18.680460000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
5477	2015-11-27 17:25:20.026894000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2
5484	2015-11-27 17:25:20.092530000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	166	Redirect is at 68:bc:0c:be:1b:c2
5487	2015-11-27 17:25:20.092570000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	696	Redirect is at 68:bc:0c:be:1b:c2
5497	2015-11-27 17:25:20.159672000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	214	Redirect is at 68:bc:0c:be:1b:c2
5500	2015-11-27 17:25:20.160587000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	326	Redirect is at 68:bc:0c:be:1b:c2
5503	2015-11-27 17:25:20.160612000	fe80::a00:27ff:febf:ed99	2800:68:a:5200:fdfa:ab17:4a62:903b	ICMPv6	1286	Redirect is at 68:bc:0c:be:1b:c2
5637	2015-11-27 17:25:21.689540000	fe80::a00:27ff:febf:ed99	fe80::b801:a598:6a37:26a1	ICMPv6	182	Redirect is at 68:bc:0c:be:1b:c2

```
2015-11-27 17:24:03.061 diego-VirtualBox
11/27-17:24:03.002708 [**] [1:127611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::28fe:f610:210a:575c -> fe80::5200:1

2015-11-27 17:24:03.061 diego-VirtualBox
11/27-17:24:03.002494 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPV6-ICMP] fe80::5
200:1 -> fe80::28fe:f610:210a:575c

2015-11-27 17:24:02.961 diego-VirtualBox
11/27-17:24:02.867663 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPV6-ICMP] fe80::a
07d:a920:1888:5010 -> fe80::5200:1

2015-11-27 17:24:00.961 diego-VirtualBox
11/27-17:24:00.889574 [**] [1:127611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::ddf6:68f6:b486:2c80 -> fe80::5200:1

2015-11-27 17:24:00.961 diego-VirtualBox
11/27-17:24:00.889344 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPV6-ICMP] fe80::5
200:1 -> fe80::ddf6:68f6:b486:2c80

2015-11-27 17:24:00.562 diego-VirtualBox
11/27-17:24:00.519446 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPV6-ICMP] fe80::5
200:1 -> fe80::dc85:3d4c:acac:c1a5

2015-11-27 17:24:00.562 diego-VirtualBox
11/27-17:24:00.519441 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::dc85:3d4c:acac:c1a5 -> fe80::5200:1
```

## Prueba 9 atk6-fake\_router6 eth0 2001:db8:bad::/64

No.	Time	Source	Destination	Protocol	Length	Info
10235	2015-11-27 17:35:46.834674000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
10692	2015-11-27 17:35:51.835012000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
11182	2015-11-27 17:35:56.691985000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 68:bc:0c:be:1b:c2
11498	2015-11-27 17:35:56.835710000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
12734	2015-11-27 17:36:01.836090000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
13222	2015-11-27 17:36:06.836531000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
13815	2015-11-27 17:36:11.836987000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
14254	2015-11-27 17:36:16.836997000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
14631	2015-11-27 17:36:21.837271000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99
14702	2015-11-27 17:36:22.691819000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 68:bc:0c:be:1b:c2
15553	2015-11-27 17:36:26.837566000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	214	Router Advertisement from 08:00:27:bf:ed:99



```

2015-11-27 17:35:06.062      diego-VirtualBox
11/27-17:35:06.001019 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::2d8b:eaf:325a:c847 -> fe80::5200:1

2015-11-27 17:35:05.063      diego-VirtualBox
11/27-17:35:04.945838 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::c483:fbcd:395f:797f -> fe80::5200:1

2015-11-27 17:35:05.063      diego-VirtualBox
11/27-17:35:04.944091 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::c483:fbcd:395f:797f

2015-11-27 17:35:04.765      diego-VirtualBox
11/27-17:35:04.567014 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::c4aa:f553:107:82da -> fe80::5200:1

2015-11-27 17:35:04.765      diego-VirtualBox
11/27-17:35:04.567002 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::c4aa:f553:107:82da

2015-11-27 17:35:01.061      diego-VirtualBox
11/27-17:35:00.995063 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::2dbb:eaf:325a:c847 -> fe80::5200:1

2015-11-27 17:35:00.661      diego-VirtualBox
11/27-17:35:00.625719 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::4997:2081:24e2:a5a2 -> fe80::5200:1

```

## Prueba 10 atk6-fake\_router6 -H eth0 2001:db8:bad::/64

Filter: icmpv6 and ipv6.addr==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
2920	2015-11-27 17:44:30.851299000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from us:00:42:101:ea:99
3000	2015-11-27 17:44:35.851567000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99
3098	2015-11-27 17:44:37.180469000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 08:bc:0c:be:1b:c2
3444	2015-11-27 17:44:40.851859000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99
4017	2015-11-27 17:44:45.852219000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99
4244	2015-11-27 17:44:50.852548000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99
4457	2015-11-27 17:44:55.853011000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99
4641	2015-11-27 17:45:00.853600000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99
4759	2015-11-27 17:45:03.178749000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 08:bc:0c:be:1b:c2
5091	2015-11-27 17:45:05.853879000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99
5745	2015-11-27 17:45:10.854372000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	222	Router Advertisement from 08:00:27:bf:ed:99

Frame 3444: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)

Internet Control Message Protocol v6  
 Type: Router Advertisement (134)

```

0030  00 00 00 00 00 01 32 00 00 00 00 00 00 00 00 00 00 00 00 00
0040  c5 59 ff 08 08 00 00 00 00 00 00 00 04 00 06 01 .....
0050  00 00 00 00 05 dc 03 04 40 c0 11 11 11 04 00 .....
0060  24 04 00 00 00 00 20 01 01 09 0b ed 00 00 00 00 .....
0070  00 00 00 00 00 01 01 08 00 27 bf ed 99 18 03 .....
0080  00 08 00 00 11 11 00 00 00 00 00 00 00 00 00 .....
0090  00 00 00 00 00 18 03 08 08 00 00 11 11 20 01 .....

```

```

2015-11-27 17:44:00.063      diego-VirtualBox
11/27-17:43:59.700589 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2880:68:a:5200:bd0b:ab99:488a:9f0b

2015-11-27 17:44:00.063      diego-VirtualBox
11/27-17:43:59.700597 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2880:68:a:5200:bd0b:ab99:488a:9f0b

2015-11-27 17:44:00.063      diego-VirtualBox
11/27-17:43:59.700593 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2880:68:a:5200:bd0b:ab99:488a:9f0b

2015-11-27 17:44:00.063      diego-VirtualBox
11/27-17:43:59.700595 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2880:68:a:5200:bd0b:ab99:488a:9f0b

2015-11-27 17:44:00.063      diego-VirtualBox
11/27-17:43:59.700602 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2880:68:a:5200:bd0b:ab99:488a:9f0b

2015-11-27 17:44:00.062      diego-VirtualBox
11/27-17:43:59.700573 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2880:68:a:5200:bd0b:ab99:488a:9f0b

2015-11-27 17:44:00.062      diego-VirtualBox
11/27-17:43:59.700586 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> 2880:68:a:5200:bd0b:ab99:488a:9f0b

```

## Prueba 11 atk6-fake\_router6 -D eth0 2001:db8:bad::/64

Filter: `icmpv6 and ipv6.addr==ff02::1`

No.	Time	Source	Destination	Protocol	Length	Info
5	2015-11-27 18:12:47.306792000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
156	2015-11-27 18:12:52.308212000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
256	2015-11-27 18:12:57.308748000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
430	2015-11-27 18:13:02.309387000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
594	2015-11-27 18:13:07.309771000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
725	2015-11-27 18:13:12.310298000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
889	2015-11-27 18:13:17.310798000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
1026	2015-11-27 18:13:22.311321000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
1147	2015-11-27 18:13:27.311485000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	494	Router Advertisement from 08:00:27:bf:ed:99
1216	2015-11-27 18:13:28.891054000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 68:bc:0c:be:1bc:2
1514	2015-11-27 18:13:32.828916000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 68:bc:0c:be:1bc:2

Frame 5: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Router Advertisement (134)

```

2015-11-27 18:10:24.362      diego-VirtualBox
11/27-18:10:24.315623 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::a00:27ff:febf:ed99 -> fe80::1925:1250:510a:3ed5

2015-11-27 18:10:12.963      diego-VirtualBox
11/27-18:10:12.969032 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::5cc:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99

2015-11-27 18:10:12.963      diego-VirtualBox
11/27-18:10:12.899646 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80:a
00:27ff:febf:ed99 -> fe80::5cc:e24e:3af9:dd1d

2015-11-27 18:10:12.963      diego-VirtualBox
11/27-18:10:12.969039 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::5cc:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99

2015-11-27 18:10:12.962      diego-VirtualBox
11/27-18:10:12.899636 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80:a
00:27ff:febf:ed99 -> fe80::5cc:e24e:3af9:dd1d

2015-11-27 18:10:08.161      diego-VirtualBox
11/27-18:10:07.889648 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
c6:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99

2015-11-27 18:10:08.161      diego-VirtualBox
11/27-18:10:07.889653 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
c6:e24e:3af9:dd1d -> fe80::a00:27ff:febf:ed99
  
```

## Prueba 12 atk6-fake\_router6 -F eth0 2001:db8:bad::/64

Filter: `icmpv6 and ipv6.addr==ff02::1`

No.	Time	Source	Destination	Protocol	Length	Info
69	2015-11-27 18:16:19.909609000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
186	2015-11-27 18:16:24.910148000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
299	2015-11-27 18:16:29.911463000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
400	2015-11-27 18:16:34.911799000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
524	2015-11-27 18:16:39.421863000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 68:bc:0c:be:1bc:2
563	2015-11-27 18:16:39.912107000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]
754	2015-11-27 18:16:44.912642000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	80	Router Advertisement[Malformed Packet]

Frame 186: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 [Malformed Packet: ICMPv6]  
 [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]

## Prueba 13 atk6-fake\_router6 -H -D eth0 2001:db8:bad::/64

No.	Time	Source	Destination	Protocol	Length	Info
96	2015-11-27 18:26:37.092956000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	502	Router Advertisement from 08:00:27:bf:ed:99
198	2015-11-27 18:26:42.093724000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	502	Router Advertisement from 08:00:27:bf:ed:99
287	2015-11-27 18:26:47.093999000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	502	Router Advertisement from 08:00:27:bf:ed:99
406	2015-11-27 18:26:52.094519000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	502	Router Advertisement from 08:00:27:bf:ed:99
420	2015-11-27 18:26:52.194628000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 08:bc:0c:be:1b:c2
550	2015-11-27 18:26:57.095074000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	502	Router Advertisement from 08:00:27:bf:ed:99

Frame 287: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Router Advertisement (134)

```

2015-11-27 18:24:13.462      diego-VirtualBox
11/27-18:24:13.299354 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPv6-ICMP] fe80::3d3d:6188:99e6:d26 -> fe80::5200:1

2015-11-27 18:24:10.661      diego-VirtualBox
11/27-18:24:10.562419 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPv6-ICMP] fe80::1925:2250:510a:3ed5 -> fe80::5200:1

2015-11-27 18:24:10.661      diego-VirtualBox
11/27-18:24:10.562142 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5
200:1 -> fe80::1925:2250:510a:3ed5

2015-11-27 18:24:08.361      diego-VirtualBox
11/27-18:24:08.295414 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::3
d3d:6188:99e6:d26 -> fe80::5200:1

2015-11-27 18:24:07.461      diego-VirtualBox
11/27-18:24:07.357948 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPv6-ICMP] fe80::38b2:170a:9bc6:eb3b -> fe80::5200:1

2015-11-27 18:24:07.461      diego-VirtualBox
11/27-18:24:07.356971 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5
200:1 -> fe80::38b2:170a:9bc6:eb3b

2015-11-27 18:24:05.761      diego-VirtualBox
11/27-18:24:05.562868 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::1
925:2250:510a:3ed5 -> fe80::5200:1
  
```

## Prueba 14 atk6-flood\_advertise6 eth0

No.	Time	Source	Destination	Protocol	Length	Info
371	2015-12-14 18:53:03.127621000	fe80::218:cfff:fe39:2234	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:cfff:fe39:2234 (ov
372	2015-12-14 18:53:03.127646000	fe80::218:4cfff:fe5c:ee04	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:4cfff:fe5c:ee04 (ov
373	2015-12-14 18:53:03.127667000	fe80::218:fefff:fe7c:d3eb	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:fefff:fe7c:d3eb (ov
374	2015-12-14 18:53:03.127687000	fe80::218:cfff:fe8:88c6	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:cfff:fe8:88c6 (ov
375	2015-12-14 18:53:03.127768000	fe80::218:bfff:fe6f:93da	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:bfff:fe6f:93da (ov
376	2015-12-14 18:53:03.127957000	fe80::218:60ff:fe01:6861	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:60ff:fe01:6861 (ov
377	2015-12-14 18:53:03.128019000	fe80::218:98ff:fe9f:4bb3	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:98ff:fe9f:4bb3 (ov
378	2015-12-14 18:53:03.128077000	fe80::218:2fff:feb3:f4d1	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:2fff:feb3:f4d1 (ovr
379	2015-12-14 18:53:03.128134000	fe80::218:edff:fe17:539	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:edff:fe17:539 (ovr
380	2015-12-14 18:53:03.128191000	fe80::218:83ff:fe3:3d79	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:83ff:fe3:3d79 (ov
381	2015-12-14 18:53:03.128246000	fe80::218:6fff:fe10:643a	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:6fff:fe10:643a (ov

Frame 371: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0  
 Ethernet II, Src: BaldrE\_L\_39:22:34 (00:18:cfc3:99:22:34), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::218:cfff:fe39:2234 (fe80::218:cfff:fe39:2234), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6

```

2015-12-14 18:53:12.912      diego-VirtualBox
12/14-18:53:12.777914 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} f
e80::218:dff:fea3:d8ae -> ff02::1

2015-12-14 18:53:12.912      diego-VirtualBox
12/14-18:53:12.777919 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} f
e80::218:dff:fea3:d8ae -> ff02::1

2015-12-14 18:53:12.912      diego-VirtualBox
12/14-18:53:12.777921 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} f
e80::218:dff:fea3:d8ae -> ff02::1

2015-12-14 18:53:12.912      diego-VirtualBox
12/14-18:53:12.777923 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} f
e80::218:dff:fea3:d8ae -> ff02::1

2015-12-14 18:53:12.912      diego-VirtualBox
12/14-18:53:12.777952 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} f
e80::218:1bfff:fe62:6841 -> ff02::1

2015-12-14 18:53:12.912      diego-VirtualBox
12/14-18:53:12.778092 [**] [1:24294:2] PROTOCOL-ICMP IPv6 neighbor advertisement flood attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} f
e80::218:cfff:fe39:2234 -> ff02::1

2015-12-14 18:53:12.691      diego-VirtualBox
12/14-18:53:12.612637 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::bc25:c519:b603:6c8e -> fe80::5200:1

```

## Prueba 15 atk6-flood\_solicitatie6 eth0

The screenshot shows a Wireshark capture of network traffic. The filter is set to `icmpv6 and ipv6.addr==ff02::1`. The packet list shows several Neighbor Solicitation (NS) packets from source `fe80::218:13ff:fe29:e3af` to destination `ff02::1`. The selected packet (No. 1285) is expanded to show the packet bytes and the packet details pane. The details pane shows the packet type as Neighbor Solicitation (135) and the destination address as `ff02::1`.

```

2015-12-14 18:59:14.489      diego-VirtualBox
12/14-18:59:14.395160 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::2
18:b7ff:fe4a:3c45 -> ff02::1

2015-12-14 18:59:14.489      diego-VirtualBox
12/14-18:59:14.395175 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::2
18:b7ff:fe4a:3c45 -> ff02::1

2015-12-14 18:59:14.489      diego-VirtualBox
12/14-18:59:14.395176 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::2
18:b7ff:fe4a:3c45 -> ff02::1

2015-12-14 18:59:14.489      diego-VirtualBox
12/14-18:59:14.395023 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::2
18:13ff:fe29:e3af -> ff02::1

2015-12-14 18:59:14.396      diego-VirtualBox
12/14-18:59:14.292869 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::852c:31e4:1cd5:b4e4 -> fe80::fd98:710d:4461:5c32

2015-12-14 18:59:14.396      diego-VirtualBox
12/14-18:59:14.290347 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::852c:31e4:1cd5:b4e4 -> fe80::f40a:52a:2f79:bde5

2015-12-14 18:59:14.396      diego-VirtualBox
12/14-18:59:14.292874 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] {IPV6-ICMP} fe80::f40a:52a:2f79:bde5 -> fe80::852c:31e4:1cd5:b4e4

```

## Prueba 16 atk6-flood\_router6 eth0

Wireshark capture showing a flood of ICMPv6 Router Advertisement messages. The filter is set to `icmpv6 and ipv6.addr==ff02::1`. The table below shows the captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
220	2015-12-14 20:19:02.945502000	fe80::218:c3ff:fe9f:4529	ff02::1	ICMPv6	118	Router Advertisement from 00:18:c3:9f:45:29
221	2015-12-14 20:19:02.945549000	fe80::218:12ff:fe45:779e	ff02::1	ICMPv6	118	Router Advertisement from 00:18:12:45:77:9e
222	2015-12-14 20:19:02.945591000	fe80::218:a5ff:fe74:22d2	ff02::1	ICMPv6	118	Router Advertisement from 00:18:a5:74:22:d2
223	2015-12-14 20:19:02.945641000	fe80::218:acff:fe3d:c2f1	ff02::1	ICMPv6	118	Router Advertisement from 00:18:ac:3d:c2:f1
224	2015-12-14 20:19:02.945689000	fe80::218:55ff:fe8b:72cc	ff02::1	ICMPv6	118	Router Advertisement from 00:18:55:d8:72:cc
225	2015-12-14 20:19:02.946742000	fe80::218:5dff:fe61:b80	ff02::1	ICMPv6	118	Router Advertisement from 00:18:5d:61:0b:80
230	2015-12-14 20:19:02.946909000	fe80::218:eff:fe71:7b1	ff02::1	ICMPv6	118	Router Advertisement from 00:18:ef:71:07:b1
231	2015-12-14 20:19:02.946990000	fe80::218:31ff:fedc:64a3	ff02::1	ICMPv6	118	Router Advertisement from 00:18:31:dc:64:a3
232	2015-12-14 20:19:02.947075000	fe80::218:52ff:fe5d:a55d	ff02::1	ICMPv6	118	Router Advertisement from 00:18:52:5d:a5:5d
233	2015-12-14 20:19:02.947146000	fe80::218:f5ff:fe95:84fc	ff02::1	ICMPv6	118	Router Advertisement from 00:18:f5:95:84:fc
234	2015-12-14 20:19:02.947213000	fe80::218:9eff:fe1c:d1fd	ff02::1	ICMPv6	118	Router Advertisement from 00:18:9e:1c:d1:fd

Frame 220: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0  
Ethernet II, Src: Cs\_9f:45:29 (00:18:c3:9f:45:29), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
Internet Protocol Version 6, Src: fe80::218:c3ff:fe9f:4529 (fe80::218:c3ff:fe9f:4529), Dst: ff02::1 (ff02::1)  
Internet Control Message Protocol v6  
Type: Router Advertisement (134)

```
2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546050 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:12ff:fe45:779e -> ff02::1

2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546054 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:12ff:fe45:779e -> ff02::1

2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546055 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPv6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:12ff:fe45:779e -> ff02::1

2015-12-14 20:19:11.579 diego-VirtualBox
12/14-20:19:11.546029 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2]
{IPV6-ICMP} fe80::218:c3ff:fe9f:4529 -> ff02::1

2015-12-14 20:19:11.078 diego-VirtualBox
12/14-20:19:11.027270 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe98:esb6

2015-12-14 20:19:11.078 diego-VirtualBox
12/14-20:19:11.027273 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe98:esb6

2015-12-14 20:19:11.078 diego-VirtualBox
12/14-20:19:11.032413 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe99:esb6
```

## Prueba 17 atk6-flood\_router6 -F eth0

Wireshark capture showing a flood of ICMPv6 Router Advertisement messages. The filter is set to `icmpv6 and ipv6.addr==ff02::1`. The table below shows the captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
862	2015-12-14 20:26:01.921054000	fe80::218:86ff:fea9:a4ae	ff02::1	ICMPv6	126	Router Advertisement from 00:18:86:a9:a4:ae
863	2015-12-14 20:26:01.921190000	fe80::218:47ff:feee:6a09	ff02::1	ICMPv6	126	Router Advertisement from 00:18:47:ee:6a:09
864	2015-12-14 20:26:01.921190000	fe80::218:b3ff:fed9:2bb4	ff02::1	ICMPv6	126	Router Advertisement from 00:18:b3:d9:2b:b4
865	2015-12-14 20:26:01.921266000	fe80::218:f2ff:fe5f:f996	ff02::1	ICMPv6	126	Router Advertisement from 00:18:f2:5f:f9:96
866	2015-12-14 20:26:01.921333000	fe80::218:86ff:fe35:45f0	ff02::1	ICMPv6	126	Router Advertisement from 00:18:86:35:45:f0
867	2015-12-14 20:26:01.921400000	fe80::218:ff:fe9e:a32b	ff02::1	ICMPv6	126	Router Advertisement from 00:18:00:9e:a3:2b
868	2015-12-14 20:26:01.921466000	fe80::218:71ff:fe78:20b8	ff02::1	ICMPv6	126	Router Advertisement from 00:18:71:78:20:b8
869	2015-12-14 20:26:01.921534000	fe80::218:cfff:fe83:7814	ff02::1	ICMPv6	126	Router Advertisement from 00:18:cf:c8:78:14
870	2015-12-14 20:26:01.921604000	fe80::218:f5ff:fe11:d98	ff02::1	ICMPv6	126	Router Advertisement from 00:18:f5:f1:d9:8
871	2015-12-14 20:26:01.921672000	fe80::218:c5ff:fe2c:2ce5	ff02::1	ICMPv6	126	Router Advertisement from 00:18:c5:f2:2c:e5
872	2015-12-14 20:26:01.921794000	fe80::218:f5ff:fe83:1c6d	ff02::1	ICMPv6	126	Router Advertisement from 00:18:f5:83:1c:6d

Frame 862: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0  
Ethernet II, Src: El\_Tech\_a9:a4:ae (00:18:86:a9:a4:ae), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
Internet Protocol Version 6, Src: fe80::218:86ff:fea9:a4ae (fe80::218:86ff:fea9:a4ae), Dst: ff02::1 (ff02::1)  
Internet Control Message Protocol v6  
Type: Router Advertisement (134)

2015-12-14 20:26:10.680	diego-VirtualBox
12/14-20:26:10.535285 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2] {IPV6-ICMP} fe80::218:b3ff:fed9:2bb4 -> ff02::1	
2015-12-14 20:26:10.680	diego-VirtualBox
12/14-20:26:10.535286 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2] {IPV6-ICMP} fe80::218:b3ff:fed9:2b04 -> ff02::1	
2015-12-14 20:26:10.680	diego-VirtualBox
12/14-20:26:10.535288 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2] {IPV6-ICMP} fe80::218:f2ff:fe5f:f996 -> ff02::1	
2015-12-14 20:26:10.680	diego-VirtualBox
12/14-20:26:10.534979 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPv6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2] {IPV6-ICMP} fe80::218:47ff:feee:6a09 -> ff02::1	
2015-12-14 20:26:10.680	diego-VirtualBox
12/14-20:26:10.535287 [**] [1:23178:6] PROTOCOL-ICMP IPv6 router advertisement flood attempt [**] [Classification: Attempted Denial of Service] [Priority: 2] {IPV6-ICMP} fe80::218:f2ff:fe5f:f996 -> ff02::1	
2015-12-14 20:26:10.680	diego-VirtualBox
12/14-20:26:10.534667 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPv6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2] {IPV6-ICMP} fe80::218:82ff:fe65:19 -> ff02::1	
2015-12-14 20:26:10.680	diego-VirtualBox
12/14-20:26:10.534948 [**] [1:2014996:3] ET DOS Microsoft Windows 7 ICMPv6 Router Advertisement Flood [**] [Classification: Attempted Denial of Service] [Priority: 2] {IPV6-ICMP} fe80::218:86ff:fe99:84ae -> ff02::1	
2015-12-14 20:26:09.805	diego-VirtualBox
12/14-20:26:09.572282 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::a00:27ff:fe38:56ce	

## Prueba 18 atk6-flood\_rs6 eth0

The screenshot shows a Wireshark capture of network traffic on interface eth0. The filter is set to 'icmpv6 and ipv6.addr==ff02::1'. The packet list pane shows a series of ICMPv6 Router Advertisement packets from source fe80::5200:1 to destination ff02::1. The packet details pane shows the structure of an ICMPv6 Router Advertisement message, including fields like M, S, O, P, and R.

No.	Time	Source	Destination	Protocol	Length	Info
2096	2015-12-14 19:10:00.660142000	fe80::5200:1	ff02::1	ICMPv6	118	Router Advertisement from 08:00:27:bf:ed:99
2198	2015-12-14 19:10:00.660492000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2199	2015-12-14 19:10:00.660521000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2140	2015-12-14 19:10:00.660521000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2141	2015-12-14 19:10:00.660587000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2142	2015-12-14 19:10:00.660657000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2144	2015-12-14 19:10:00.660750000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2145	2015-12-14 19:10:00.660847000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2146	2015-12-14 19:10:00.660916000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2147	2015-12-14 19:10:00.660983000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2148	2015-12-14 19:10:00.661053000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99

2015-12-14 19:10:04.977	diego-VirtualBox
12/14-19:10:04.862963 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] {IPV6-ICMP} fe80::c982:1761:7aa8:67f0 -> fe80::5200:1	
2015-12-14 19:10:04.977	diego-VirtualBox
12/14-19:10:04.862842 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::c982:1761:7aa8:67f0	
2015-12-14 19:10:04.878	diego-VirtualBox
12/14-19:10:04.757743 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::d32c:f451:deb2 -> fe80::5200:1	
2015-12-14 19:10:03.376	diego-VirtualBox
12/14-19:10:03.308879 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::c982:1761:7aa8:67f0	
2015-12-14 19:10:02.177	diego-VirtualBox
12/14-19:10:02.164794 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::d32c:f451:deb2 -> fe80::5200:1	
2015-12-14 19:10:02.077	diego-VirtualBox
12/14-19:10:01.984283 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::d4e:7e3a:ec4f:c769 -> fe80::5200:1	
2015-12-14 19:10:01.576	diego-VirtualBox
12/14-19:10:01.475736 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::86e:71f6:b59:1e68 -> fe80::5200:1	
2015-12-14 19:10:01.176	diego-VirtualBox
12/14-19:10:01.104096 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5200:1 -> fe80::1f5:35f:fff7:a46c -> fe80::5200:1	



## Prueba 19 atk6-flood\_rs6 -s eth0

Filter: icmpv6 and ipv6.addr==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
2897	2015-12-14 19:14:01.984772000	fe80::a00:27ff:fe9a:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2898	2015-12-14 19:14:01.984787000	fe80::a00:27ff:fe9b:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2899	2015-12-14 19:14:01.984800000	fe80::a00:27ff:fe9c:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2900	2015-12-14 19:14:01.984812000	fe80::a00:27ff:fe9d:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2901	2015-12-14 19:14:01.984825000	fe80::a00:27ff:fe9e:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2902	2015-12-14 19:14:01.984837000	fe80::a00:27ff:fe9f:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2903	2015-12-14 19:14:01.984850000	fe80::a00:27ff:fea0:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2904	2015-12-14 19:14:01.984925000	fe80::a00:27ff:fea1:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2905	2015-12-14 19:14:01.984968000	fe80::a00:27ff:fea2:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2906	2015-12-14 19:14:01.985040000	fe80::a00:27ff:fea3:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99
2907	2015-12-14 19:14:01.985105000	fe80::a00:27ff:fea4:34b6	ff02::1	ICMPv6	70	Router Solicitation from 08:00:27:bf:ed:99

Frame 2897: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0  
 Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:fe9a:34b6 (fe80::a00:27ff:fe9a:34b6), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Router Solicitation (133)

```

0000 33 33 00 00 00 01 08 00 27 bf ed 99 86 dd 60 00 33.....
0010 00 00 00 10 3a ff fe 80 00 00 00 00 00 0a 00 .....
0020 27 ff fe 9a 34 b6 ff 02 00 00 00 00 00 00 00 ...4.....
0030 00 00 00 00 00 01 85 00 19 85 00 00 00 01 01 .....
0040 08 00 27 bf ed 99
  
```

```

2015-12-14 19:14:00.876 diego-VirtualBox
12/14-19:14:00.831627 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::f40a:52a:2f79:bde5 -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876 diego-VirtualBox
12/14-19:14:00.831647 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::fd98:710d:4461:5c32 -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876 diego-VirtualBox
12/14-19:14:00.830006 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::48e4:1db2:aefe:51ef -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876 diego-VirtualBox
12/14-19:14:00.829212 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::4997:2001:24e2:a5a2 -> fe80::48e4:1db2:aefe:51ef

2015-12-14 19:14:00.876 diego-VirtualBox
12/14-19:14:00.831626 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::f40a:52a:2f79:bde5 -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876 diego-VirtualBox
12/14-19:14:00.830005 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::48e4:1db2:aefe:51ef -> fe80::4997:2001:24e2:a5a2

2015-12-14 19:14:00.876 diego-VirtualBox
12/14-19:14:00.829417 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::4997:2001:24e2:a5a2 -> fe80::2ca9:42fc:f1a0:5c7a

2015-12-14 19:14:00.176 diego-VirtualBox
12/14-19:14:00.139648 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack]
[Priority: 2] [IPV6-ICMP] fe80::fd98:710d:4461:5c32 -> fe80::520b:1
  
```

## Prueba 20 atk6-flood\_rs6 -S eth0

Filter: icmpv6 and ipv6.addr==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
249	2015-12-14 19:19:08.811355000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:0b:14:fe:64
250	2015-12-14 19:19:08.811435000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:0c:14:fe:64
251	2015-12-14 19:19:08.811491000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:0d:14:fe:64
252	2015-12-14 19:19:08.811546000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:0e:14:fe:64
253	2015-12-14 19:19:08.811600000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:0f:14:fe:64
254	2015-12-14 19:19:08.811729000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:11:14:fe:64
255	2015-12-14 19:19:08.811810000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:11:14:fe:64
256	2015-12-14 19:19:08.811878000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:12:14:fe:64
257	2015-12-14 19:19:08.811946000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:13:14:fe:64
258	2015-12-14 19:19:08.812016000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:14:14:fe:64
259	2015-12-14 19:19:08.812083000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	70	Router Solicitation from 08:00:15:14:fe:64

Frame 249: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0  
 Ethernet II, Src: Unsysys\_14:fe:64 (08:00:0b:14:fe:64), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
 Internet Control Message Protocol v6  
 Type: Router Solicitation (133)

```

0000 33 33 00 00 00 01 08 00 0b 14 fe 64 86 dd 60 00 33.....
0010 00 00 00 10 3a ff fe 80 00 00 00 00 00 0a 00 .....
0020 27 ff fe bf ed 99 ff 02 00 00 00 00 00 00 00 ...:.....
0030 00 00 00 00 01 85 00 4c 5d 00 00 00 01 01 .....
0040 08 00 0b 14 fe 64
  
```

2015-12-14 19:19:04.176	diego-VirtualBox	12/14-19:19:04.188488 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> fe80::c982:1761:7aa8:67f0
2015-12-14 19:19:03.676	diego-VirtualBox	12/14-19:19:03.588202 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> fe80::6cb2:7e00:6962:6feb
2015-12-14 19:19:03.676	diego-VirtualBox	12/14-19:19:03.615265 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::a0f:e3c8:4515:7a5a -> fe80::5200:1
2015-12-14 19:19:03.676	diego-VirtualBox	12/14-19:19:03.588441 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::6cb2:7e00:6962:6feb -> fe80::5200:1
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126499 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::a080:1b5e:9f9e:fc61 -> fe80::9c1:83dd:d873:13f6
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126670 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::9c1:83dd:d873:13f6 -> fe80::a080:1b5e:9f9e:fc61
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126500 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::a080:1b5e:9f9e:fc61 -> fe80::9c1:83dd:d873:13f6
2015-12-14 19:19:03.176	diego-VirtualBox	12/14-19:19:03.126670 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::9c1:83dd:d873:13f6 -> fe80::a080:1b5e:9f9e:fc61

## Prueba 21 atk6-flood\_rs6 -s -S eth0

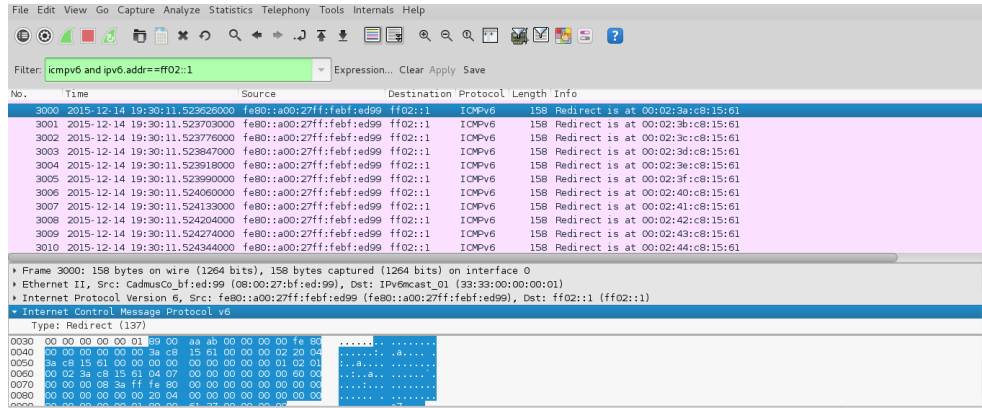
The screenshot shows a Wireshark capture of network traffic. The filter is set to 'icmpv6 and ipv6.addr==ff02::1'. The packet list shows multiple ICMPv6 Router Solicitation packets from source fe80::a00:27ff:fe00:36ce to destination ff02::1. The packet details pane shows the structure of an Internet Control Message Protocol (ICMP) Router Solicitation (133) packet, including the Ethernet II header, Internet Protocol Version 6 header, and the ICMP Router Solicitation payload.

No.	Time	Source	Destination	Protocol	Length	Info
852	2015-12-14 19:25:01.683284000	fe80::a00:27ff:fe00:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:00:36:ce:58
853	2015-12-14 19:25:01.683389000	fe80::a00:27ff:fe01:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:01:36:ce:58
854	2015-12-14 19:25:01.683405000	fe80::a00:27ff:fe02:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:02:36:ce:58
855	2015-12-14 19:25:01.683418000	fe80::a00:27ff:fe03:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:03:36:ce:58
856	2015-12-14 19:25:01.683430000	fe80::a00:27ff:fe04:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:04:36:ce:58
857	2015-12-14 19:25:01.683442000	fe80::a00:27ff:fe05:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:05:36:ce:58
858	2015-12-14 19:25:01.683523000	fe80::a00:27ff:fe06:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:06:36:ce:58
859	2015-12-14 19:25:01.683563000	fe80::a00:27ff:fe07:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:07:36:ce:58
860	2015-12-14 19:25:01.683619000	fe80::a00:27ff:fe08:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:08:36:ce:58
861	2015-12-14 19:25:01.683680000	fe80::a00:27ff:fe09:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:09:36:ce:58
862	2015-12-14 19:25:01.683758000	fe80::a00:27ff:fe0a:36ce	ff02::1	ICMPv6	70	Router Solicitation from 08:00:0a:36:ce:58

2015-12-14 19:21:04.978	diego-VirtualBox	12/14-19:21:04.967650 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> fe80::58e8:2b03:8d0:cbd1
2015-12-14 19:21:03.678	diego-VirtualBox	12/14-19:21:03.617782 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::a080:1b5e:9f9e:fc61 -> fe80::5200:1
2015-12-14 19:21:03.678	diego-VirtualBox	12/14-19:21:03.617154 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> fe80::a080:1b5e:9f9e:fc61
2015-12-14 19:21:03.076	diego-VirtualBox	12/14-19:21:02.938025 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] 2000:68:a:5200:f4a6:2add:868a:1aba -> fe80::5200:1
2015-12-14 19:21:03.076	diego-VirtualBox	12/14-19:21:02.937824 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> 2000:68:a:5200:f4a6:2add:868a:1aba
2015-12-14 19:21:03.076	diego-VirtualBox	12/14-19:21:03.040874 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> 077:ebe:261:eeb -> fe80::5200:1
2015-12-14 19:21:02.876	diego-VirtualBox	12/14-19:21:02.858028 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> 982:1761:7aa8:67f0 -> fe80::5200:1
2015-12-14 19:21:02.676	diego-VirtualBox	12/14-19:21:02.569051 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::200:1 -> fe80::581f:52ad:a6d1:4abc



## Prueba 22 atk6-flood\_redir6 eth0

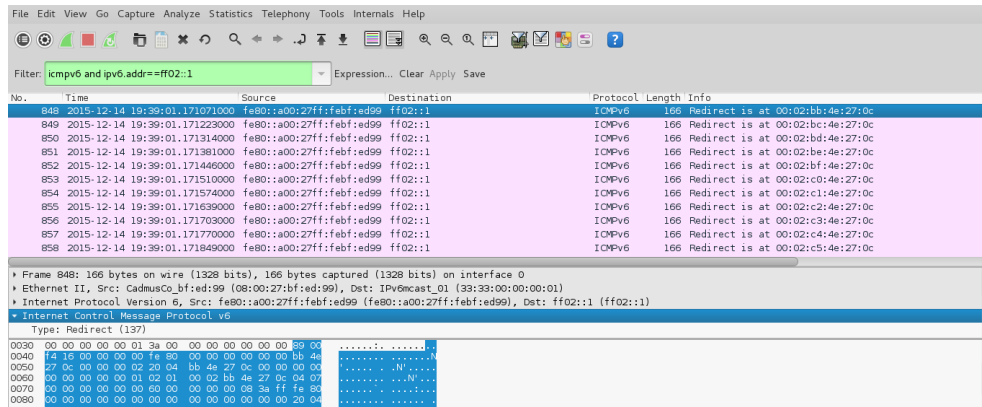


Wireshark capture showing a flood of ICMPv6 Redirect messages. The filter is 'icmpv6 and ipv6.addr==ff02::1'. The table below summarizes the captured packets.

No.	Time	Source	Destination	Protocol	Length	Info
3000	2015-12-14 19:30:11.52926000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:3a:c8:15:61
3001	2015-12-14 19:30:11.529703000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:3b:c8:15:61
3002	2015-12-14 19:30:11.52976000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:3c:c8:15:61
3003	2015-12-14 19:30:11.529847000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:3d:c8:15:61
3004	2015-12-14 19:30:11.529918000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:3e:c8:15:61
3005	2015-12-14 19:30:11.529990000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:3f:c8:15:61
3006	2015-12-14 19:30:11.524060000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:40:c8:15:61
3007	2015-12-14 19:30:11.524133000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:41:c8:15:61
3008	2015-12-14 19:30:11.524204000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:42:c8:15:61
3009	2015-12-14 19:30:11.524274000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:43:c8:15:61
3010	2015-12-14 19:30:11.524344000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	158	Redirect is at 00:02:44:c8:15:61

- 2015-12-14 19:30:59.576 diego-VirtualBox  
12/14-19:30:59.478027 [\*\*] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [\*\*] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::4cb4:5f46:44b8:2922 -> fe80::5280:1
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.233069 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::c54b:d32c:f451:deb2 -> fe80::fd98:710d:4461:5c32
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.233115 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::f40a:52a:2f79:bde5 -> fe80::c54b:d32c:f451:deb2
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.223014 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::c54b:d32c:f451:deb2 -> fe80::f40a:52a:2f79:bde5
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.233068 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::c54b:d32c:f451:deb2 -> fe80::fd98:710d:4461:5c32
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.223014 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::c54b:d32c:f451:deb2 -> fe80::f40a:52a:2f79:bde5
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.233070 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::fd98:710d:4461:5c32 -> fe80::c54b:d32c:f451:deb2
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.233114 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::f40a:52a:2f79:bde5 -> fe80::c54b:d32c:f451:deb2
- 2015-12-14 19:30:58.276 diego-VirtualBox  
12/14-19:30:58.222043 [\*\*] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [\*\*] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] fe80::c54b:d32c:f451:deb2 -> fe80::2ca9:42fc:f1a0:5c7a

## Prueba 23 atk6-flood\_redir6 -H eth0



Wireshark capture showing a flood of ICMPv6 Redirect messages with the host flag set. The filter is 'icmpv6 and ipv6.addr==ff02::1'. The table below summarizes the captured packets.

No.	Time	Source	Destination	Protocol	Length	Info
849	2015-12-14 19:30:01.171071000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:bb:4e:27:c0
849	2015-12-14 19:30:01.171223000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:bc:4e:27:c0
850	2015-12-14 19:30:01.171314000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:bd:4e:27:c0
851	2015-12-14 19:30:01.171381000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:be:4e:27:c0
852	2015-12-14 19:30:01.171446000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:bf:4e:27:c0
853	2015-12-14 19:30:01.171510000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:c0:4e:27:c0
854	2015-12-14 19:30:01.171574000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:c1:4e:27:c0
855	2015-12-14 19:30:01.171639000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:c2:4e:27:c0
856	2015-12-14 19:30:01.171703000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:c3:4e:27:c0
857	2015-12-14 19:30:01.171770000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:c4:4e:27:c0
858	2015-12-14 19:30:01.171849000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:c5:4e:27:c0

```

2015-12-14 19:39:01.476      diego-VirtualBox
12/14-19:39:01.452321 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fedd:b0b6

2015-12-14 19:39:00.676      diego-VirtualBox
12/14-19:39:00.559549 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> 2800:68:a:5200:cd5e:4ce4:6b55:2863

2015-12-14 19:39:00.676      diego-VirtualBox
12/14-19:39:00.559422 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] 2800:68:a:5200:cd5e:4ce4:6b55:2863 -> fe80::5200:1

2015-12-14 19:39:00.476      diego-VirtualBox
12/14-19:39:00.447541 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:feda:70b7

2015-12-14 19:39:00.476      diego-VirtualBox
12/14-19:39:00.436679 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fedd:80b6

2015-12-14 19:39:00.476      diego-VirtualBox
12/14-19:39:00.447352 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fedd:b0b6

2015-12-14 19:39:00.276      diego-VirtualBox
12/14-19:39:00.280980 [**] [1:27611:1] PROTOCOL-ICMP Truncated ICMPv6 denial of service attempt [**] [Classification: Detection of a Denial of Service Attack] [Priority: 2] [IPv6-ICMP] 2800:68:a:5200:c15d:e222:61:600e -> fe80::5200:1

2015-12-14 19:39:00.076      diego-VirtualBox
12/14-19:38:59.996932 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:9d17:f834:80a3:3894

```

## Prueba 24 atk6-flood\_redir6 -F eth0

Filter: icmpv6 and ipv6.addr==ff02::1

No.	Time	Source	Destination	Protocol	Length	Info
855	2015-12-14 19:45:01.527014000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:e9:2d:89:04
856	2015-12-14 19:45:01.527105000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:ea:2d:89:04
857	2015-12-14 19:45:01.527124000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:eb:2d:89:04
858	2015-12-14 19:45:01.527146000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:ec:2d:89:04
859	2015-12-14 19:45:01.527168000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:ed:2d:89:04
860	2015-12-14 19:45:01.527293000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:ee:2d:89:04
861	2015-12-14 19:45:01.527362000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:ef:2d:89:04
862	2015-12-14 19:45:01.527428000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:fo:2d:89:04
863	2015-12-14 19:45:01.527477000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:ff:2d:89:04
864	2015-12-14 19:45:01.527492000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:f2:2d:89:04
865	2015-12-14 19:45:01.527508000	fe80:a00:27ff:fabf:ed99	ff02::1	ICMPv6	166	Redirect is at 00:02:f3:2d:89:04

Frame 855: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0  
Ethernet II, Src: CadmusCoLb,ef:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
Internet Protocol Version 6, Src: fe80:a00:27ff:fabf:ed99 (fe80:a00:27ff:fabf:ed99), Dst: ff02::1 (ff02::1)  
Internet Control Message Protocol v6  
Type: Redirect (137)

```

0030  00 00 00 00 00 01 3a 00 00 00 01 00 00 00 89 0c  .....
0040  88 80 00 00 00 00 fa 80 00 00 00 00 00 e9 2d  .....
0050  89 04 00 00 00 02 2d 04 e9 2d 89 04 00 00 00 00  .....
0060  00 00 00 00 01 02 01 00 02 e9 2d 89 04 04 07  .....
0070  00 00 00 00 00 00 00 00 00 00 08 3a ff fa 85  .....
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 2d  .....
0090  89 04 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

```

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148118 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148125 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148109 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148116 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148120 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148121 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148117 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

2015-12-14 19:46:00.176      diego-VirtualBox
12/14-19:46:00.148122 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] [IPv6-ICMP] fe80::5200:1 -> fe80:a00:27ff:fe9f:31cf

```

# Prueba 25 atk6-flood\_redir6 -H -F eth0

No.	Time	Source	Destination	Protocol	Length	Info
990	2015-12-14 19:51:00.703947000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:46:d9:dc:68
991	2015-12-14 19:51:00.704044000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:47:d9:dc:68
992	2015-12-14 19:51:00.704061000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:48:d9:dc:68
993	2015-12-14 19:51:00.704104000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:49:d9:dc:68
994	2015-12-14 19:51:00.704181000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:4a:d9:dc:68
995	2015-12-14 19:51:00.704248000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:4b:d9:dc:68
996	2015-12-14 19:51:00.704299000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:4c:d9:dc:68
997	2015-12-14 19:51:00.704346000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:4d:d9:dc:68
998	2015-12-14 19:51:00.704362000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:4e:d9:dc:68
999	2015-12-14 19:51:00.704377000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:4f:d9:dc:68
1000	2015-12-14 19:51:00.704392000	fe80::a00:27ff:febf:ed99	ff02::1	ICMPv6	174	Redirect is at 00:02:50:d9:dc:68

Frame 990: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0  
Ethernet II, Src: CadmusCo\_bf:ed:99 (08:00:27:bf:ed:99), Dst: IPv6mcast\_01 (33:33:00:00:00:01)  
Internet Protocol Version 6, Src: fe80::a00:27ff:febf:ed99 (fe80::a00:27ff:febf:ed99), Dst: ff02::1 (ff02::1)  
Internet Control Message Protocol v6  
Type: Redirect (137)

```
2015-12-14 19:51:00.276 diego-VirtualBox
12/14-19:51:00.238808 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe56:2b7

2015-12-14 19:51:00.276 diego-VirtualBox
12/14-19:51:00.240602 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe3e:62ce

2015-12-14 19:51:00.276 diego-VirtualBox
12/14-19:51:00.240603 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe3e:62ce

2015-12-14 19:51:00.276 diego-VirtualBox
12/14-19:51:00.240606 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe3e:62ce

2015-12-14 19:51:00.276 diego-VirtualBox
12/14-19:51:00.241637 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe3e:62ce

2015-12-14 19:51:00.276 diego-VirtualBox
12/14-19:51:00.238942 [**] [1:24303:6] PROTOCOL-ICMP IPv6 multicast neighbor add attempt [**] [Classification: Misc activity] [Priority: 3] {IPV6-ICMP} fe80::5
200:1 -> fe80::a00:27ff:fe3e:82ce
```