METODOLOGÍA DE EVALUACION DE SISTEMA DE DETECCIÓN DE INTRUSOS FRENTE ATAQUES DE SUPLANTACIÓN PROTOCOLO DE RESOLUCION DE DIRECCIONES Y SISTEMA DE NOMBRES DE DOMINIOS

YENIFER RIVAS MORENO
1088306151
DIANA ALEJANDRA AGUIRRE UTIMA
1088310343

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
INGENIERIA
SISTEMAS Y COMPUTACIÓN
PEREIRA, RISARALDA
2017

METODOLOGÍA DE EVALUACION DE SISTEMA DE DETECCIÓN DE INTRUSOS FRENTE ATAQUES DE SUPLANTACIÓN PROTOCOLO DE RESOLUCION DE DIRECCIONES Y SISTEMA DE NOMBRES DE DOMINIOS

YENIFER RIVAS MORENO
1088306151
DIANA ALEJANDRA AGUIRRE UTIMA
1088310343

Trabajo de grado presentado como requisito para optar el título de ingeniera en sistemas y computación

Directora
Ana María de las Mercedes López Echeverry

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
INGENIERIA
SISTEMAS Y COMPUTACIÓN
PEREIRA, RISARALDA
2017

Agradecimientos

Agradecemos a todas las personas que hicieron parte de este proceso, nuestras familias por apoyarnos moral y financieramente, a los profesores por aportar sus conocimiento y hacer que este proyecto fuera posible.

TABLA DE CONTENIDOS

Pág.

1. LISTA DE ILUSTRACIONES

Pág.

2. LISTA DE TABLAS

Pág.

3. INTRODUCCIÓN.

Hoy en día una de las pertenencias más preciadas para las empresas, instituciones, entidades y personas es la información, ya que por medio de esta se realizan todo tipo de procedimientos en la gran mayoría de escenarios en los que se use la tecnología, por lo tanto, se estaría hablando de tecnologías de la información (TI).

Hoy en día las personas se han convertido en dependientes casi totales de la información, proteger esta tiene que ser un punto primordial, evitando por ejemplo que esta se pueda filtrar por medio de las redes usadas para transmitirla gracias a fisuras en la seguridad de estas redes debido a la constante actualización de los sistemas de los cuales se ha ido dependiendo para realizar muchas tareas diarias.

Si se quiere evitar que la información pueda llegar a filtrarse y caer en manos de personas inescrupulosas es necesario fortalecer la seguridad de las redes, por ejemplo, por medio de la caracterización de los dos tipos de productos de seguridad para intrusión en redes que existen: IDS e IPS para saber cuál puede ser más efectivo para lograr este fin.

4. DEFINICION DEL PROBLEMA.

Las empresas pequeñas y medianas cuando realizan un despliegue de red de comunicaciones, deben considerar no sólo elementos a nivel de operación y capacidad de transferencia de datos sino también en términos de seguridad de la información. Dentro de las temáticas relacionadas con seguridad de la información, existe una relacionada con la capacidad de detectar y prevenir intrusiones en la red. Sin embargo, las empresas se enfrentan con la necesidad de seleccionar una herramienta para ser implementada.

Con base en lo anterior, se hace necesario contar con criterios objetivos de selección de herramientas de seguridad tipo IDS e IPS, pero la información que se encuentra a nivel de comparaciones entre productos de seguridad tipo IDS e IPS suele ser sesgada porque la mayoría de estas comparaciones son hechas por los fabricantes de productos comerciales, razón por la cual, es necesario establecer una metodología de comparación que unifique los criterios con los cuales se evalúan los productos y la efectividad de los mismos, y así permitir a las organizaciones proteger sus sistemas de las amenazas que aparecen al incrementar la conectividad en la red y la dependencia que se tiene hacia los sistemas de información.

Por otra parte, uno de los problemas principales de la seguridad corresponde al tiempo que transcurre desde que se descubre una nueva vulnerabilidad y se comenta en diversas listas de seguridad, hasta que las empresas de software comienzan a preparar y desarrollar una forma de contrarrestar este.

Dicho lo anterior se propuso realizar la comparación bajo los parámetros establecidos para la caracterización de los productos de seguridad y establecer un escenario de prueba real en el que se puedan llevar a cabo ataques para validar la respuesta.

5. JUSTIFICACIÓN.

Con el presente proyecto se busca establecer un marco de comparación que unifique los criterios con los cuales se evalúan los productos y la efectividad de los diferentes sistemas de detección de intrusos (IDS), frente ataques de suplantación de protocolo de resolución de direcciones (ARP) y sistema de nombres de dominios (DNS). En donde se pretende contribuir a la sociedad los conocimientos que puede llegar a generar esta investigación sobre los diferentes tipos de IDS que minimizaría los riesgos en la red y crean un entorno más seguro.

Además se espera tener un impacto positivo por parte de los diferentes usuarios ya que se busca tener una efectividad de los diferentes IDS y proporcionar a largo plazo la identificación de los ataques y tráficos por medio de registros que se generan en una red LAN y al mismo tiempo beneficiar de una u otra manera a los , profesores, estudiantes y la comunidad en general fortaleciendo las redes de la planta física de la universidad; sobre una información útil de los tipos de IDS y las vulnerabilidades o brechas de seguridad en una red.

Dicho lo anterior este proyecto se realiza para evaluar y documentar los diferentes ataques de suplantación ARP y DNS donde se busca conocer las amenazas existentes y la efectividad de los tipos de IDS.

6. OBJETIVO GENERAL Y OBJETIVO ESPECÍFICOS.

6.1. General

Diseñar una metodología para la evaluación de sistema de detección de intrusos frente a ataques de suplantación ARP y DNS.

6.2. Específicos

- Documentar los ataques de spoofing típicos en una red LAN típica.

- Documentar herramientas de ataques que implementen los ataques típicos en una red LAN.

- Diseñar una topología de prueba en la que se puedan instalar diferentes IDS y se puedan atacar sin inconvenientes legales.

- Diseñar una estrategia de medición de la efectividad de la detección para cualquier IDS dentro de cada categoría.

- Implementar la estrategia de medición que compara dos productos IDS en la misma categoría.

7. MARCO DE REFERENCIA

7.1 MARCO TEORICO

7.1.1 Sistema de prevención de intrusos

Se encarga de ejercer una monitorización pasiva en la red en el que su propósito principal es analizar el flujo de datos y dependiendo de su contenido, lugar de la dirección IP o puertos el sistema según estas variables toma la decisión de bloquear o no el flujo o los flujos de datos implicados.

7.1.2 Sistema de detección de intrusos

Es el encargado de alertar sobre posibles anomalías en la red o un posterior intento de acceso no permitido, además de tomar acciones frente a estas anomalías como bloquear el acceso del usuario en sospecha.

7.1.2.1 Características

El IDS presenta las siguientes Características[1]:

- Identifica posibles amenazas.
- Registrar la información acerca de la amenaza detectada.
- Informa al administrador y configura los Reuters y firewalls para evitar que el posible intruso puede acceder.
- Este no se encuentra en el camino de la red sino fuera de él.
- Genera alertas y registros de la actividad maliciosa cuando está sucediendo el hecho.
- No puede resolver ataques en la red.
- Avisa al administrador cuando se produjo un ataque.
- Se basa de ciertas reglas predefinidas y los registros de ataques o intrusiones (patrones) para la identificación de ataques.

[1] (Ashoor y Gore, Difference between Intrusion Detection System (IDS) & Intrusion Prevention System (IPS) Pune University, India. Julio de 2011.)

7.1.2.2 Arquitectura

En la arquitectura de los IDS se encontró los siguientes componentes básicos que debería tener[2]:

- Una fuente de información que proporciona eventos del sistema o red informática.
- Una base de datos de patrones de comportamiento considerados como normales, así como de los perfiles de distintos tipos de ataque.
- Un motor de análisis encargado de detectar evidencias de intentos de instrucción.
- Un módulo de respuesta capaz de llevar a cabo determinadas actuaciones a partir de las indicaciones del motor de análisis.

En la arquitectura de los IPS tenemos los siguientes componentes[3]:

- Uno o más sensores colocados estratégicamente para monitorear el flujo particular de ciertos segmentos de la red.

- Una consola de manejo centralizada para monitorear, configurar y mantener todos los sensores.

7.1.2.3 Clasificación

De los IDS encontramos las siguientes clasificaciones[4]:

- En cuanto a tipos de ataques y utilización de recursos.
- En cuanto a la metodología de detección de intrusos.
- En cuanto a lugar y sistemas a monitorear.

[2] (Pablo Muñiz Botello Cholula 2010)
[3] (Scarfone, The basics of network intrusion prevention systems Octubre de 2015)
[4] (Pablo Muñiz Botello Cholula 2010, Cholula Cholula, Puebla, México. 13 de Mayo de 2010)

7.1.2.4 Tipos de sistema de detección de intrusos

Existen dos tipos de sistemas de detección de intrusos:

- Sistema de detección de intrusiones en la Red.
- Sistema de detección de intrusiones en el Host.

7.1.2.4.1 Sistema de detección de intrusiones en la Red

Es un sistema de detección de intrusiones, que se encarga de la seguridad dentro de la red, este IDS funciona como un sniffer el cual escucha todo el tráfico de la red en espera de actividades malintencionadas, como las exploraciones o los ataques de instituciones reales. Normalmente los NIDS se ejecutan en una sola máquina dedicada, dentro o fuera de un cortafuego, para observar los intentos de intrusiones procedentes de internet. Existen diversas formas de clasificar los NIDS:

- por objeto de análisis.
- por situación de los componentes del IDS.
- por tipo de análisis efectuado y la técnica de análisis empleada.

7.1.2.4.1.1 Características

En los NIDS presenta las siguientes características[5]:

- Detectan ataques capturando y analizando los paquetes de red.
- Suelen consistir en un conjunto de host que actúan como sensores cada uno con único propósito
- Los datos de todos estos equipos se envían una consola de control central.
- Protegen mejor los equipos frente a ataques.

[5] (Victor Manuel Mendoza Anaya 2017)

7.1.2.4.1.2 Ventajas

Las ventajas de los NIDS son[6]:

- Con pocos NIDS bien situados se puede controlar una red de gran tamaño.
- El despliegue de la infraestructura de NIDS tiene poco impacto en el funcionamiento de la red.
- Son muy seguros porque se pueden hacer casi invisibles a los atacantes.

7.1.2.4.1.3 Desventajas

Las desventajas de los NIDS son[7]:

- Eficiencia, es difícil analizar todo el tráfico en una red grande y con mucho tráfico.
- No son apropiados para redes conmutadas.
- No pueden analizar información cifrada (VPN).
- No pueden informar si el ataque ha sido o no exitoso.
- Pueden tener problemas con la fragmentación.

7.1.2.4.1.4 Productos comerciales basados en NIDS

Algunos productos comerciales que proponen las empresas para los sistemas de detección de intrusos basados en red son:

Snort

Es un sistema de detección de intrusos basado NIDS, de código abierto que monitoriza todo un dominio de colisión y funciona detectando usos indebidos y enviar alertas a tiempo real. El snort puede configurarse modo sniffer y mostrar solo los encabezados grabar los paquetes permite crear reglas.[8]

[6] (Victor Manuel Mendoza Anaya 2017)
[7] (Victor Manuel Mendoza Anaya 2017)
[8] (Jimènez 2003)

Snort puede ser usado para detectar una gran variedad de ataques y pruebas como[9]:

- Escaneo de puertos oculto,
- Ataques basados en la Common Gateway Interface (CGI)
- Spoofing ng de protocolo ARP, y
- Ataques en daemons con vulnerabilidades conocidas, etc.

Reglas de Snort

Una de las funciones más valoradas de Snort es la capacidad de que los usuarios puedan escribir sus propias reglas, además de una larga base de datos de reglas que Snort contiene por default, administradores de IDS pueden tomar ventajas de dicha capacidad para desarrollar sus propias reglas en vez de tener que depender de una agencia externa, vendedor o administrador para actualizaciones en caso de que un nuevo ataque o exploit sea descubierto, los administradores de Snort pueden escribir sus propias reglas para todo tráfico que ellos consideren anómalo y comparar notas con una gran comunidad de escritores de reglas de Snort en internet. Esto permite capacidades imprecedentes en cuanto a velocidad de actualización y personalización. Una regla es un conjunto de instrucciones diseñadas para tomar un paquete del tráfico de la red y comparar un patrón específico, para entonces tomar una acción cuando la regla coincida con el paquete de tráfico[10].

Base de datos de las reglas de ataques

El NIDS implementado en este proyecto será capaz de analizar el tráfico de la red mediante la base de datos de ataques de Snort. Un buen NIDS necesita una buena y extendida base de datos de firmas. Pero para crear y mantener una base de datos actualizada que sea suficientemente buena para este proyecto, implica un gran esfuerzo. Por esa razón este NIDS, será capaz de procesar las reglas basadas en Snort, el cual cuenta con una gran cantidad de reglas desarrolladas y

[9] (Velásquez Ed. Coruniamericana, Vol. I, 2012. 9-24)
[10] (Botello Cholula, Puebla, México. 13 de Mayo de 2010. http://catarina.udlap.mx/u_dl_a/tales/documentos/mcc/muniz_b_p/portada.html)

actualizadas, además cuenta con amplia documentación y facilita la creación de nuevas reglas

El lenguaje usado por Snort es flexible y potente, basado en una serie de normas que servirán de guía para la escritura de las reglas. Dentro de estas normas tenemos:

- La descripción de cada regla.
- Cabecera.
- Opciones.
- Uso de preprocesadores

Las reglas de Snort se pueden dividir en dos secciones lógicas: cabecera y opciones como se puede observar en la Tabla:

- La cabecera contiene la acción de la regla en sí, protocolo, IPs, máscaras de red, puertos origen y destino y destino del paquete o dirección de la operación.

- La sección opciones contiene los mensajes y la información necesaria para la decisión a tomar por parte de la alerta en forma de opciones.

Tabla 1

Cabecera	**Opciones**
Acción	Mensaje
Protocolos involucrados	Opciones de decisión
Direcciones IP	
Numero de puerto	
Dirección de la operación	

|| *CABECERA ~- Acción ~- Protocolos involucrados ~- Direcciones IP ~- Números de puerto ~- Di- rección de la operación* || *OPCIONES ~- Mensaje ~- Opciones de decisión* ||

Ejemplo de regla Snort para alertar de un escaneo Nmap del tipo TCP ping:

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Escaneo ping con nmap";flags:A;ack:0; reference:arachnids,28;classtype:attempted-recon; sid:628; rev:1;)

Los elementos del ejemplo anterior son:

Cabecera:

- **Acción de la regla**: alert
- **Protocolo**: tcp
- **Dirección IP origen**: $EXTERNAL_NET(toda la red)
- **Puerto IP origen: any** (cualquiera)
- **Dirección IP destino**: $HOME_NET (toda nuestra red)
- **Puerto IP destino**: any (cuaquiera)
- **Direccion de la operación**: -> (puede ser ->, <-, <>)

Opciones:

- **Mensaje**: msg
- **Opciones**: flags:A;ack:0; reference:arachnids…(1)

Desglosando las opciones:

- **Flags:A** Establece el contenido de los flags ó banderas TCP, en este caso ACK (puede tener varios valores y operadores).
- **Ack:0** Caso particular para valor ACK=0, es el valor que pone Nmap para TCP ping scan.
- **reference:arachnids,28** Referencia un a un Advisory, alerta tipo Bugtrac, etc.
- **classtype:attempted-recon** Categoría de la alerta según unos niveles predefinidos y prio- ridades.
- **sid:628** Identificación única para esta regla Snort según unos tramos determinados.
- **rev:1** Identificación de la revisión o versión de la regla.

EasyIDS

Es un sistema de detección de intruso basado en Snort, el cual integra varias herramientas de monitoreo bajo una interfaz web fácil de manejar, este viene integrado con las herramientas básicas para el análisis de tráfico.[11]

Suricata

Es un motor de detección de amenaza de red gratuito, capaz de detectar intrusos en tiempo real. Este inspecciona el tráfico de la red utilizando una potente y extensa normativa contando con un potente soporte de secuencias de comandos Lua para la detección de amenazas.

Suricata implementa un lenguaje de firma completo para coincidir con amenazas conocidas, infracciones de políticas y comportamiento malicioso. Suricata también detectará muchas anomalías en el tráfico que inspecciona. Suricata es capaz de utilizar el conjunto de reglas especializadas Emerging Threats Suricata y el conjunto de reglas VRT[12].

A continuación, se mostrará las características de suricata

Configuración

- Archivo de configuración YAML - legible por humanos y máquinas
- bien comentado y documentado
- soporte para incluir otros archivos

Analizadores de protocolo

- Soporte para la decodificación de paquetes de
    - IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE
    - Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN
- Decodificación de capa de aplicación de:
    - HTTP, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, Modbus, ENIP / CIP, DNP3, NFS, NTP

[11] (jonhatan 2010)
[12] (elhacker 2017)

- Soporte experimental para el desarrollo de analizadores en el lenguaje Rust, para una decodificación segura y rápida.

Salidas

- Guiones de salida Lua
- Registro de solicitud HTTP
- TLS handshake logging
- Alerta de registro rápido
- Registro de depuración de alertas: para escritores de reglas
- Registro de tráfico usando registrador pcap
- syslog - alert to syslog
- Registrador de solicitud / respuesta DNS, incluidos datos TXT.

7.1.2.4.2 Sistema de detección de intrusiones en el host

Este es un sistema de detección de intrusiones, que garantiza la seguridad en el host, en el que busca actividad sospechosa analizando los sistemas constantemente. Hay que mencionar, además que los HIDS residen en el propio host que monitorizan, lo cual permite informar con gran precisión sobre el estado blanco atacado. Y así mismo determinan los procesos y usuarios que están involucrados en un ataque particular en el sistema.

7.1.2.4.2.1 Características

Las características de los HIDS son[13]:

- fuentes de información.
- pueden observar el desenlace de un determinado ataque.
- Pueden analizar actividades con gran precisión y fiabilidad determinando qué procesos y usuarios están involucrados en un determinado ataque.

[13] (Victor Manuel Mendoza Anaya 2017)

7.1.2.4.2.2 Ventajas

Las ventajas de los HIDS son[14]:

- Detecta ataques que no pueden ser detectados en un NIDS.
- Analiza los datos antes de que sean cifrados en el host origen.
- Al operar en los hosts pueden trabajar en entornos donde se intercambie información cifrada.
- No les afectan las redes conmutadas.
-

7.1.2.4.2.3 Desventajas

Las desventajas de los HIDS son[15]:

- Hay que configurar y gestionar la información de cada uno de los host que está monitoreando.
- No son muy apropiados para escaneos de red o para ataques de sondeo de redes enteras.
- Pueden ser deshabilitados por ataques DOS.
- la cantidad de información puede ser muy elevada.

7.1.2.4.2.4 Productos comerciales basados en HIDS

Algunos sistemas de detección de intrusos basados en host son:

Tripwire: Viene en dos versiones, Tripwire Enterprise y Tripwire Open Source. Fundamentalmente, ambos son sistemas de detección de intrusiones basados en host para monitorear cambios de archivos y configuración. FIM ha sido sin duda el fuerte de Tripwire, con otras características sólidas como informes y monitoreo basado en políticas para cumplimiento normativo (p. Ej., PCI DSS, NERC, NIST).

RPM como IDS[16]: El manejador de paquetes Red Hat Package Manager (RPM), es un programa que puede ser usado como sistema de detección de intruso basado en host, que contiene varias opciones

[14] (Victor Manuel Mendoza Anaya 2017)
[15] (Victor Manuel Mendoza Anaya 2017)
[16] (Sandra A. Moore 2005)

para consultar paquetes y sus contenidos, estas opciones de verificación son importantes para el administrador de la red que sospeche que los archivos del sistema y ejecutables hayan sido modificados.

SWATCH[17]: WATCHer o SWATCH utiliza archivos de registro generados por syslog para alertar a los administradores de las anomalías, basándose en los archivos de configuración del usuario. SWATCH fue diseñado para registrar cualquier evento que el usuario desee añadir en el archivo de configuración; sin embargo, ha sido adoptado ampliamente como un IDS basado en host.

OSSEC: E s un proyecto open source de gestión de Logs, que monitoriza una máquina, y que detecta las anomalías que puedan producirse en ella. Para hacer esto utiliza herramientas para la detección de rootkits, para revisar la integridad de ficheros y ejecutables del sistema, y por último un potente sistema para analizar logs.

Está basado en un modelo de cliente-servidor, con lo cual tendremos un servidor centralizado que se encarga de recibir y actuar en base a la información que reciba de los agentes que, en definitiva, son las máquinas que están siendo monitorizadas y atacadas. La forma de actuar del servidor es, por una parte, enviando notificaciones, y por otro lado, si así se configura, generando reglas firewall que se ejecutarán en los propios agentes.

7.1.2.5 Tipo de respuesta de los sistemas de detección de intrusos

Activos: Las respuestas activos son acciones automáticas que detectan cuando hay una intrusión en la red, generando algún tipo de respuesta sobre el sistema atacante, como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración. Podemos establecer dos categorías:

- **Recogida de información adicional:** Este incrementa el nivel de sensibilidad de los sensores para obtener más pistas de un posible ataque, por ejemplo, capturando todos los paquetes que vienen de la máquina del atacante durante cierto tiempo.

[17] (Sandra A. Moore 2005)

- **Cambio del entorno:** Este puede parar el ataque; por ejemplo, en el caso de una conexión TCP se puede cerrar la sesión establecida y filtrar en el Reuter de acceso o en el firewall la dirección IP del intruso.

Pasivos: Este tipo de respuesta notifica al administrador de la red, mediante una alerta que el sistema está siendo atacado, así mismo es posible que le puede avisar al administrador desde donde se produjo el ataque.

7.1.3 Diferencia entre sistema de detección de intruso e sistema de prevención de intruso

Estos dos fueron desarrollados para brindar un soporte más fuerte a las redes sin depender del firewall solamente. Generalmente los IDS se establecen en secciones de la red en los cuales se encarga de detectar amenazas o intrusiones. Los IPS por otra parte se encargan de identificar estas amenazas o intrusiones y bloquear o dejar caer sus actividades.

Los IDS e IPS cuentan con funciones muy similares como[18]:

- Inspección de paquetes.
- Análisis de estado.
- Relocalización de segmento TCP.
- Inspección profunda de paquetes.
- Validación de protocolos.
- Correspondencia de firmas.

7.1.3.1 Categorización de los IDS e IPS

La diferencia entre los IDS e IPS están categorizado en cuatro objetivos concretos que son:

Estabilidad de la red y rendimiento

Ya que el IDS no se encuentra alineado con el flujo de datos de la red puede tener una latencia en el tiempo de captura y reporte de las situaciones anómalas de segundos hasta minutos, pero su tiempo de

[18] (Ashoor y Gore, Difference between Intrusion Detection System (IDS) & Intrusion Prevention System (IPS) Pune University, India. Julio de 2011.)

respuesta depende sobre todo del tiempo de respuesta del factor humano.

Por otro lado, el IPS se encuentra alineado con el flujo de datos de la red y puede pasar a través de los dispositivos, por lo tanto, tiene una latencia de microsegundos la cual provee un tiempo de respuesta óptimo y además cuenta con una capacidad de procesamiento más alta.

Precisión - Falsos Positivos

Existen tres reglas básicas para determinar la precisión de los IDS e IPS en cuanto a falsos positivos:

- El IDS minimiza los falsos positivos, pero el IPS no cuenta con falsos positivos. Esto cambia o afecta dramáticamente la escritura y testeo de los filtros de alertas.
- Las alertas de falsos positivos en los IDS pueden ser o no exitosas, pero en los IPS los falsos positivos bloquean el tráfico legítimo.
- Los filtros de anomalías no se pueden usar para realizar bloqueos.

Falsos Negativos

Los falsos negativos solo se tratan de un ataque fallido. El IDS puede llegar a ser abrumado por tráfico que sobrepase su capacidad, soltando paquetes necesarios para detectar un ataque, por otro lado, el IPS abruma el dispositivo, hace que el tráfico sea bloqueado o lo deja caer impidiendo que el ataque tenga éxito para descubrir anomalías.

Análisis del registro de datos

Los datos registrados por el IDS e IPS suelen ser comprensibles, y pueden ser usados para corroborar la información en un escenario de post-ataque. Estos tipos de datos son más que todo para analizar durante y después de un ataque y ayudar a la organización de ambas respuestas, además de la evidencia de que el ataque tuvo lugar.

8. DISEÑO METODOLOGICO

8.1. Hipótesis

Sera posible desarrollar una metodología para la comparación de los diferentes IDS y realizar un escenario de pruebas en el que se puedan llevar a cabo ataques para validar la efectividad de cada uno?

8.2. Población

El resultado de esta investigación va dirigido y pueden verificar tanto a los fabricantes de productos de seguridad como a las personas y/o empresas que dependen de ellos para mantener la seguridad de sus datos.

8.3. Diseño experimental

Se implementará dos IDS uno dentro de la red y otro fuera de la red y se realizaran tres tipos de ataques diferentes, primero al IDS interno luego al IDS externo para ver la reacción de cada uno y su efectividad por separado frente al sistema después se le hará ataque a los dos IDS para ver la efectividad de los dos en conjunto, también se utilizarán un IPS para que monitoree el tráfico y me identifique la amenaza.

9. ATAQUES SPOOFING TIPÍCOS EN UNA RED LAN

Una red LAN mantiene constantemente atacada por personas inescrupulosas, para sacar un beneficio personal o económico, por tal razón diariamente se presentan muchos ataques a esta, como por ejemplo la suplantación de identidad o pérdida de información al usuario. Debido a lo anterior nos enfocaremos en los ataques de suplantación (spoofing) típicos en una red LAN.

9.1 IP Spoofing

Es conocido como enmascaramiento de la dirección IP, en los cuales usuarios malintencionados o intrusos modifican los paquetes con una dirección IP de origen falsa para así enviarlo a un determinado sistema informático y simular que proviene de un equipo diferente, para luego apoderarse y hacerse pasar por otra persona y sacar beneficios para sí mismo.

Entre los ataques IP Spoofing podemos incluir los siguientes:

- Man-in-the-middle (MITM).
- Routing re-direct.
- Enrutamiento de origen.
- Inundación.
- Smurfing.

9.1.1 Como hacer IP Spoofing

A Continuación, se realizará una práctica el cual se mostrará como hacer una suplantación IP.

Herramientas utilizadas

- Una computadora con sistema Operativo Windows 7.
- símbolo del sistema.
- Wireshark.

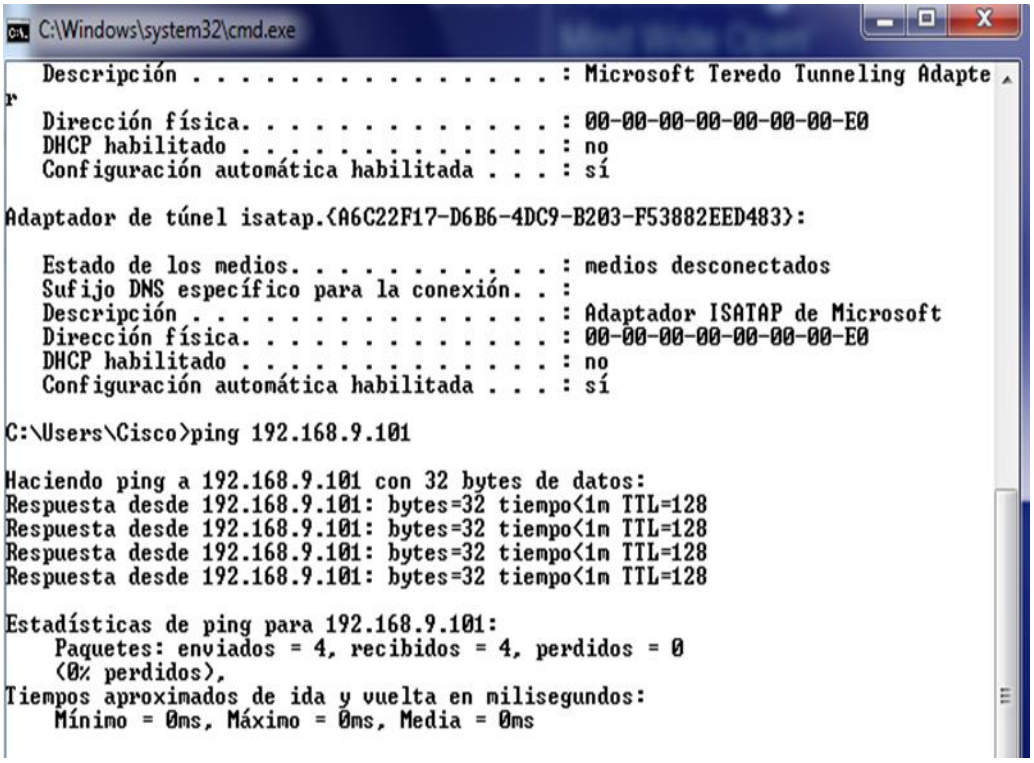
a. Abrir el símbolo del sistema y escribir el comando ipconfig/all, para ver la dirección IP de la máquina.

Ilustración 1

b. Luego instalar Wireshark en el siguiente link https://www.wireshark.org/download.html

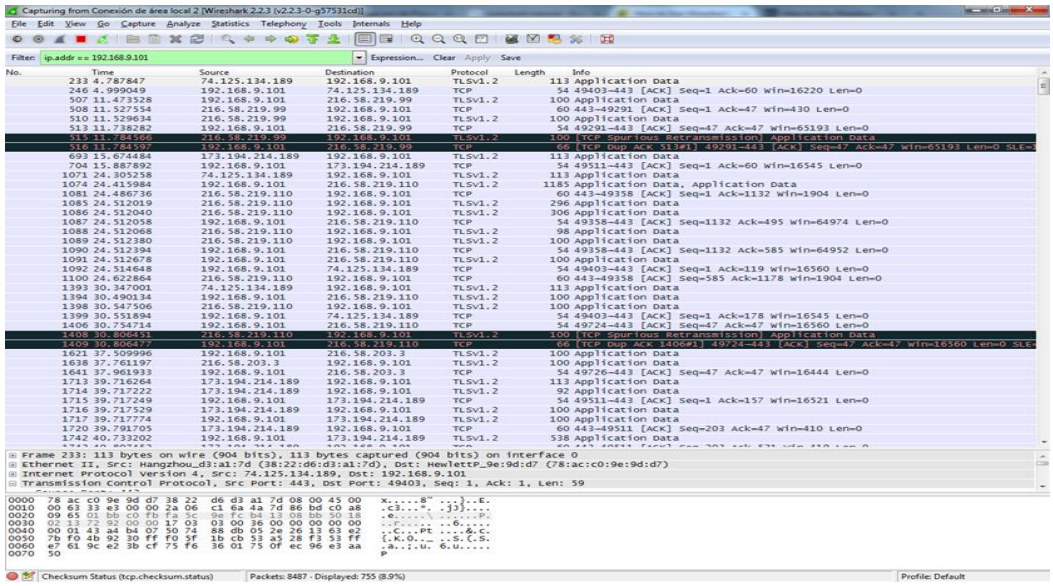
c. Después abrir el símbolo del sistema y hacer ping a la dirección IP, en mi caso 192.168.9.101

Ilustración 2



d. Ahora se abre Wireshark y se escribe ip.addr == 192.168.9.101, para capturar todo el tráfico de la red.

Ilustración 3



9.2 DNS Spoofing

Es la suplantación de la dirección IP del dominio de la web, en el cual un intruso pretende provocar un direccionamiento erróneo al usuario, para que este pueda ingresar a una página web falsa y así interceptar mensajes de correo electrónico o claves de accesos a informaciones personales.

Para este tipo de ataques los intrusos consiguen que un servidor DNS legítimo que acepte y utilice información incorrecta obtenida de un ordenador que no posee autoridad para ofrecer[19].

[19] (vieites s.f.)

9.2.1 Como hacer DNS Spoofing

A Continuación, se mostrará cómo hacer DNS Spoofing[20].

Herramientas utilizadas

- Kali Linux
- Una computadora para spoofear

a. Descargar Kali Linux https://www.kali.org/.

b. Abrir la terminal de Kali Linux para editar el archivo de configuración Ettercap y escribir: getdit /etc/ettercap/etter.conf, se abrirá el archivo etter.conf y editar los valores **uid** y **git** asi como se ve en la siguiente imagen.

Ilustración 4

```
#  (at your option) any later version.                                    #
#                                                                         #
#                                                                         #
###########################################################################

[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_smart = 0          # boolean
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
arp_poison_request = 0        # boolean
arp_poison_equal_mac = 1      # boolean
dhcp_lease_time = 1800        # seconds
port_steal_delay = 10         # seconds
port_steal_send_delay = 2000  # microseconds
```

Ahora desplazarse hacia abajo hasta que encuentre el encabezado que dice Linux y debajo de eso elimine los dos signos # debajo donde dice "si usa iptables".

[20] (TRT 2016)

Ilustración 5

```
#--------------
#     Linux
#--------------

# if you use ipchains:
   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port
   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %por

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport

#--------------
#    Mac Os X
#--------------

# quick and dirty way:
   #redir_command_on = "ipfw -q add set %set fwd 127.0.0.1,%rport tcp from any
   #redir_command_off = "ipfw -q delete set %set"

# a better solution is to use a script that keeps track of the rules interted
```

c. Ahora ejecutar el comando ettercap -G, con este comando se abrirá Ettercap.

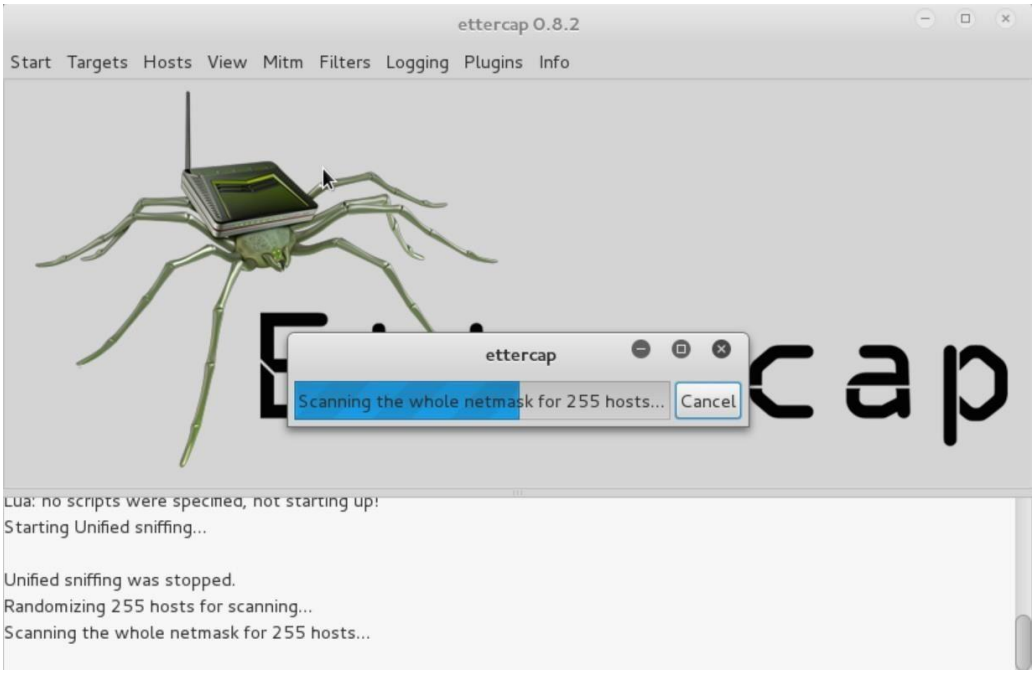
Ilustración 6

d. Primero seleccionar Sniff > **Unified sniffing** ... > (Seleccione la interfaz conectada a internet)> OK

e. Luego ir a **Start** > **Stop sniffing** porque comienza a olfatear automáticamente después de presionar **OK** y no queremos eso.

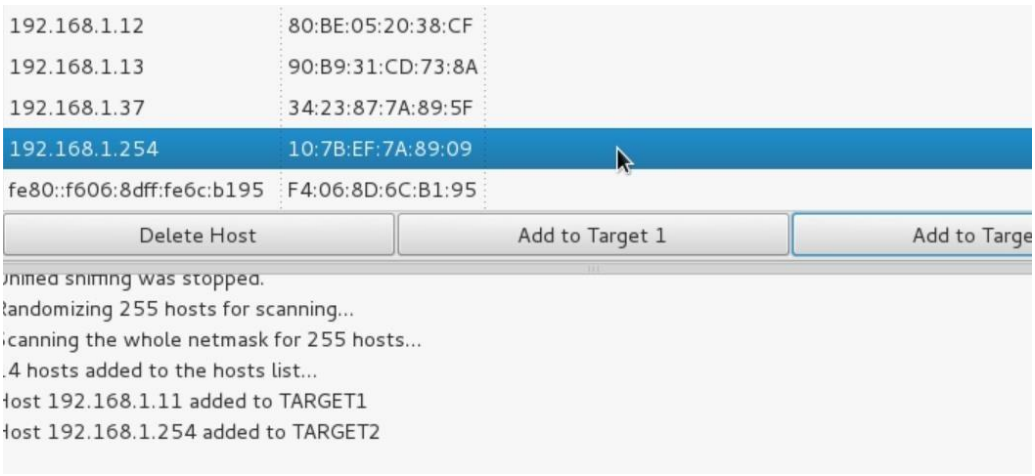
f. Ahora ir a Hosts > Buscar hosts y espere hasta que realice el escaneo. Solo debería tomar unos segundos dependiendo del tamaño de su red (que supongo que no es muy grande).

Ilustración 7



Luego ir a Hosts y seleccionar list host, y seleccionar la dirección IP de la víctima y agerarlo al objetivo 1, después elegir la puerta de enlace y agregarlo al objetivo 2.

Ilustración 8



g. Ir MITM y seleccione Spoof ARP, elija **Sniff conexiones remotas** y presione **OK**. Ahora vaya a **Complementos** > **Administre los complementos** y haga doble clic en **dns_spoof** para activar ese complemento.

h. Ahora se necesita editar otro archivo en la carpeta Ettercap.
Gedit /etc/ettercap/etter.dns
Este archivo etter.dns es el archivo hosts y es responsable de redirigir las solicitudes DNS específicas. Básicamente, si el objetivo ingresa a facebook.com, será redireccionado al sitio web de Facebook, pero este archivo puede cambiar todo eso. Aquí es donde sucede la magia, así que editémosla.

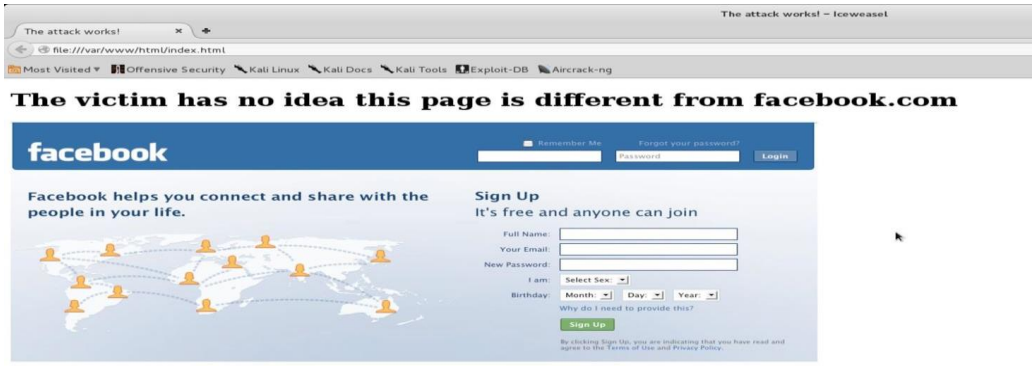
i. En primer lugar, redirija el tráfico desde cualquier sitio web que desee a su máquina Kali. Para eso, vaya a donde dice "microsoft sucks;)" y agregue otra línea como la que se encuentra debajo, pero ahora use el sitio web que desee. Además, no olvide cambiar la dirección IP a su dirección IP.

Ilustración 9

```
# or for TXT query (value must be wrapped in double quotes):                  #
#    google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all"                           #
#                                                                              #
# NOTE: the wildcarded hosts can't be used to poison the PTR requests          #
#       so if you want to reverse poison you have to specify a plain           #
#       host. (look at the www.microsoft.com example)                          #
#                                                                              #
################################################################################

###############################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   107.170.40.56
*.microsoft.com    A   107.170.40.56
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed
facebook.com       A   192.168.1.39
*.facebook.com     A   192.168.1.39

########################################
# no one out there can have our domains...
#

www.alor.org  A 127.0.0.1
www.naga.org  A 127.0.0.1
www.naga.org  AAAA 2001:db8::2

########################################
# dual stack enabled hosts does not make life easy
# force them back to single stack

www.ietf.org   A    127.0.0.1
www.ietf.org   AAAA ::

www.example.org  A    0.0.0.0
www.example.org  AAAA ::1
```

j. Ahora tenemos que iniciar Apache para aceptar el tráfico entrante, escribir en la terminal service apache2 start.
Pasemos a la carpeta predeterminada de la página html. Ahí es donde se puede tomar el control de lo que la víctima ve cuando es redirigido. La ubicación es / var / www / html, donde encontrará la página index.html . Puede modificar el documento según sus necesidades y, una vez que crea que ha engañado lo suficiente a su víctima, puede guardar la página y los cambios tendrán efecto al instante. Ver la ilustración

Ilustración 10



9.3 Web Spoofing

Es la suplantación de una página web real, en que el atacante redirige a la víctima a una página falsa realizando una copia exacta de los marcos del navegador de este, World Wide Web en que la víctima pretende entrar. El atacante observa y controla todo lo que la víctima hace registrando toda su información sensible aunque el usuario utilice conexiones TLS/SSL seguras ya se encuentra en la página web falsa así que ya no cuenta con ninguna protección de sus datos.

9.3.1 Como hacer Web spoofing

La siguiente práctica que se realizará, se mostrará cómo suplantar un sitio Web[21].

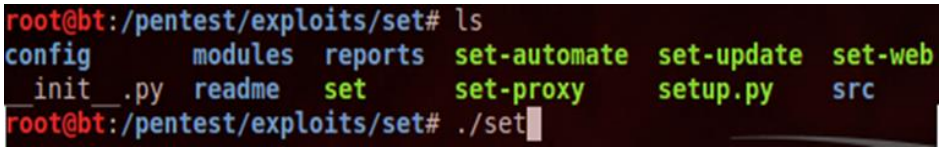
Herramientas utilizadas

- Backtrack5.
- Una computadora con sistema operativo LINUX.

a. Descargar backtrack5 en el siguiente link: http://es.ccm.net/download/descargar-17456-backtrack

b. Después de descargarlo, es muy importante correr la herramienta backtrack 5 en modo gráfico. Posteriormente se ingresa al directorio de nombre set y se ejecuta el binario correspondiente; cd/pentes/exploits/set y escribir ./set

Ilustración 11



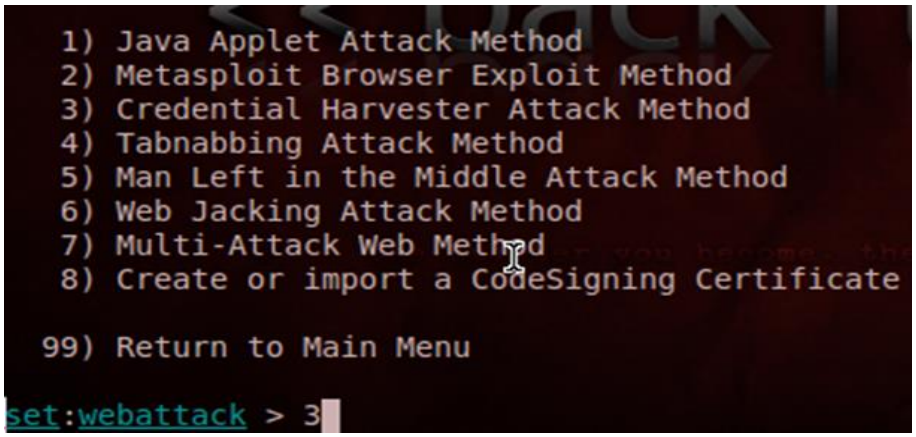
c. Se selecciona la opción 2 (Website attack vectors).

[21] (lsilva 2012)

Ilustración 12

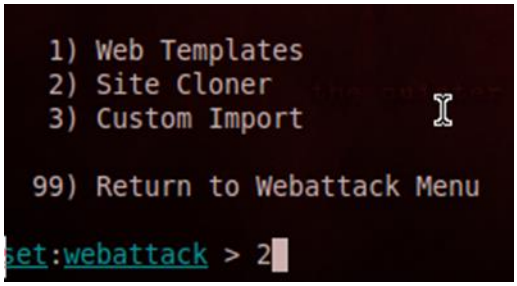
d. Selecciona la opción 3 (Credential Harvester Attack Method).

Ilustración 13



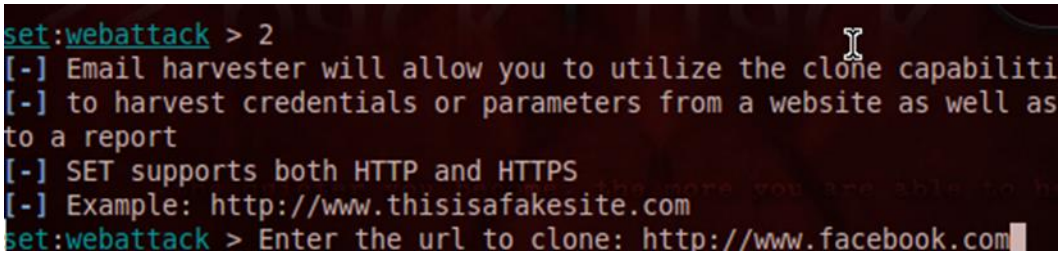
e. Selecciona la opción 2 (Site Cloner).

Ilustración 14



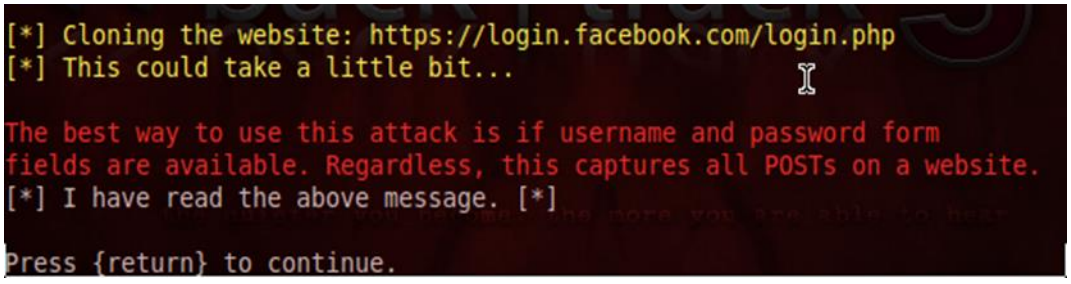
f. Se escribe el sitio web que se desea suplantar, en este ejemplo, seleccione el sitio web Facebook.

Ilustración 15



g. Después de unos segundos el sitio web estará suplantado.

Ilustración 16

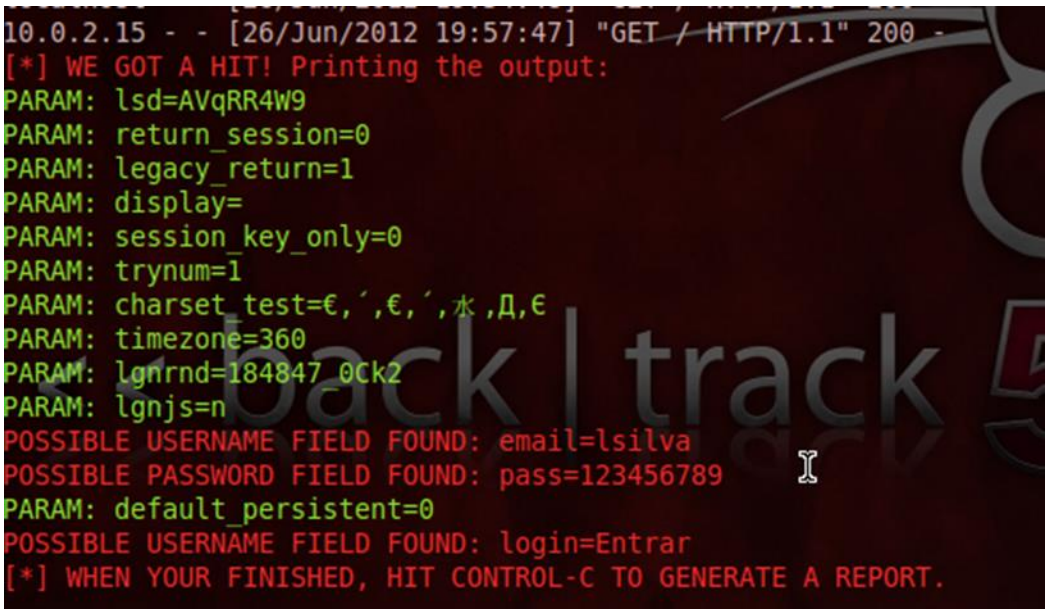


h. Se dirige al navegador web para verificar si fue efectiva la suplantación del sitio web y se escribe la dirección IP local externa (atacante).

Ilustración 17

i. Si se quiere probar el acceso con un usuario ficticio, se capturará el nombre de usuario y contraseña de la víctima.

Ilustración 18



Nota: Es necesario que el servidor web apache esté funcionando.

9.4 ARP Spoofing

Es la suplantación de identidad por la falsificación de la tabla ARP, este protocolo es responsable de encontrar la dirección MAC con la dirección IP de una computadora falseando la tabla del ARP; permitiendo a los atacantes tener accesos a la intercepción o la modificación de los datos que están en tránsito y así robar información sensible de una persona o una empresa. la suplantación de ARP es utilizado para otros caso como:

Secuestro de sesiones (Session hijacking): ataques de secuestro de sesión pueden hacer uso de ARP Spoofing para robar los identificadores de sesión, garantizando así el acceso a los atacantes y los sistemas privados de datos.

Ataques tipo Hombre en el Medio (Man-in-the-middle Attacks): Los ataques MITM pueden utilizar ARP Spoofing para interceptar y/o modificar el tráfico entre dos víctimas[22].

9.4.1 Como hacer ARP Spoofing

La siguiente práctica se realizará, se mostrará como hacer ARP Spoofing[23].

Herramientas Utilizadas

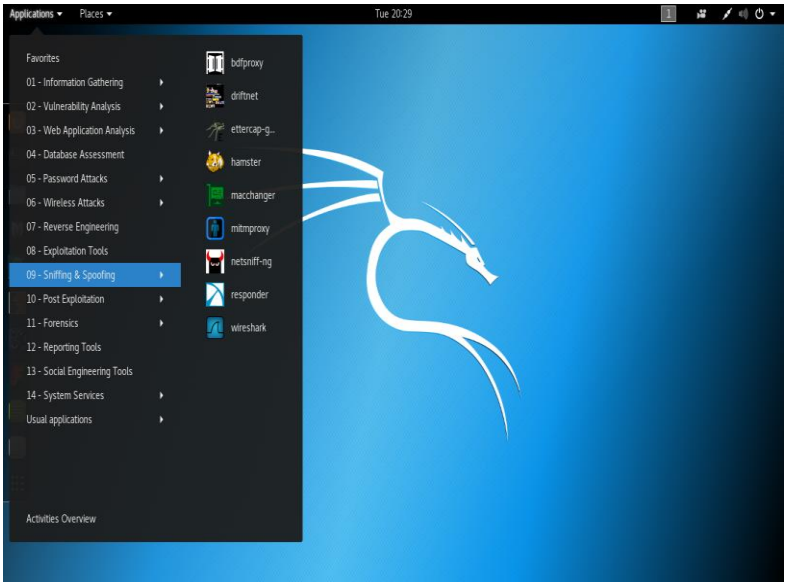
- Kali Linux.
- Ettercap

a. Primero instalar la herramienta Kali Linux https://www.kali.org/

b. Ir a aplicaciones y buscar el apartado “9.Sniffing y Spoofing”, hay se encontrara las herramientas necesarias para llevar acabo un ataque informático.

[22] (Soto 2016)
[23] (Velasco 2016)

Ilustración 19



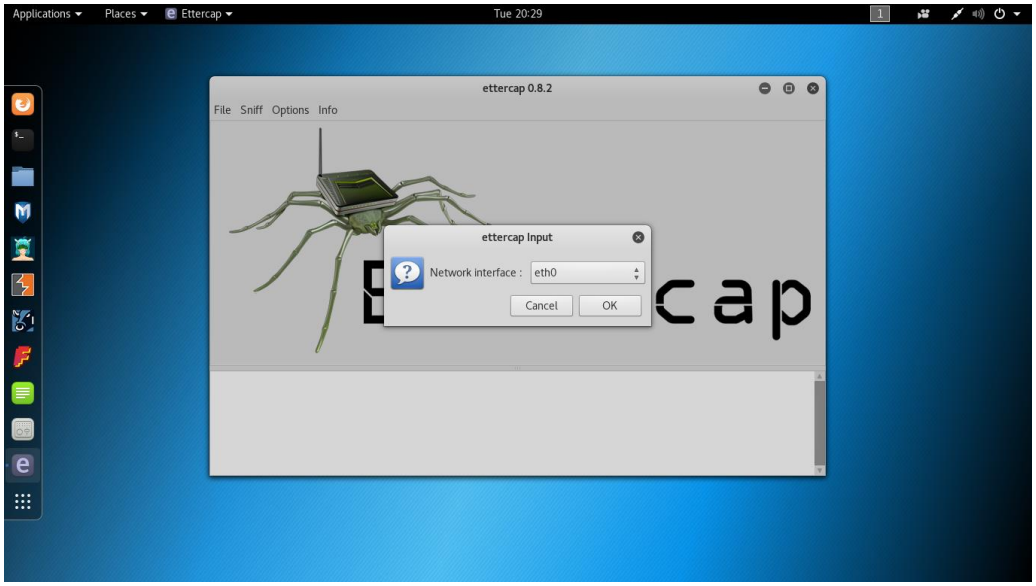
c. Elegir “Ettercap” y se verá una ventana similar a la siguiente.

Ilustración 20

d. El siguiente paso es seleccionar la tarjeta de red con la que se va a trabajar. Para ello, en el menú superior de Ettercap seleccionar

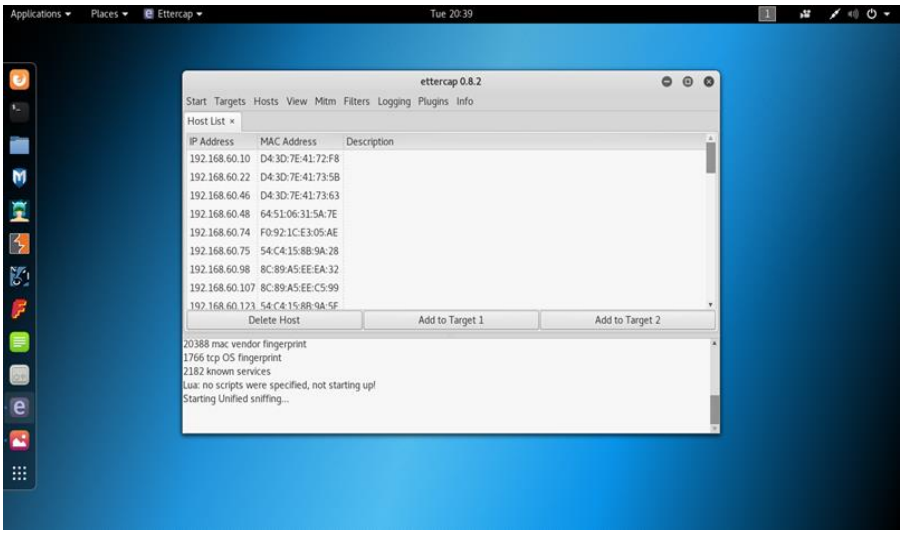
“Sniff > Unified Sniffing” y, cuando pregunte, seleccionar la tarjeta de red (eth0).

Ilustración 21



e. El siguiente paso es buscar todos los hosts conectados a nuestra red local. Para ello, seleccionar “Hosts” del menú de la parte superior y seleccionar la primera opción, “Hosts List.

Ilustración 22

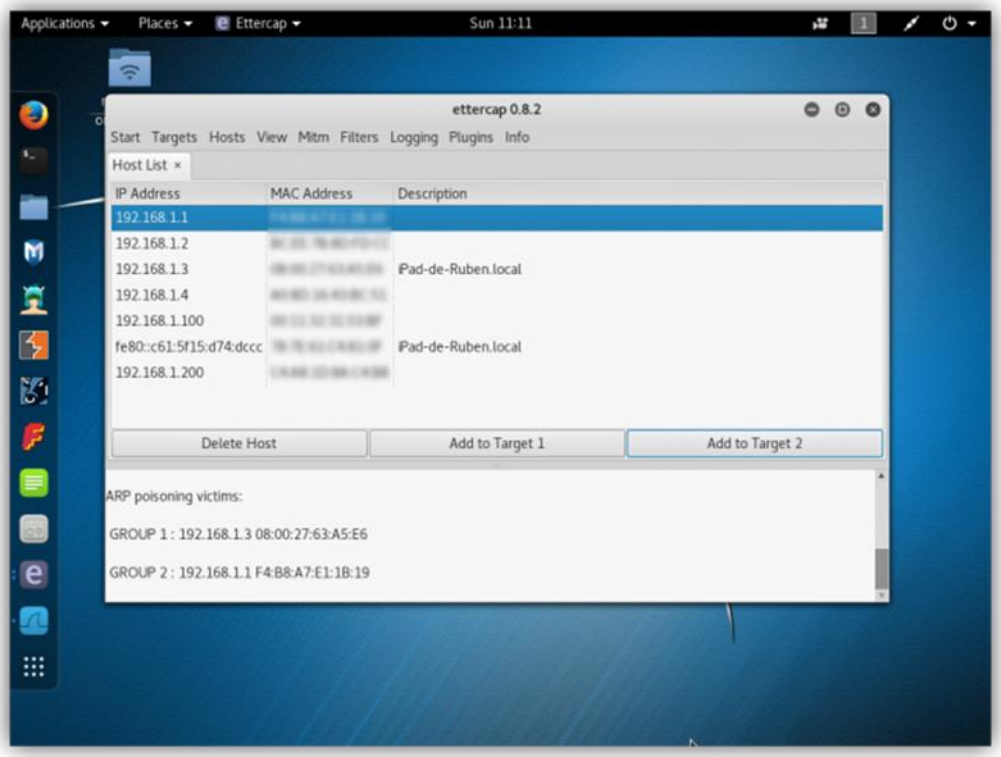


Aquí deberían salir todos los hosts o dispositivos conectados a nuestra red. Sin embargo, en caso de que no salgan todos,

podemos realizar una exploración completa de la red simplemente abriendo el menú “Hosts” y seleccionando la opción “Scan for hosts“. Tras unos segundos, la lista de antes se debería actualizar mostrando todos los dispositivos, con sus respectivas IPs y MACs, conectados a nuestra red.

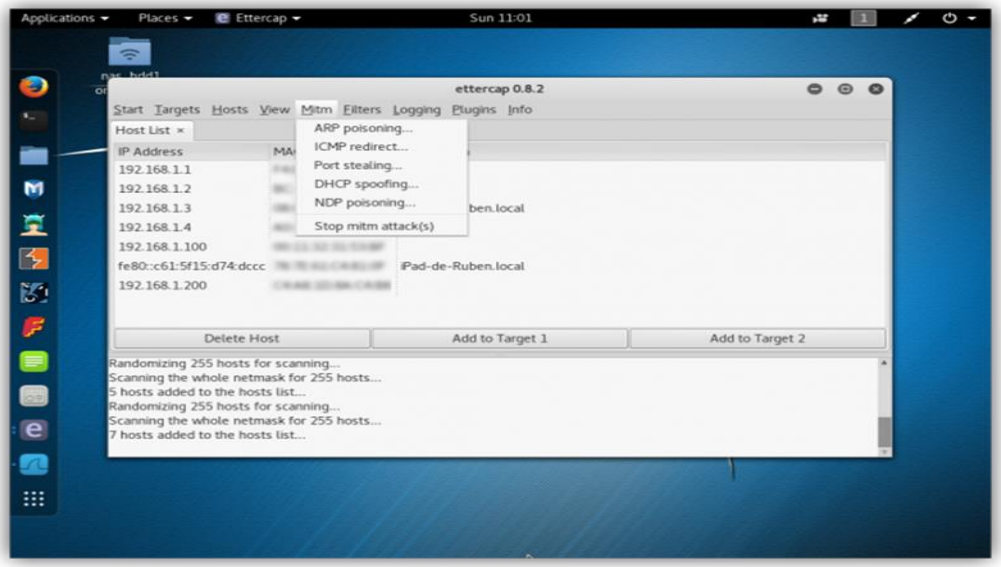
f. En caso de querer realizar un ataque dirigido contra un solo host, por ejemplo, suplantar la identidad de la puerta de enlace para monitorizar las conexiones del iPad que nos aparece en la lista de dispositivos, antes de empezar con el ataque debemos establecer los dos objetivos.
Para ello, debajo de la lista de hosts se podrá ver tres botones:
Target 1 – Seleccionar la IP del dispositivo a monitorizar y pulsar sobre dicho botón.
Target 2 – Pulsar la IP que se quiere suplantar, en este caso, la de la puerta de enlace.

Ilustración 23



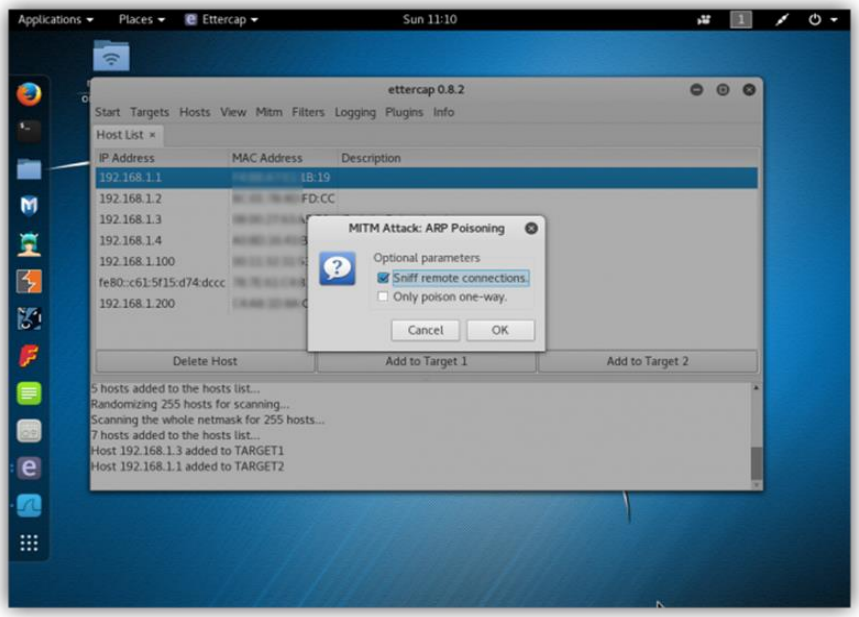
g. Ahora solo se debe elegir el menú “MITM” de la parte superior y, en él, escoger la opción “ARP Poisoning”.

Ilustración 24



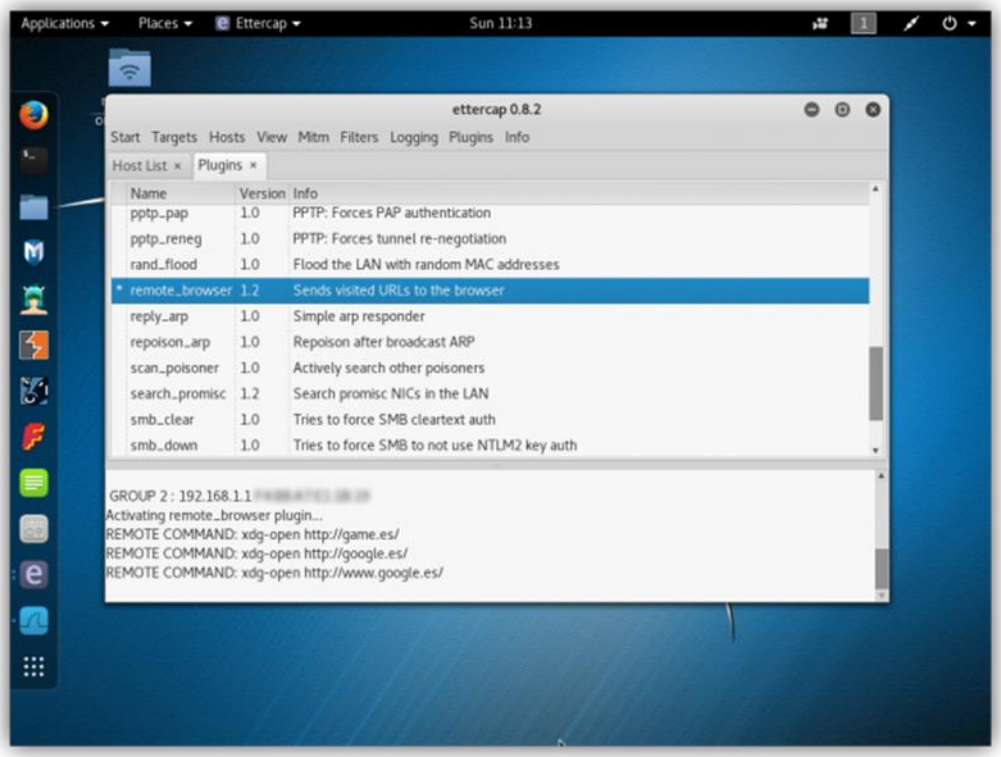
h. Aparecerá una pequeña ventana de configuración, en la cual se debe asegurar de marcar “Sniff Remote Connections”.

Ilustración 25



i. Pulsar sobre “Ok” y se iniciará el ataque. Ahora ya se puede tener el control sobre el host que se haya establecido como “Target 1“. Lo siguiente que se debe hacer es, por ejemplo, ejecutar Wireshark para capturar todos los paquetes de red y analizarlos en busca de información interesante o recurrir a los diferentes plugins que ofrece Ettercap, como, por ejemplo, el navegador web remoto, donde se carga todas las webs que visite el objetivo.

Ilustración 26



9.5 E-MAIL Spoofing

Como su nombre lo indica es la suplantación de correos en el cual el atacante cambia la dirección del remitente, para así parecer como si el correo proviniera de un origen diferente, el E-MAIL Spoofing es muy utilizada para el SPAM y la suplantación de identidad. Este es posible porque el protocolo SMTP no cuenta con un sistema de autenticación,

por lo tanto, es sencillo para un intruso ingresar a una red con comandos propios del protocolo variando la dirección de origen.

De hecho, muchos virus emplean esta técnica para facilitar su propagación, al ofrecer información falsa sobre el posible origen de la infección. Asimismo, este tipo de ataque es muy utilizado por los "spammers", que envían gran cantidad de mensajes de "correo basura" bajo una identidad falsa[24].

Muchos spammers usan ahora software especial para crear direcciones de remitente arbitrarias, de modo que, si incluso el usuario encuentra el origen del e-mail, es poco probable que la dirección sea verdadera[25].

Algunos correos suplantados no tienen mucha importancia y no se solicita mucha atención, Aunque también hay algunos que requieren importancia porque pueden ocasionar problemas serios y causar riesgos de seguridad al usuario, considerando que algunos correos solicitarán contraseñas, datos personales y hasta número de cuenta bancaria.

9.5.1 Como hacer E-MAIL Spoofing

A Continuación, se procederá hacer un ataque E-MAIL Spoofing con SMTP sobre SSL/TLS en Gmail. Google tiene ya en producción el uso de DKIM para algunos servicios como EBay o PayPal que hacen uso de ellos y que cuando el mensaje viene correctamente firmado desde uno de los servidores autorizados, entonces se muestra la famosa llavecita de DKIM[26].

Ilustración 27

[24] (vieites s.f.)
[25] (Garcia 2010)
[26] (Alonso 2016)

En el caso del candado rojo, este significa que es un mensaje que simplemente se ha enviado sin cifrar, pero aunque se envíe por un canal seguro SSL o TLS este no garantiza para nada que el mensaje sea original, por lo que si se hace un E-mail spoofing con comandos SMTP que salte los filtros SPF, o las tecnologías de scoring antispam, entonces el mensaje aparecerá sin el candado rojo como siempre ha sido.

Ilustración 28

Para hacerlo, basta con elegir un servidor de correo entrante de Gmail para enviar el mensaje falso. En este caso he elegido **gmail.smtp-in.l.google.com.**

Ilustración 29

```
Chemas-MacBook-Pro:~ Chema$ nslookup
> set type=mx
> gmail.com
Server:
Address:

Non-authoritative answer:
gmail.com       mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 5 gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
```

Después se tira con OpenSSL una conexión cifrada, en este caso por el puerto 25. Puede que suene raro que se use una conexión cifrada SSL por el mismo puerto que se usa para el tráfico no cifrado,Gmail

reconoce en la pasarela de entrada la conexión y la dirige hacia el servicio adecuado.

Ilustración 30

```
Chemas-MacBook-Pro:~ Chema$ openssl s_client -starttls smtp -connect gmail-smtp-
in.l.google.com:25 -crlf -ign_eof
CONNECTED(00000003)
depth=2 /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=mx.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIGoTCCBYmgAwIBAgIIM0fbJICF75UwDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
BhMCVVMxEzARBgNVBAoTCkdvb2dsZSBJbmMxJTAjBgNVBAMTHEdvb2dsZSBJbnRl
```

Para tirar la conexión, utilizar el cliente de OpenSSL con los parámetros que aparecen en la captura superior, y se establece el túnel cifrado por el puerto especificado.

Ilustración 31

```
New, TLSv1/SSLv3, Cipher is AES128-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES128-SHA
    Session-ID: 2AF2731D280EAF61BACC8A607E72910787653A44C5A351B454F
    Session-ID-ctx:
    Master-Key: 577A6F364B5934ABD7904A8860BC4A5BC5683CF33680D8E8482
C9710AE8028FD993527CFC5C7499E737
    Key-Arg   : None
    Start Time: 1455555558
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
250 SMTPUTF8
ehlo chema
250-mx.google.com at your service, [           1]
250-SIZE 35882577
250-8BITMIME
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
```

Una vez creada la conexión, el resto es como siempre, escribir el mensaje con el protocolo SMTP como si fuéramos un servidor de correo saliente que envía mensajes a un destinatario de Gmail.

Ilustración 32

```
mail from: <chema@i64.com>
250 2.1.0 OK y125si26518626wmy.113 - gsmtp
rcpt to: <[redacted]@gmail.com>
250 2.1.5 OK y125si26518626wmy.113 - gsmtp
data
354  Go ahead y125si26518626wmy.113 - gsmtp
Subject: Falsito
Sin candadito, porque voy cifradito
.
```

Y si todo ha ido bien, entonces el mensaje de correo llegará a la cuenta de Gmail del destinatario sin que aparezca el candado rojo.

Ilustración 33

9.6 MAC Spoofing

La suplantación de dirección MAC es una técnica para suplantar esta dirección, y así evitar los mecanismos de seguridad existente y hacerse pasar por dispositivos finales legítimos, la dirección MAC solo es utilizada por una VLAN o una subred. Igual que la suplantación IP en la suplantación MAC también puede ser usada para la suplantación de identidad, acceso a servicios no encontrados, evasión de filtros MAC, anonimato y envenenamiento ARP.

9.6.1 Como hacer MAC Spoofing

A Continuación, procederemos hacer MAC Spoofing[27].

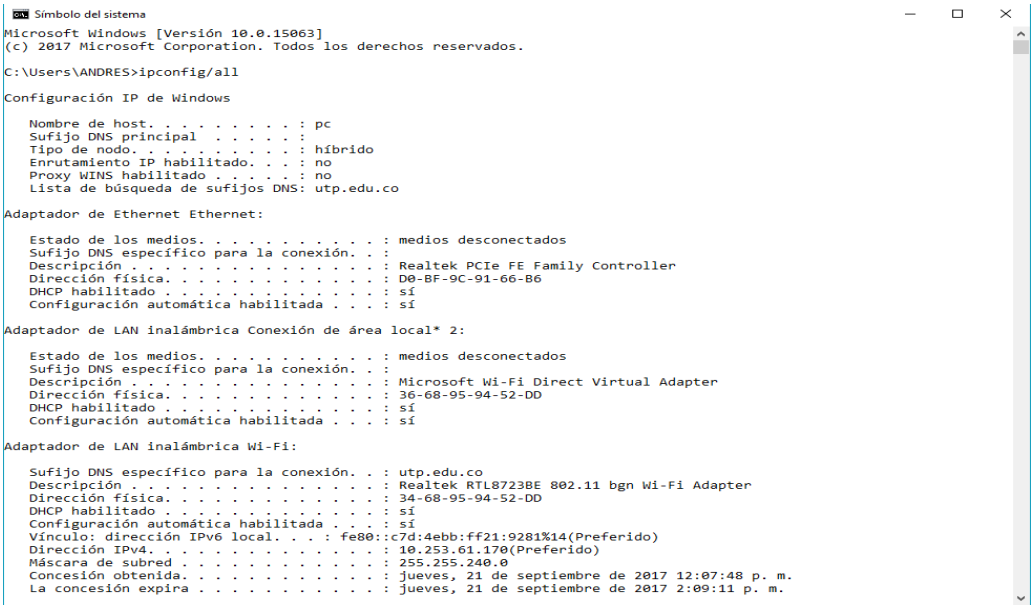
Herramientas utilizadas

- Una computadora con el sistema operativo Windows 10.
- Símbolo del sistema.
- Etherchange.exe.

a. Abrir el símbolo del Sistema y escribir el siguiente comando **Ipconfig /all** para ver la configuración completa de la tarjeta de red, mostrará la puerta de enlace, el servidor DNS primario y secundario, configuración Proxy, etc.

[27] (Heidegger 2010)

Ilustración 34



b. Ahora descargar la herramienta Etherchange.exe en: http://ccm.net/download/download-4685-etherchange

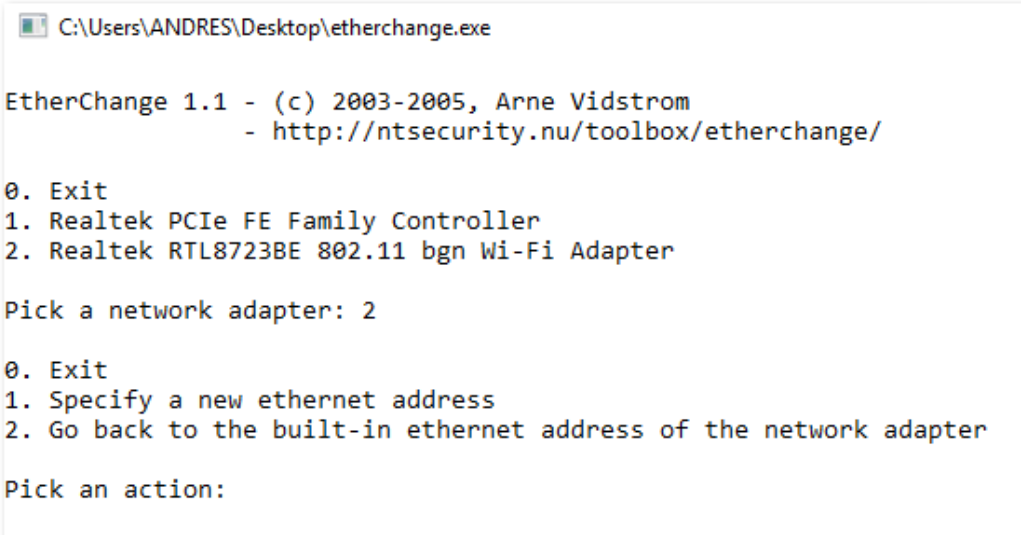
c. Desactivar el adaptador de red que estemos utilizando.

d. Después de haber descargado Etherchange.exe lo ejecutarlo como administrador. y se abrirá el símbolo del sistema y mostrará los siguiente

Ilustración 35

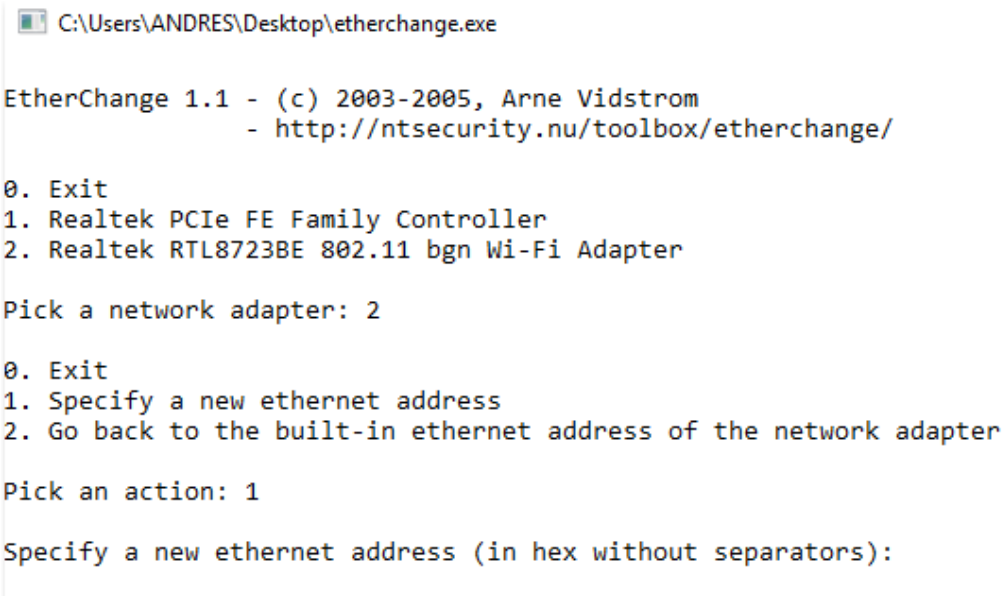
e. Elegir la Opción 2.

Ilustración 36



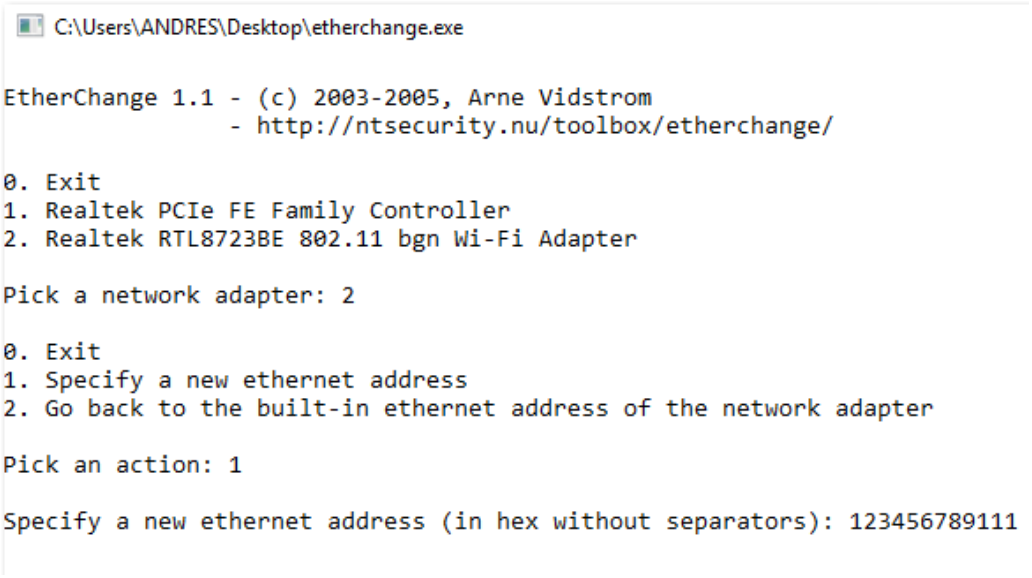
f. Luego escoger la opción 1, para poner la dirección MAC de la otra máquina y así suplantarla o spoofearla

Ilustración 37



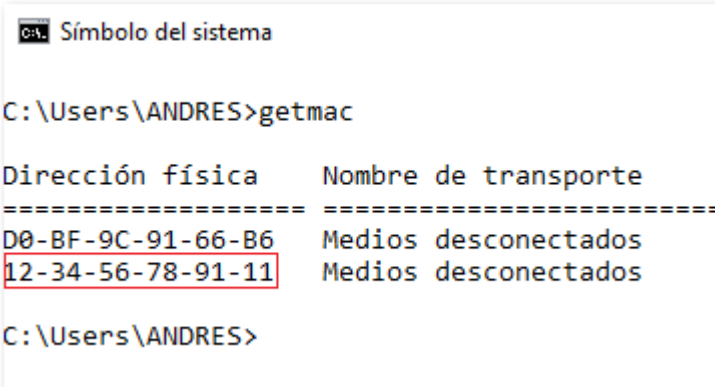
g. Especificar la nueva dirección MAC de la otra máquina que ustedes ya tienen que tener, la ponemos sin espacio, Ejemplo: 123456789111

Ilustración 38



h. Luego abrir el símbolo del sistema y escribir el siguiente comando getmac el cual arrojará todas las direcciones físicas de la red, y se verá la dirección MAC que se ingresó anteriormente, como se muestra en la siguiente imagen.

Ilustración 39



i. Luego activar el adaptador de red que se está utilizando.

j. Como podrán observar desde un principio mi MAC era esta. 34-68-95-94-52-DD, pero gracias al Etherchange las cambie.

Ilustración 40

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : utp.edu.co
   Descripción . . . . . . . . . . . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
   Dirección física. . . . . . . . . . . . . : 34-68-95-94-52-DD
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::c7d:4ebb:ff21:9281%14(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 10.253.61.170(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.240.0
   Concesión obtenida. . . . . . . . . . . . : jueves, 21 de septiembre de 2017 12:07:48 p. m.
   La concesión expira . . . . . . . . . . . : jueves, 21 de septiembre de 2017 2:09:11 p. m.
```

9.7 DHCP Spoofing

Es una característica de seguridad que provee seguridad filtrando los mensajes DHCP no confiables, construyendo y manteniendo una tabla de asociaciones DHCP spoofing, y actuando como un firewall entre los hosts. Hay que mencionar además que el DHCP nos permite diferenciar entre interfaces no confiables conectadas a usuarios finales e interfaces confiables conectadas a los servidores DHCP o Switch.Cuando se habilita DHCP Spoofing en una VLAN, el Switch actúa como un puente de capa 2 dentro del dominio de la VLAN. El DHCP spoofing es necesario para prevenir los ataques de tipo "man-in-the-middle" en nuestras redes[28].

9.7.1 Como hacer DHCP Spoofing

A continuación, se mostrará cómo hacer una suplantación DHCP, a través de Alice, Este es un host de la red.

Existe un atacante que ha iniciado un servidor DHCP con una configuración especialmente manipulada, indicando que dirección IP debe asignarse a Alice y en particular que la dirección IP del Atacante debe ser indicada como puerta de enlace predeterminada.

[28] (Gumucio 2016)

Si Alice solicita configuración mediante DHCP, es posible que el Atacante gane la carrera al DHCP legítimo y logre re configurar la puerta de enlace predeterminada de Alice, forzándola a utilizar como puerta de enlace predeterminada al Atacante.

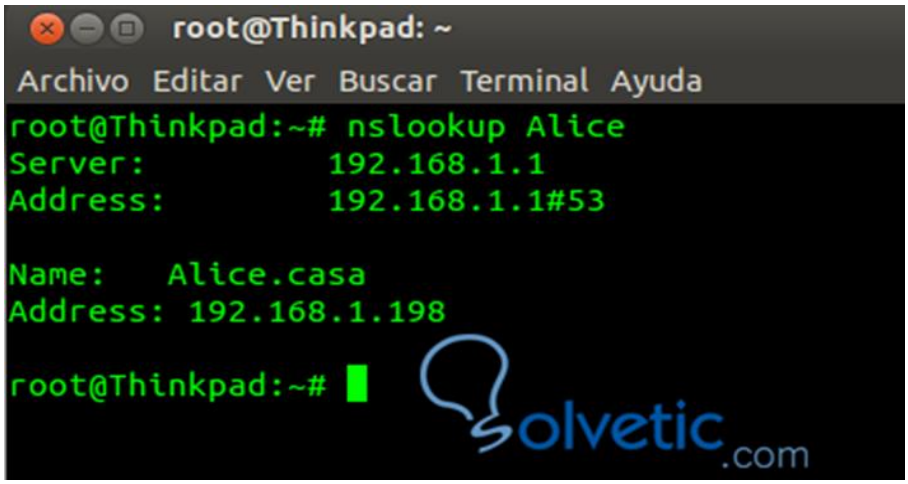
Sistemas involucrados

Tabla 2 DHCP Spoofing

Victima	Atacante
Dirección MAC: AA:BB:CC: 22:33:44	Dirección MAC: AA:BB:CC: 88:88:88
Dirección IP: 192.168.1.198/24	Dirección IP: 192.168.1.124/24
OS: Windows XP	OS: GNU/Linux Ubuntu 14.04
Gateway de la red: (DNS + DHCP)	
Dominio: casa	Dominio: casa Dominio: dhcp.spoofed.casa

El atacante desea aplicar una técnica DHCP Spoofing sobre Alice. Para ello puede identificar la dirección IP de Alice mediante el DNS local (nslookup), utilizando nbtscan, o cualquier otro método.

Ilustración 41



a. El Atacante instala un servidor DHCP, por ejemplo, isc. dhcp-server. Para ello en Ubuntu ejecutar el siguiente comando en la una terminal.

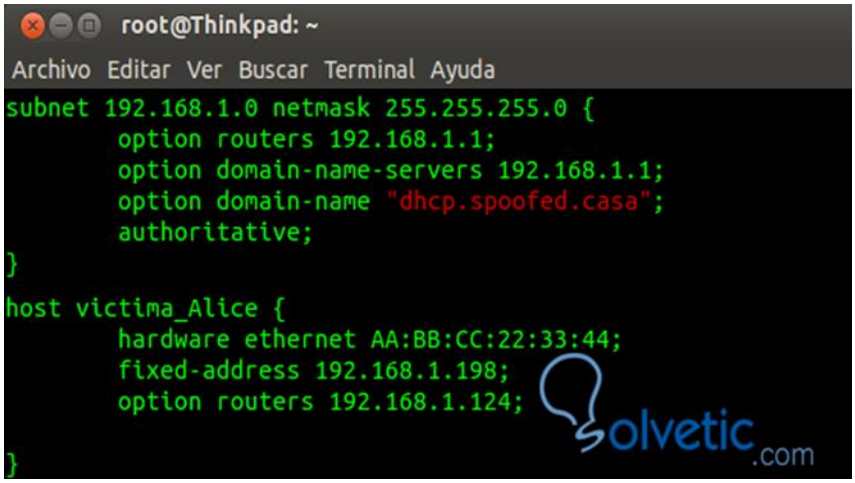
$ sudo apt-get install isc-dhcp-server

b. Para configurar el servidor DHCP el Atacante utiliza datos conocidos, como la IP de Alice, MAC de Alice (gracias ARP), Subred, DNS, etc. La configuración se realiza mediante la edición del fichero dhcpd.conf, en una terminal del

$ sudo vim /etc/dhcp/dhcpd.conf

Para este caso de estudio, el fichero de configuración debe lucir así

Ilustración 42



c. La sección “subnet” define la subred, máscara, puerta de enlace predeterminada de la red, servidor de nombres, etc. Se ha especificado también como dominio dhcp.spoofed.casa (a propósito, sólo para resaltarlo en las capturas de este tutorial).
Nótese que debajo, se ha especificado explícitamente una configuración para el host de Alice (bien diferenciado por su dirección MAC). En particular, se ha especificado como puerta de enlace para Alice, la dirección IP del Atacante mediante la instrucción

option routers 192.168.1.124

Y se ha forzado que se asigne la IP 192.168.1.198 a la MAC de Alice, respetando la configuración que asignó inicialmente el DHCP legítimo de la red

…hardware ethernet AA:BB:CC:22:33:44fixed-address 192.168.1.198...

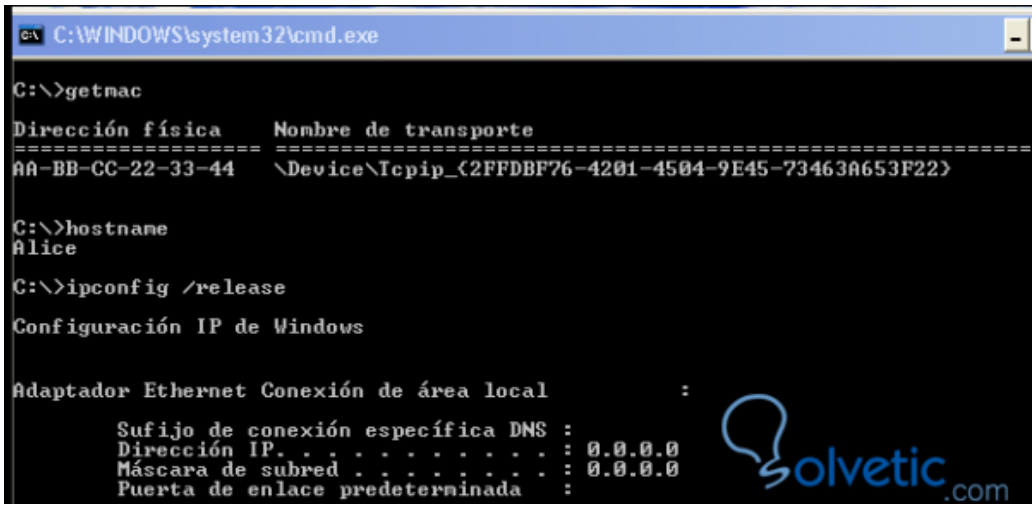
d. Una vez configurado, el atacante inicia el servicio de DHCP con el comando

$ sudo / etc/init.d/isc-dhcp-server start

Estaría iniciado. Para simular la condición de carrera, en un entorno controlado puede obligarse a Alice a volver a solicitar configuración mediante DHCP.
Para ello, Alice libera la dirección IP asignada (ejecutar en una terminal de Alice el comando)

C:\ipconfig / reléase

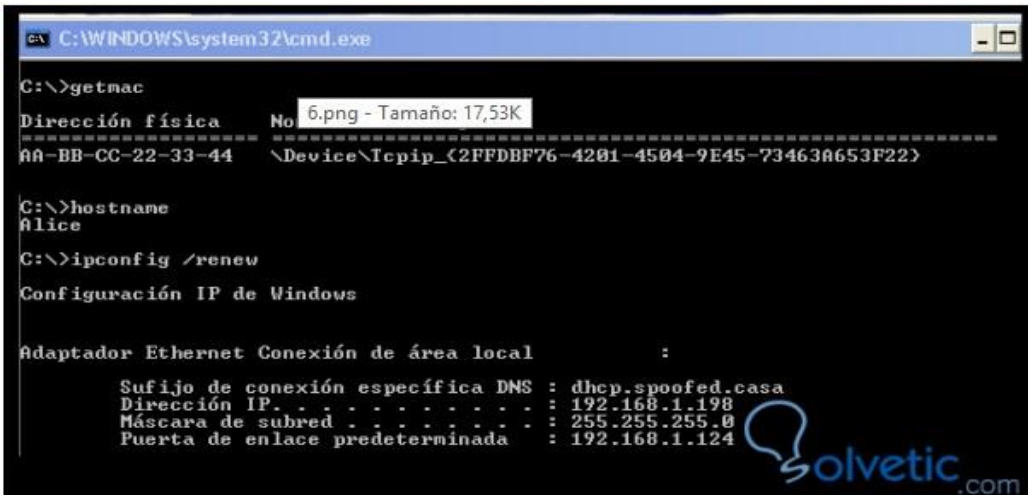
Ilustración 43



e. Luego solicita nuevamente una dirección IP : C:\ipconfig / renew

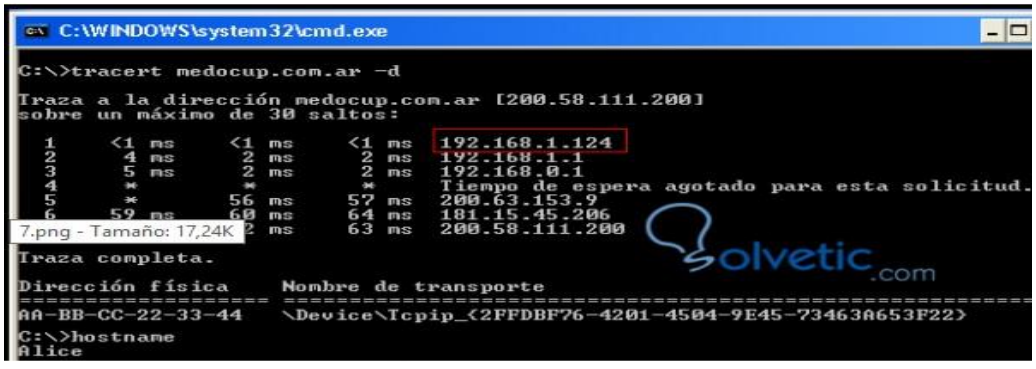
f. Si el atacante “gana la carrera” al servidor DHCP legítimo de la red, se asignarán los parámetros de configuración DHCP preconfigurados.

Ilustración 44



g. Alice ha obtenido la dirección IP “correcta” y se le ha asignado como puerta de enlace predeterminada la dirección IP del Atacante. Nótese el dominio “dhcp.spoofed.casa, a modo de referencia respecto a la configuración inicial. A partir de este punto, Alice enviará los paquetes destinados a Internet al Atacante, dado que se le ha indicado que la dirección IP 192.168.1.124 es su puerta de enlace predeterminada. Si desde la terminal de Alice se ejecuta una traza a 8.8.8.8, se puede observar el cambio en el primer salto.

Ilustración 45



10. HERRAMINETAS DE ATAQUES TÍPICOS EN UNA RED LAN

10.1 Sniffing[29]

Es un dispositivo que utilizando ARP Spoofing permite al atacante escuchar todo lo que circula en una red, básicamente Sniffing es robo de información que detienen, interpretan y almacenan los paquetes de datos que viajan por la red, para así analizar cada uno de esos datos como tales, contraseñas, mensajes de correo electrónico, datos bancarios, por tal razón es muy importante encripta la información como por ejemplo, el correo electrónico debe de enviarse encriptado con PGP o GNuPG, para que las personas inescrupulosas que están escuchando a través de la red, no puedan tener un acceso fácil a nuestra información.

10.2 Exploits[30]

Es una herramienta que le permite al atacante buscar y explotar fácilmente las vulnerabilidades conocidas de un sistema informático, con el propósito de obtener un comportamiento no deseado del sistema y así tomar el control de esta.

10.3 Backdoor[31]

Es una herramienta muy utilizada por los atacantes ya que este permite abrir y explorar “puertas traseras” en los sistemas, permitiéndoles manipular o controlar el sistema con fines malicioso, sin conocimiento alguno del usuario.

10.4 Rootkits[32]

Es una herramienta utilizada por los atacantes para acceder indebidamente a un sistema informático. Se debe agregar que también

[29] (vieites s.f.)
[30] (vieites s.f.)
[31] (vieites s.f.)
[32] (vieites s.f.)

los Rootkits se instalan como parte del sistema operativo reemplazando un servicio legítimo, proporcionando el control del equipo de la víctima.

10.5 Auto-rooters[33]

Herramientas capaces de automatizar totalmente un ataque, realizando toda la secuencia de actividades para localizar un sistema, escanear sus posibles vulnerabilidades, explotar una determinada vulnerabilidad y obtener el acceso al sistema comprometido[34].

10.6 Password crackers[35]

Es una aplicación que permite averiguar las contraseñas del sistema mediante un ataque de fuerza bruta o diccionarios de búsqueda siendo capaz de identificar incluso contraseñas encriptadas.

10.7 Spammer[36]

Es una herramienta que el atacante utiliza para enviar correos electrónicos no solicitados al usuario, con fines malicioso, para adquirir información personal de este, esta herramienta se utiliza para la suplantación E-MAIL y SMTP.

10.8 Kali Linux

Es una distribución basada en Linux este ofrece las herramientas necesarias para llevar a cabo los diferentes ataque DNS Spoofing, ARP Spoofing y así alterar las direcciones de los servidores DNS.

[33] (vieites s.f.)
[34] (vieites s.f.)
[35] (vieites s.f.)
[36] (vieites s.f.)

11. COMPARACION DE LOS PRODUCTOS DE SISTEMA DE DETECCION DE INTRUSO

Los sistemas de detección de intrusos son una herramienta que detecta las anomalías en la red, estas se clasifican es 2 tipos; NIDS y HIDS.

Los NIDS son herramientas que se encargan de la seguridad dentro de la red, este funciona como un sniffer el cual escucha todo el tráfico de la red en espera de actividades malintencionadas. Actualmente hay muchos productos comerciales basados en NIDS como Suricata, Snort, EasyIDS, entre otros. Dicho lo anterior, se procederá hacer una comparación de los dos productos de NIDS más populares en el mercado los cuales son Snort y Suricata, ambas alternativas se encargan de detectar intrusiones o tráfico sospechoso dentro de la red, gracias a las reglas que contiene ambas herramientas.

Hay que mencionar, además que las reglas en Suricata están compuestas por 3 partes: action, Header y rule action, cada una de estas partes tiene un conjunto de acciones sobre ese segmento de la regla que hacen que se restrinja en la búsqueda por esa firma o se realice una acción específica.

Por otra parte, las reglas en snort están formadas por 7 partes: action rule, protocolo, dirección IP, mascara y puerto origen, el sentido de la comunicación seguido por la dirección IP y por último el puerto destino. En la tabla 2, se compara el campo action de cada uno de estos productos IDS.

A continuación, se muestra una tabla comparativa entre Snort y Suricata, esta comparación será basada en las respectivas características similares que hay entre ellas[37].

[37] (Martin Roesch 2017)

Tabla 3 Comparación de dos productos de NIDS

Características	Snort	Suricata
Filtro por dirección IP/ puerto	Filtros por dirección IP y puerto **(rango).** búsqueda por contenido en la carga útil del paquete o payload	Filtra por puerto de origen con la función **any,** o por rango.
Análisis de protocolo/ paquetes	Análisis de protocolo, TCP, UDP, IP y ICMP.	Análisis por firma, análisis de paquetes y análisis por protocolos IP, TCP, UDP y ICMP, HTTP, FTP, TLS, SMB, DNS.
Modo de alerta	Tiene 7 modos de alerta en línea de órdenes, que permite gestionar de qué forma se mostrara la información de cada uno de las alertas, las cuales son: • Fast. • Full. • Socket. • Console. • None. • SMB y • Syslog.	Tiene 1 modo de alerta, que le notifica al administrador del sistema cuando se produce un evento sospechoso.

Reglas	Las reglas se pueden restringir por búsquedas del cuerpo y encabezado HTTP o por tiempo de vida del paquete. Snort en su campo action tiene disponible las siguientes acciones: • Alert. • Log. • Pass. • Activate. • Dynamic. • Drop. • Reject y • Sdrop.	Las reglas están compuestas por: • Action. • Header y • Rule options. En el campo Action en suricata tienen disponibles algunas de estas acciones, las cuales son: • Alert. • Pass. • Drop y • Reject.
Hilo de Ejecución	Trabaja con un solo hilo.	Trabaja con multi-hilos.
Detección automática de protocolo	No	Si
Análisis avanzado de http	No	SI
Soporte, IPV6 y reglas de Snort	Si	Si

Se debe agregar, que generalmente en las organizaciones se prefiere Suricata sobre Snort por su capacidad multi-hilos, debido a que es compatible con procesadores de uno o varios núcleos.

En cuanto a los HIDS este es un sistema de detección de intrusos basado en host, que busca actividades sospechosas analizando el sistema constantemente.

Así mismo, puede detectar y responder a actividades maliciosas que estén en su entorno. Por otra parte, existen diferentes productos comerciales basados en HIDS, como OSSEC, Tripwire, Dragon, RPM como IDS, SWATCH, entre otros.

Dicho lo anterior, se procederá hacer una comparación de los productos HIDS populares en el mercado los cuales son: OSSEC y Tripwire. Estas son una herramienta de código abierto que monitorizan y detectan las anomalías que pueden producirse en el sistema.

A continuación, se muestra una tabla comparativa entre OSSEC y Tripwire.

Tabla 4 comparación de dos productos de HISD

Características	**OSSEC**	**Tripwire**
Sistemas operativos soportados	Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac y VMware ESX*	Linux y *nix
Analizador de integridad de archivos (FIM)	Búsqueda de cambios en archivos causados por: • Ataque. • Mal uso. • Directorio. • Registro.	Detectar e informar cualquier cambio no autorizado en archivos y directorios, busca cambios en: • Tamaño de archivos internos.

	• Otro archivo.	• Detalles, marca de tiempo de modificación. • Marca de tiempo y de acceso. • Permisos de archivos y propiedades. • Adicción, eliminación y modificación de archivos. • Tipo de archivos. • Fecha de última. modificación • Firma del archivo.
Analizador correlacionado de logs.	Recopila, analiza y correlaciona los registros cuando sucede un evento para saber si algo malo está pasando.	No detecta intrusiones realizadas antes de su instalación guarda lo que pasa en el sistema en logs, para su posterior análisis.
Analizador de registro de Windows	• Busca procesos escondidos • Busca puerto escondidos • Revidar todas las interfaces en modo promiscuo.	No tiene unos analizados de registro en Windows.
Alertas en tiempo real	Si	No

Detector de rookits	• Identificación basada en firmas. • Identificación basada en anomalías.	si
Tipo de respuesta	Activa (Respuesta automáticas inmediatas)	Activa

12. TOPOLOGIA DE RED

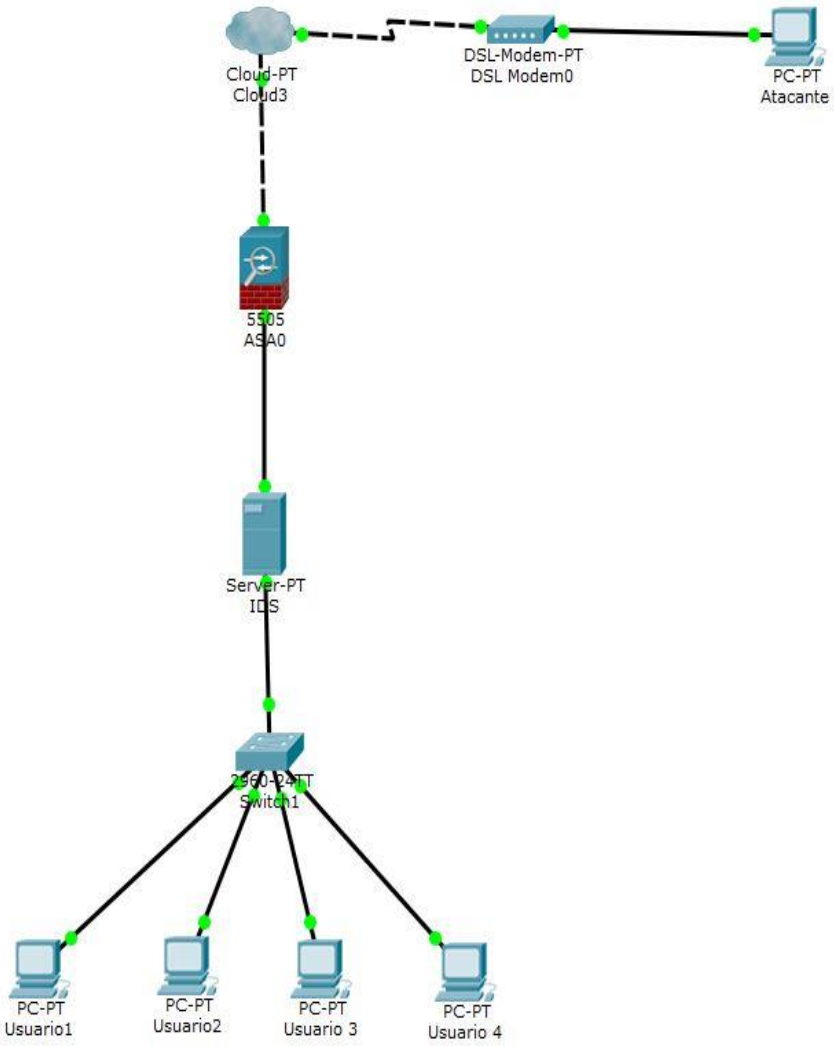
La topología de red que se desplegó para el presente proyecto, está diseñada para analizar el comportamiento de los diferentes IDS y así realizar los ataques y validar las respuestas que se originaran de esta prueba.

Esta topología de red se compone por un firewall que permitirá bloquear accesos no autorizados y un switch que interconecta los equipos dentro de la misma red.

A este diseño se le incorporo un sistema de detección de intruso (IDS), que completará la seguridad en la red de dicha topología, la colocación del IDS detrás del firewall nos permitirá monitorizar todo el tráfico que no se ha detectado por el firewall, por lo que será considerado como maliciosos en un alto porcentaje.

A continuación, se podrá observar la topología de la red.

Ilustración 46



13. ESTRATEGIA DE MEDICION DE LA EFECTIVIDAD DE LOS IDS DENTRO DE CADA CATEGORIA

13.1 Estrategia de medición de productos basado en NIDS

Como se pudo ver en el capítulo 11, donde se hizo la comparación de los productos comerciales basado en NIDS, llamados Snort y Suricata se pudo ver y analizar, que Suricata es preferido en el mercado por su capacidad de procesamiento multi-hilos, puesto que ofrece compatibilidad con diferentes procesadores de uno o varios núcleos, por otro lado, Snort solamente cuenta con un procesador que ofrece un solo hilo, el cual repercute en la capacidad de analizar una anomalía en la red y ejecutar un procedimiento de respuesta a dicho ataque.

Por lo tanto, se vio la necesidad de diseñar una estrategia de medición de la efectividad de la detección para cualquier IDS, realizando ataques Spoofing DNS y ataques Spoofing ARP, ya que tanto Snort y Suricata, disponen de firmas para ellos, por lo que tendrían que ser detectados cuando se haga un ataque de ese tipo.

A continuación, se mostrará la estrategia de medición basados en los elementos de comparación de la tabla 2.

Herramientas utilizadas

- Maquina atacante: Kali Linux, versión 2017.2.
- Maquina víctimas: Snort y Suricata.
- Para analizar el tráfico de red y protocolos se utilizará wireshark.

Procedimiento

1. Montar la topología de red que se muestra en el capítulo 12, ilustración 46, en el laboratorio de NYQUIST.
2. En cada una de las maquinas víctimas se debe instalar Snort y Suricata, respectivamente.

3. Revisar la conectividad de las máquinas.

4. El atacante conociendo la dirección IP de las maquinas victimas al cual quiere intervenir, realizará 10 ataques Spoofing ARP, y luego realizará 10 ataques Spoofing DNS.
5. Durante el ataque se procederá analizar:
   a) Ataques detectados por Snort vs Ataques detectados por Suricata, este se medirá por el número de ataques realizados, respecto al número de anomalías detectadas.
   b) Captura automática de los protocolos en Snort y Suricata, empleando wireshark
   c) Medir la cantidad de memoria que consume Snort al realizar un proceso de detección vs Cantidad de memoria que consume Suricata al realizar un proceso de detección.
   d) Contar el número de paquetes procesados por Suricata vs Número de paquetes procesados por Snort, se enviaran 10 paquetes a Snort y Suricata.
   e) Comparar el número de paquetes filtrados por dirección IP/ Puerto en Snort vs número de paquetes filtrados por dirección IP/Puerto en Suricata.
   f) Número de alertas activadas por paquetes detectados en Snort vs número de alertas activadas por paquetes detectados en Suricata.
   g) Análisis del protocolo capturados en el ítem b (Análisis de protocolo/paquete en Snort vs Análisis de protocolo/paquete en Suricata).
   h) Comparar el número de paquetes entrante procesado por Snort vs Paquetes entrantes procesado por Suricata.
   i) Comparar el número de paquetes entrante descartado por Snort vs Paquetes entrantes descartado por Suricata.
   j) Análisis del consumo del procesador de Snort vs el consumo del procesador de Suricata cuando existe un tráfico entrante.

13.2 Estrategia de medición de productos basado en HIDS

Como se pudo ver en el capítulo 11, donde se hizo la comparación de los productos comerciales basado en HIDS llamados OSSEC y Tripwire se pudo analizar que Tanto OSSEC como Tripwire son excelentes herramientas de código abierto HIDS. Ambos tienen fortalezas y debilidades únicas, aunque OSSEC cuenta con características más completas que Tripwire Open Source.

A continuación, se mostrará la estrategia de medición basados en los elementos de comparación de la tabla 3.

Software utilizado

- Maquina atacante: Kali Linux, versión 2017.2
- Maquinas víctimas: OSSEC y Tripwire.

Procedimiento

1. Montar la topología de red que se muestra en el capítulo 12, ilustración 46, en el laboratorio de NYQUIST.
2. En cada una de las maquina victimas instalar OSSEC y Tripwire respectivamente.
3. Revisar conectividad.
4. El atacante conociendo la dirección IP de las maquinas victimas al cual quiere intervenir, realizará 10 ataques Spoofing ARP, y luego realizará 10 ataques Spoofing DNS.
5. Durante el ataque analizar:
    a. Ataques detectados por OSSEC vs Ataques detectados por Tripwire.
    b. Numero de alertas activadas al detectar anomalías en OSSEC vs Alertas activadas al detectar anomalías en Tripwire.
    c. Detección de abusos o firmas.
    d. Numero de archivos analizados en OSSEC vs archivos analizados en Tripwire.

e. Número de cambios realizados a archivos críticos del sistema detectados por OSSEC vs Número de cambios realizados a archivos críticos Tripwire
f. Cantidad de memoria consumida por OSSEC vs cantidad de memoria consumida por Tripwire.

Esta estrategia de medición nos va a permitir analizar y verificar que tan efectivos son estos productos a la hora de detectar las anomalías que se presentan en la red, y cuál producto sería óptimo para tener una red segura.

14 PRUEBAS Y RESULTADOS

En este capítulo, se trabajará con los cuatro IDS más populares que se encuentran a disposición del público, los cuales son: Snort, Suricata, OSSEC y Tripwire. El principal objetivo de trabajar con ellos, es tener un punto de comparación con el IDS desarrollado. De esta manera, es posible comparar el desempeño de cada uno de ellos mediante la estrategia implementada en el capítulo 13.

14.1 Pruebas de desempeño de cada uno de los IDS

En este apartado se podrán a prueba los IDS programado, Snort, Suricata, OSSEC y Tripwire, basándose en la estrategia de medición de comparación para estos productos (ver capítulo 13).

14.1.1 Escenario para las pruebas

El escenario utilizado para las pruebas está compuesto por un IDS, firewall, switch, modem y por cinco computadores, uno será el atacante, y las otras serán las víctimas. El atacante realizará ataques de suplantación ARP y ataques de suplantación DSN en contra de la víctima, la cual tendrá servicios corriendo en ellas. Se harán pruebas con cada uno de los IDS (Snort, Suricata, OSSEC, Tripwire), con el objetivo de comparar los resultados entre Suricata, Snort y OSSEC, Tripwire. La ilustración 46, muestra el escenario para llevar a cabo las pruebas de los IDS.

14.1.2 Desarrollo de las pruebas

Se compararán cada uno de los IDS dentro de la misma categoría. Contra ataques de suplantación ARP y contra ataques de suplantación DNS. De esta manera se pone en práctica la estrategia de medición de la efectividad de los IDS.

14.2 Comparación y evaluación de resultados

Los resultados que presentan Snort, Suricata, OSSEC y Tripwire, son importantes para esta investigación, debido a los diferentes ítems analizados anteriormente para cada producto IDS open source comparado en su categoría se podrá hacer un análisis de estas respuestas y así respectivamente hacer una comparación de estos productos.

La tabla 5 y la tabla 6. Muestra en detalle los resultados de la estrategia que se implementó para comparar cada uno de los IDS.

Tabla 5 comparación de los productos basado en NISD

	Snort	**Suricata**
Ataques Spoofing ARP detectados, ver ilustración (48)	80%/100%	0/100%
Ataques Spoofing DNS detectados, ver ilustración (47)	0/100%	80/100%
Captura automática		

de protocolos, ver ilustración (51 y 52)	ICMP, TCP, ARP	ICMP, TCP, DNS
Cantidad de memoria consumida al realizar un proceso de detección, ver ilustración (53)	1.9MB	1.7MB
Número de paquetes procesados, ver ilustración (58 y 59)	100%/100%	100%/100%
Número de paquetes filtrados por dirección IP/ Puerto, ver ilustración (58 y 59)	100%/100%	100%/100%
Número de alertas activadas por paquetes detectados, ver ilustración (55 y 56)	29	38
Análisis de protocolo/paquete, ver ilustración (58 y 59)	ICMP	ICMP
Número de paquetes entrantes descartados	0/100%	0/100%
Análisis del consumo del procesador, ver ilustración (53)	4,6%	3.3%

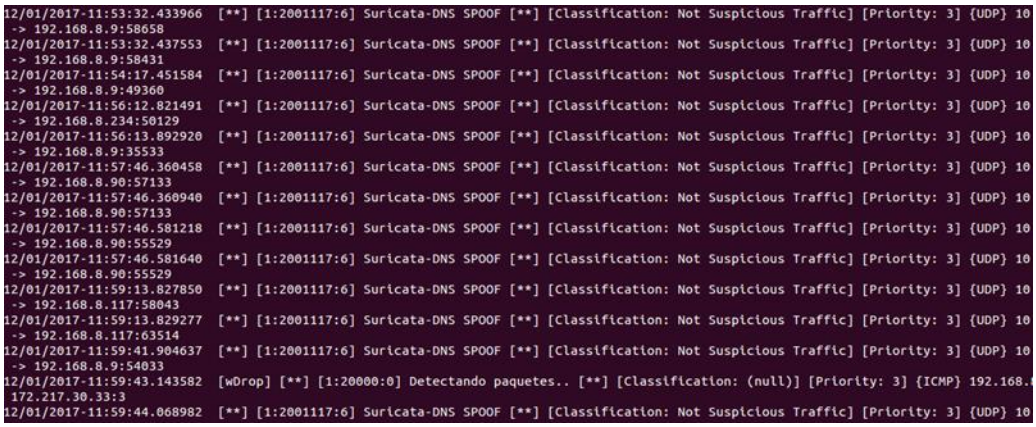
Prueba con Suricata

Durante las pruebas realizadas al IDS Suricata, se realizaron los diez ataques Spoofing ARP y DNS, como se estipulaba en la estrategia de medición de los IDS en el capítulo 13, sin embargo, a la maquina victima que tenía instalado dicho producto, a la cual se le realizaron ataques de tipo Spoofing ARP, Suricata no detectó estos ataques, básicamente esto sucedió porque Suricata no cuenta con una regla para detectar este tipo de ataques.

La Regla que se utiliza en Suricata para detectar ataques Spoofing DNS es:

alert udp $EXTERNAL_NET 53 -> $HOME_NET any (msg:"Suricata DNS SPOOF query response PTR with TTL of 1 min. and no authority"; flow:to_client; content:"|85 80 00 01 00 01 00 00 00 00|"; content:"|C0 0C 00 0C 00 01 00 00 00|<|00 0F|"; fast_pattern:only; metadata:ruleset community, service dns; classtype:bad-unknown; sid:253; rev:14;)

Ilustración 47



Prueba con Snort

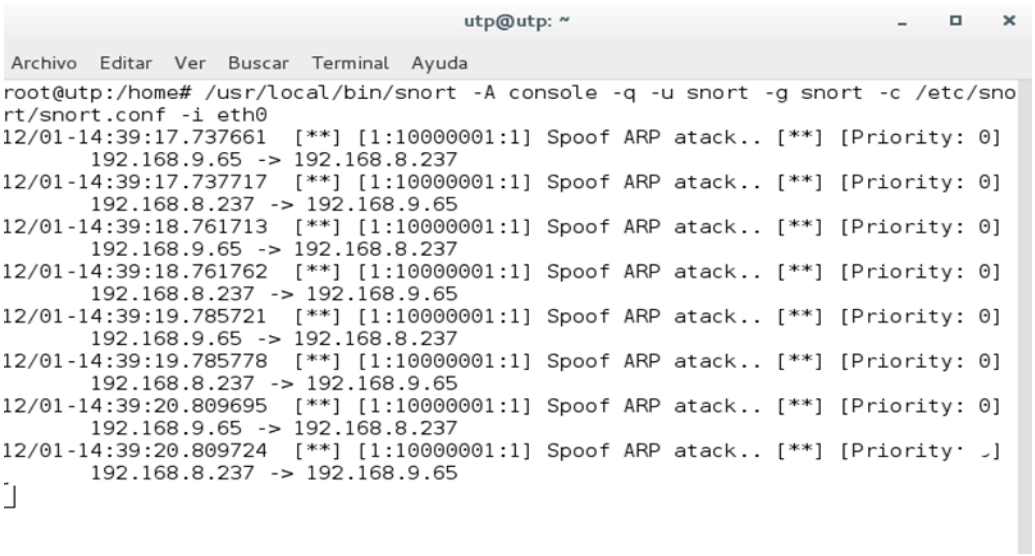
Durante las pruebas realizadas al IDS Snort, se puso en práctica las estrategias de medición del capítulo 13, sin embargo, cuando se realizó el ataque DNS Spoofing, no se generaron ninguna alerta, ya que básicamente Snort no detecta este tipo de ataques, porque no cuenta con una regla para detectarlos. Pero si cuenta con una regla para detectar ataques ARP Spoofing, esta regla ya viene por defecto en Snort.conf, a continuación, se puede ver dicha regla.

preprocessor arpspoof

preprocessor arpspoof_detect_host: 192.168.8.237 20:6a:8a:b4:f5

Esta regla lo que permite es que él preprocessor inspeccione las direcciones Ethernet, para detectar ataques ARP Spoofing o paquetes ARP y decodificar esos paquetes, generando una alerta de una solicitud de ARP detectado.

Ilustración 48



En las siguientes ilustraciones 48 y 49, se podrá apreciar la comparación que se hace con respecto a los resultados obtenidos de la tabla 5, en donde se compara los Ataques detectados por Snort con Ataques detectados por Suricata.

Ilustración 49

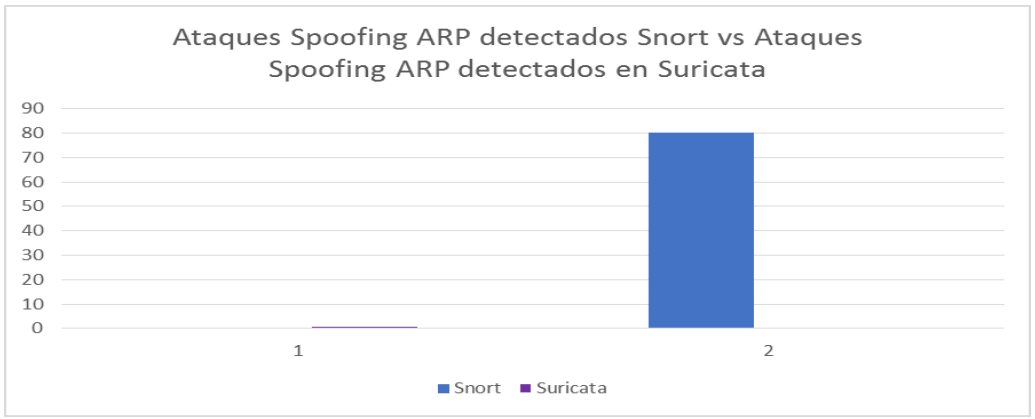
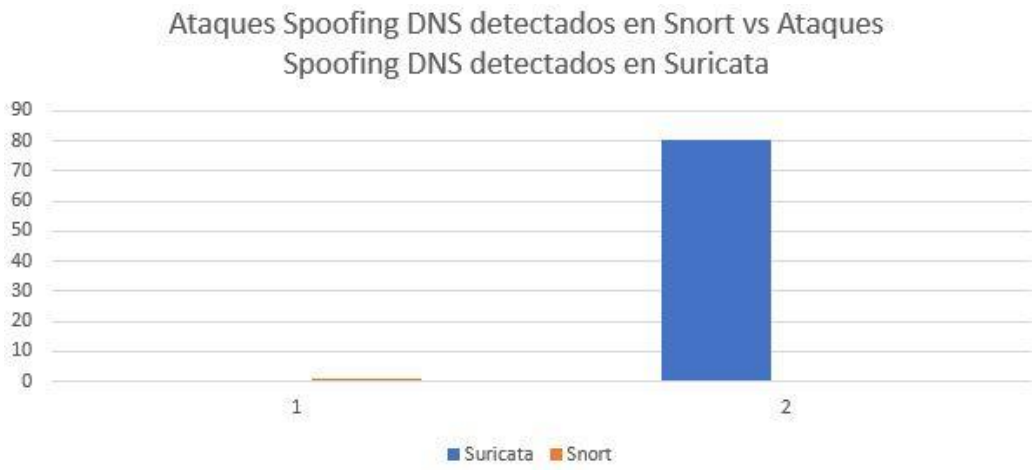


Ilustración 50



Como se pudo ver, de los 10 ataques que se realizaron basados en la estrategia de medición del capítulo 13, a los productos basados en NIDS. Tanto Snort como Suricata detectaron un 80% de los ataques, ARP Spoofing Y DNS Spoofing, ya que básicamente, cuentan con unos parámetros o reglas para detectar esos tipos de ataques, como se mencionaba anteriormente.

Por otra parte, en las ilustraciones 50 y 51, se puede apreciar la captura automática de los protocolos empleando wireshark cuando se está realizando los ataques.

Ilustración 51

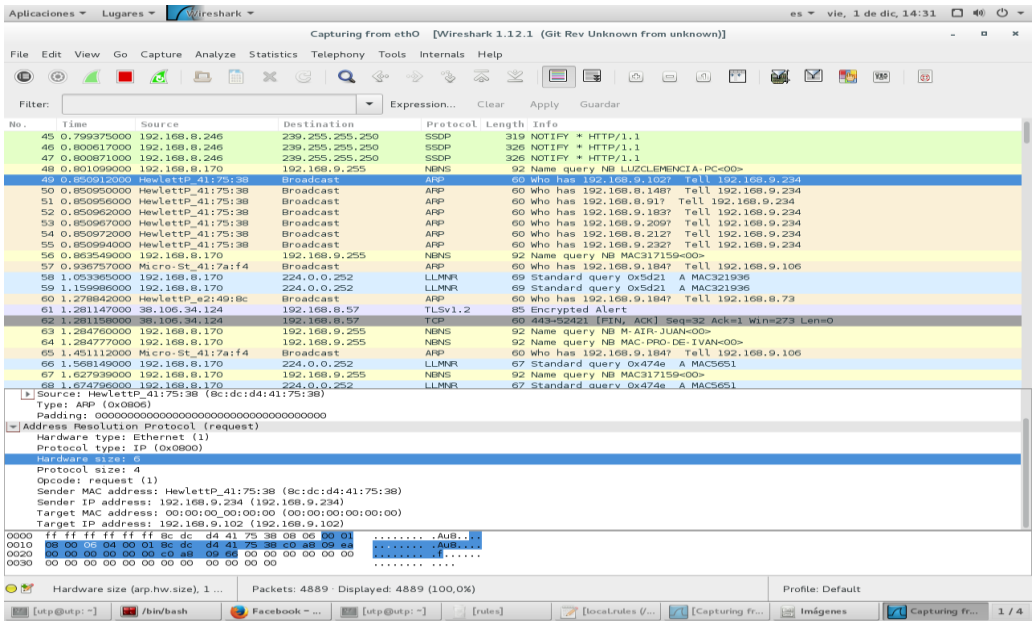
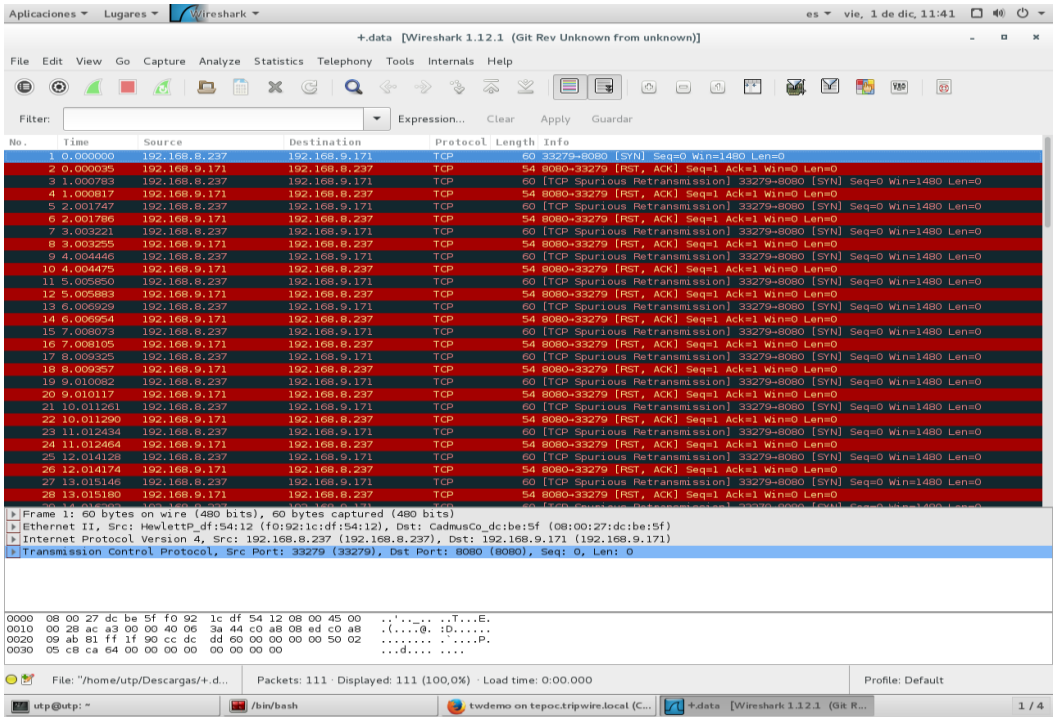
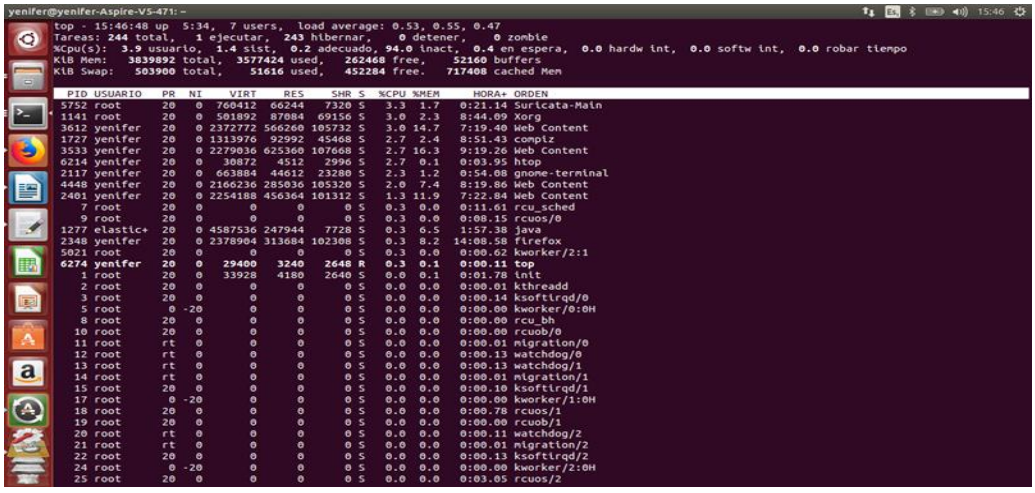


Ilustración 52



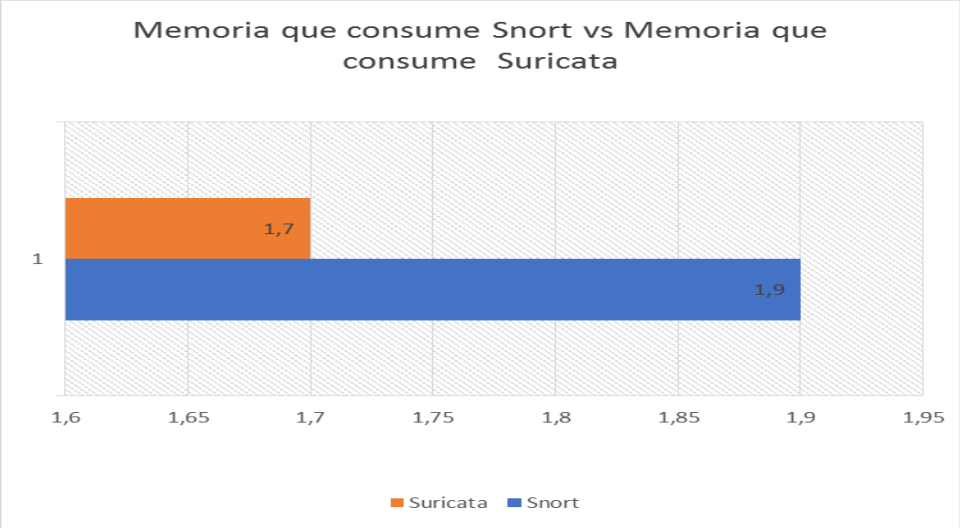
Para analizar la cantidad de memoria que consume Snort y Suricata al Realizar un proceso de detección se utilizó TOP, es un programa que viene instalado por defecto en el sistema operativo Linux, que muestra la cantidad de CPU o Memoria que se consume al realizar un proceso.

Ilustración 53



Si miramos en la ilustración 53, se verá la cantidad de memoria consumida al realizar un proceso de detección en Snort con la cantidad de memoria consumida al realizar un proceso de detección en Suricata.

Ilustración 54



Como se pudo apreciar en la ilustración 53, Snort tuvo un aumento de 2%, en consumir la memoria a la hora de realizar un proceso de detección con respecto a Suricata, al de detectar un ataque, Esto Puede ser debido al exceso de descarte de ataques o la complejidad a la hora de analizarlos.

Otro punto importante a tratar, son las alertas que se generan cuando se detectan alguna anomalía o paquetes en la red, estas alertas se pueden ver en Snort cuando se accede al directorio de los logs y se abre el archivo alert y en Suricata cuando se ejecuta stats.log que lo que hace es arrojar la estadística y análisis de rendimiento o si se ejecuta /usr/bin/suricata/ -c /etc/suricata/suricata.yaml -i eth0 que se utiliza para correr Suricata y cuando este termine de ejecutarse o si se cancela la ejecución este arrojara unas estadística del análisis de la red, a continuación, se podrá apreciar en las siguientes ilustraciones.

Ilustración 55

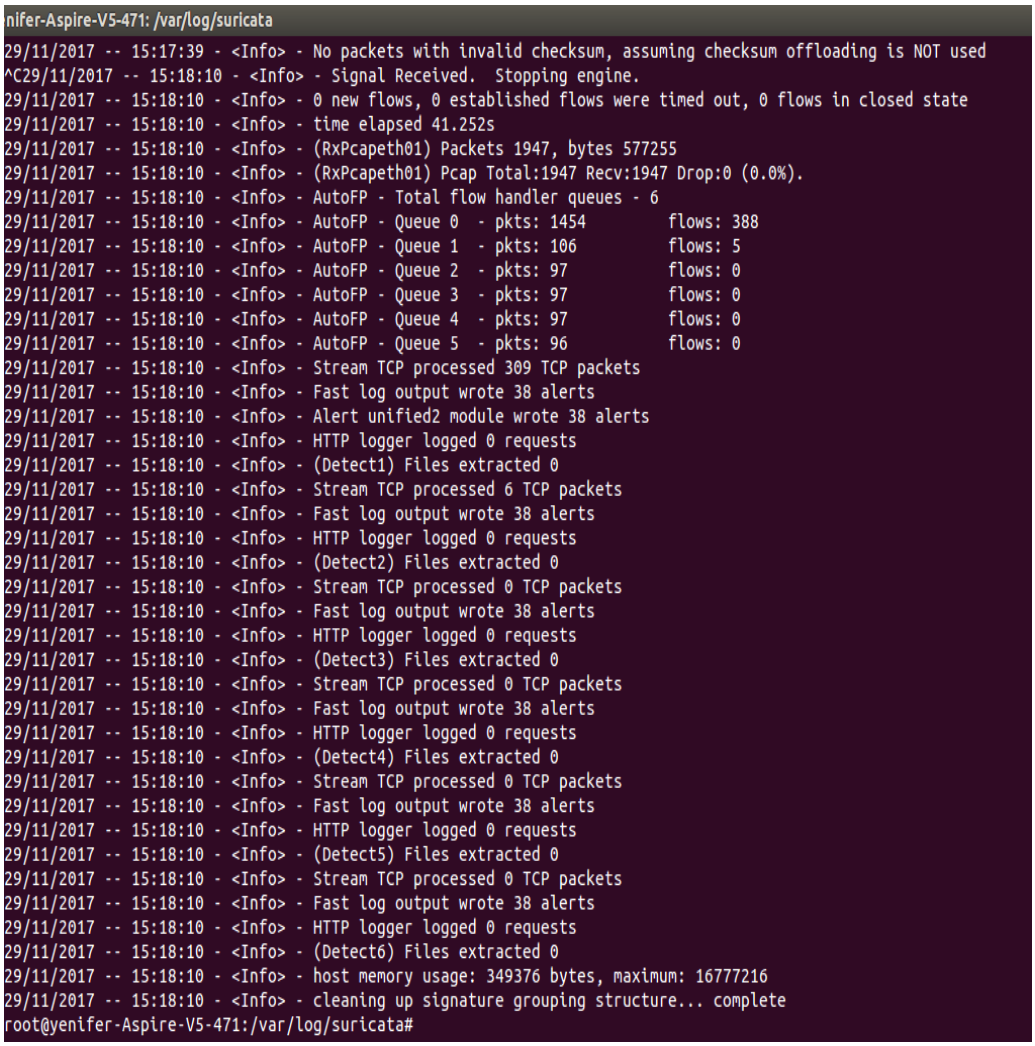
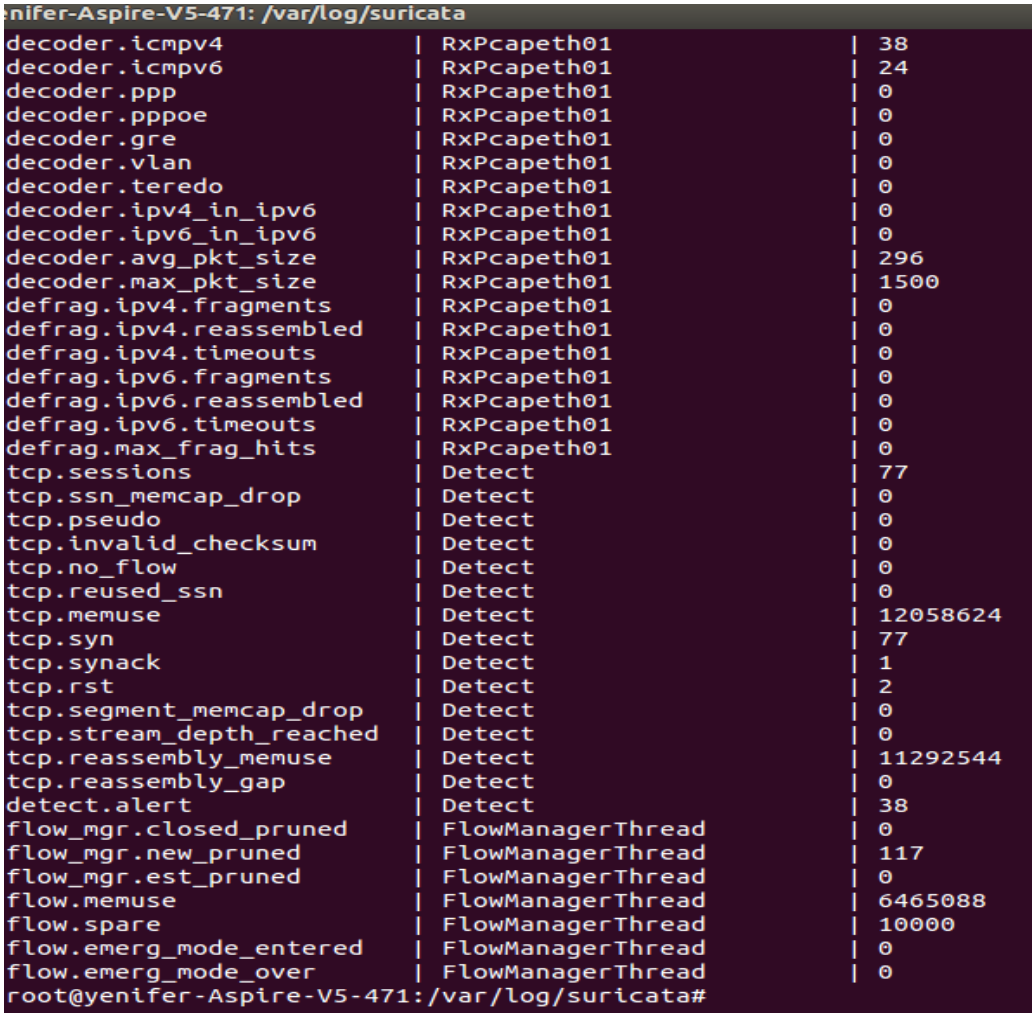
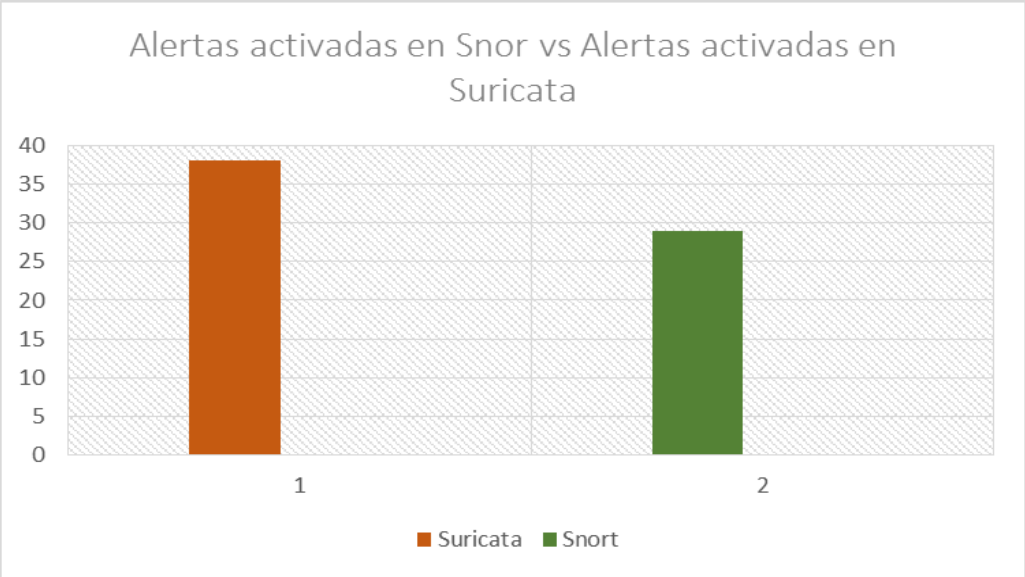


Ilustración 56



Ahora se podrá apreciar la comparación entre Snort y Suricata con respecto a las alertas que se activaron.

Ilustración 57



Este alto índice de alertas que se generaron en Snort y Suricata con respecto a los ataques que se realizaron, se les atribuye a los falsos positivos que se generaron en las pruebas. Las alertas de falsos positivos en los IDS pueden ser o no exitosas, (Ver capítulo 7.1.3.1)

Reglas utilizadas para detectar paquetes

Para esta prueba se crearon unas reglas nuevas en Snort y Suricata que permita detectar una petición de paquetes ICMP, generando una alarma “Detectando Paquetes” cuando detecta dicha petición, la regla en Suricata es la siguiente:

drop icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"Detectando paquetes..";sid:20000;)

Y la regla en Snort es la siguiente:

alert icmp any any -> $HOME_NET any (msg:"Detectando paquetes."; sid:10000001; rev:001;)

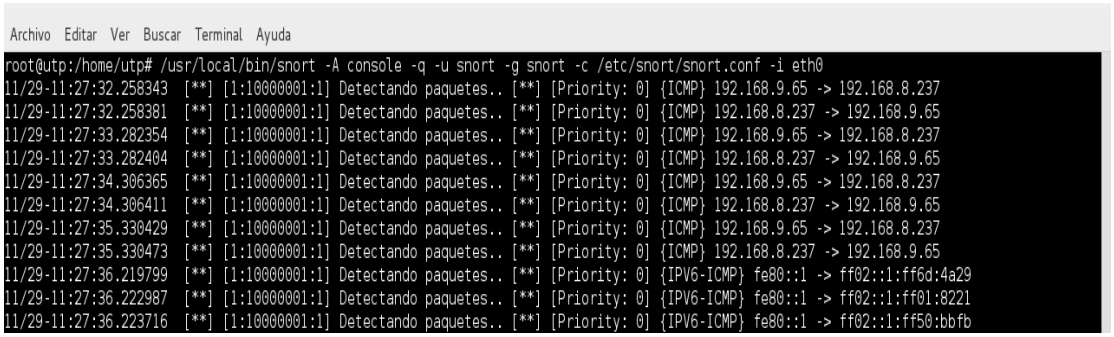
Para entender las reglas en Snort y Suricata ver capítulo 7.1.2.4.1.4

La dirección IP donde se originó el paquete es 192.168.9.65 de la máquina atacante, una vez el atacante hizo la petición de paquetes a la maquina victima con dirección IP 192.168.9.30 que tiene instalada Suricata se originó una alerta como se puede ver en la ilustración:

Ilustración 58

Y en la maquina victima que tiene instalado Snort con dirección IP 192.168.8.237 se originó la siguiente alerta (ver ilustración 58)

Ilustración 59



Como se podrá ver las alertas que se originaron en Snort y Suricata corresponde a las reglas que se crearon para detectar las peticiones de paquetes ICMP, estás alerta se activan cuando ha detectado algún paquete en la red.

En la ilustración 59, se compara el número de paquetes procesados por Suricata con el número de paquetes procesados por Snort, el eje X refleja el número de paquetes recibidos y el eje Y el tiempo medidos en mili segundos(ms). En la ilustración 60, se compara el número de paquetes entrante descartado por Snort con paquetes entrantes descartado por Suricata, podrán ver que tanto Snort como Suricata no descartaron ningún paquetes entrante ya que todos fueron recibidos.

En la ilustración 61, se compara el número de paquetes filtrados por dirección IP/ Puerto en Snort con el número de paquetes filtrados por dirección IP/Puerto en Suricata

Ilustración 60

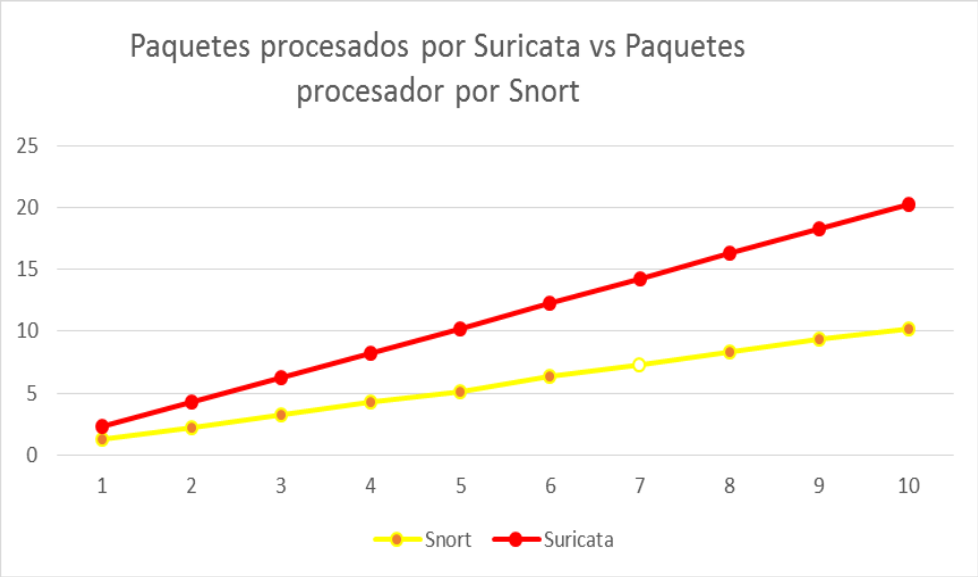


Ilustración 61

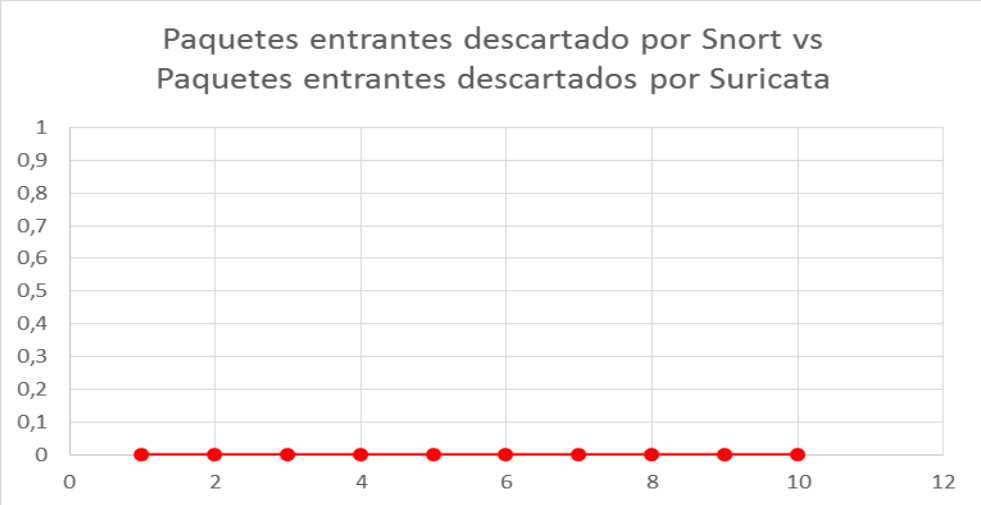
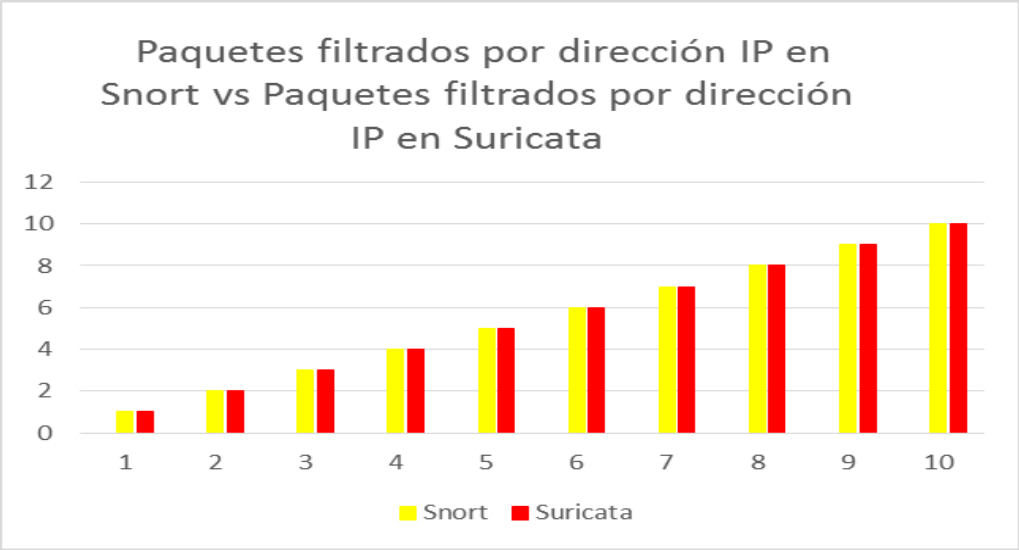
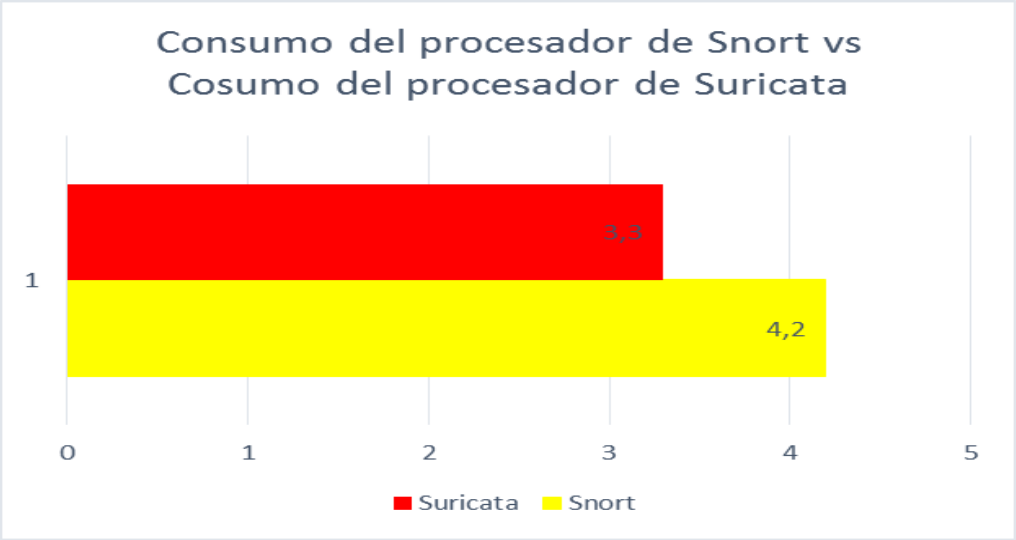


Ilustración 62



Otro dato importante es la cantidad de consumo del procesador cuando existe un tráfico entrante ya que un exceso de descarte de paquetes puede confundir la falta de CPU, para calcular la cantidad que consume Snort y Suricata cuando hay un tráfico entrante se utilizó TOP, (ver imagen 52), este programa muestra la cantidad de CPU que se consume. La ilustración 62, muestra el consumo del procesador de Snort con el consumo del procesador de Suricata cuando existe un tráfico entrante.

Ilustración 63



Como se puede ver Snort consume mucho más procesador que Suricata cuando hay un tráfico entrante, esto sucede porque Snort solo cuenta con un procesamiento de un solo hilo, en el cual implica en la capacidad de analizar o procesar una anomalía o un paquete en la red, mientras que Suricata cuenta con un procesamiento de multi-hilos, lo que le permite analizar de forma rápida el tráfico o anomalías que haya en la red.

Tabla 6 comparación de los productos basado en HISD

	Tripwire	OSSEC
Ataques detectados	0/100%	0/100%
Número de alertas activadas, ver ilustración (67 y 68 y 69)	106	224
Número de archivos analizados, ver ilustración (67 y 72)	20	23
Número de cambios realizados a archivos críticos del sistema, ver ilustración (65)	2	4
Cantidad de memoria consumida, ver ilustración (64 y 74)	326.38 MB	227.45 MB

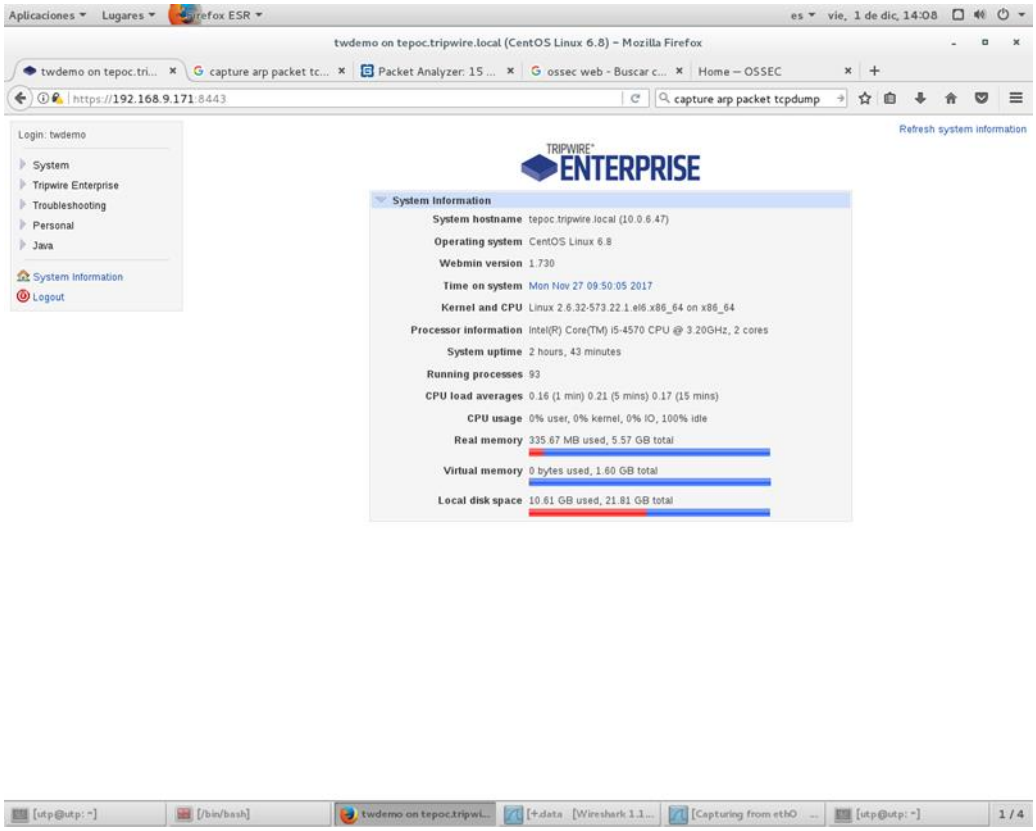
Prueba con Tripwire

Para las pruebas con Tripwire se utilizó una versión demo, para poner en práctica la estrategia de medición de los productos basado en HIDS,

cuando se realizaron los ataques Spoofing ARP y DNS, este producto no detecto ninguna amenaza, ya que el no detecta ataques ARP Spoofing y DNS Spoofing, lo que el detecta son los cambios en los archivos críticos del sistema en tiempo real.

En la siguiente ilustración se podrá ver un sistema de información que muestra Tripwire Enterprise cuando se accede a él, mostrara la memoria real que se están utilizando, la memoria virtual, entre otros.

Ilustración 64



Pruebas con OSSEC

Durante las pruebas a OSSEC, cuando se realizaron los diferentes ataques propuestos en la estrategia de medición de los HIDS, OSSEC no detecto ningún ataque, ya que este producto no detecta este tipo de ataques.

A continuación, se podrá ver en las siguientes ilustraciones, la lista de alertas que OSSEC y Tripwire muestra cuando hay algún cambio en un archivo. OSSEC envió una alarma cuando se ejecutó ossec-control start, este comando se utiliza para inicializarlo, se generó una alerta cuando se realizó un cambio en el archivo apache2.conf, el archivo emerging-dns.rules, y también cuando se realizó un nuevo de paquetes dpkg, entre otros. En Tripwire cuando se realizó un cambio al archivo critico a la capeta /dev, este es un directorio contiene todos los archivos especiales para dispositivos de hardware, Tripwire arrojo una alerta respecto a los cambios que se generaron en ese archivos.

Ilustración 65

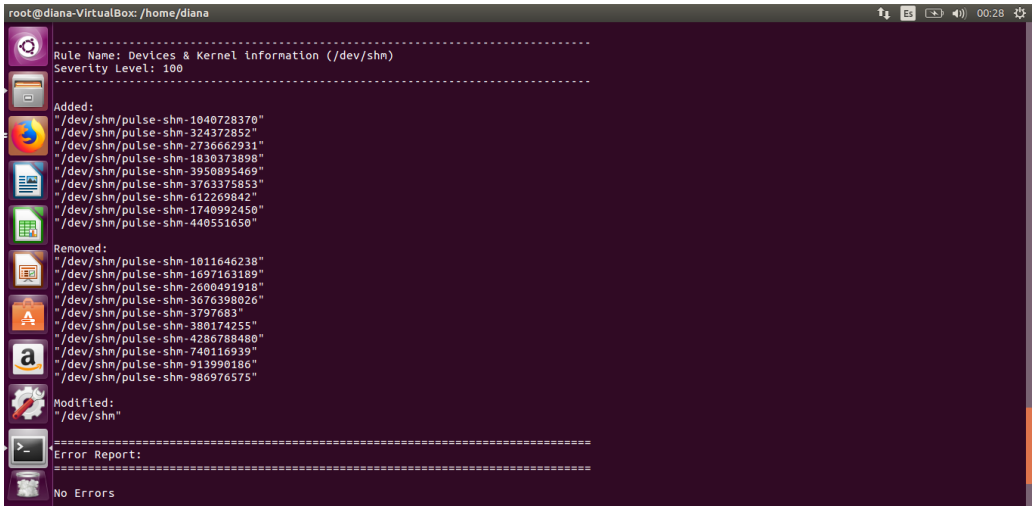


Ilustración 66

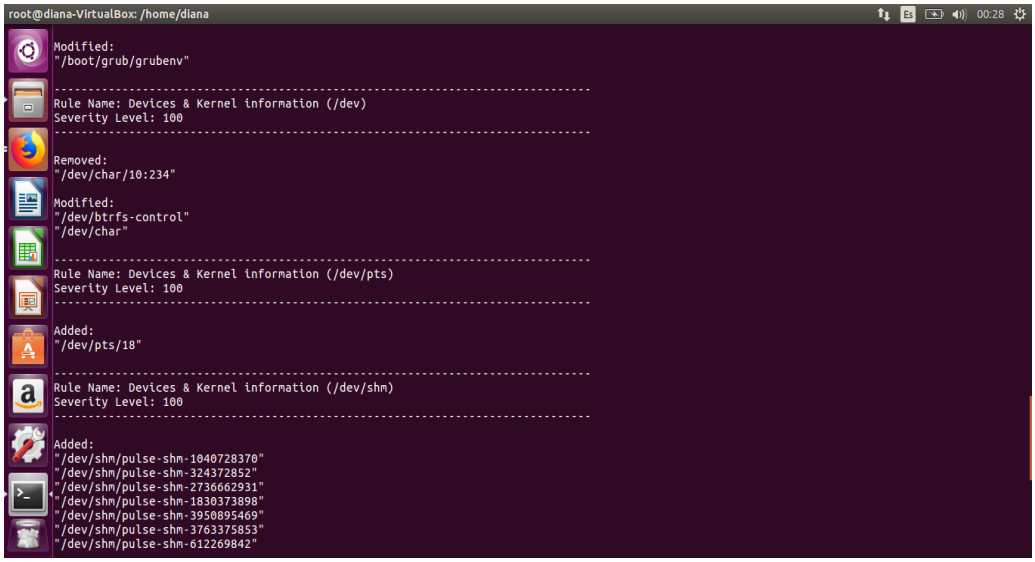
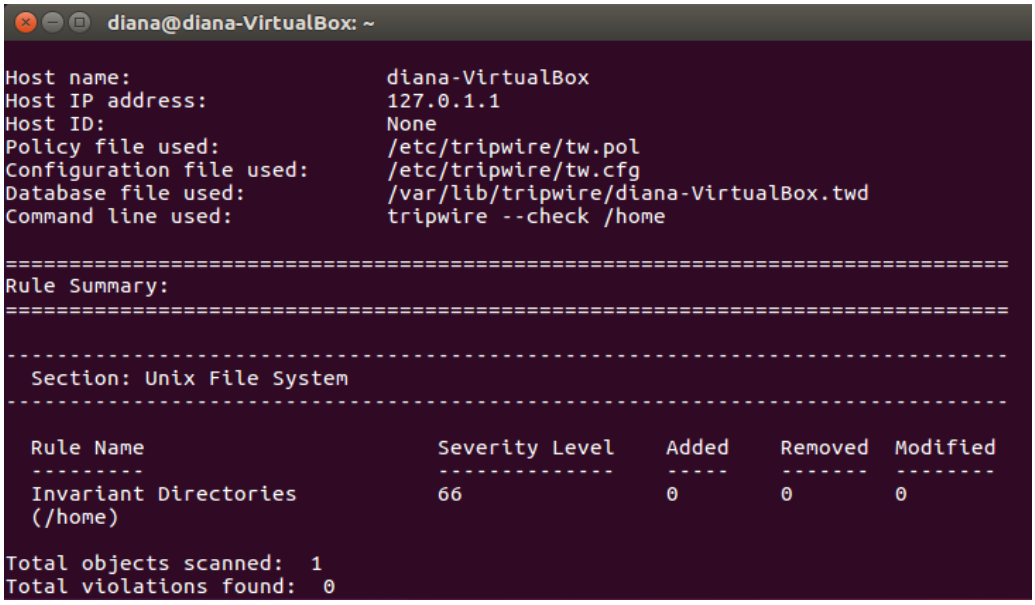


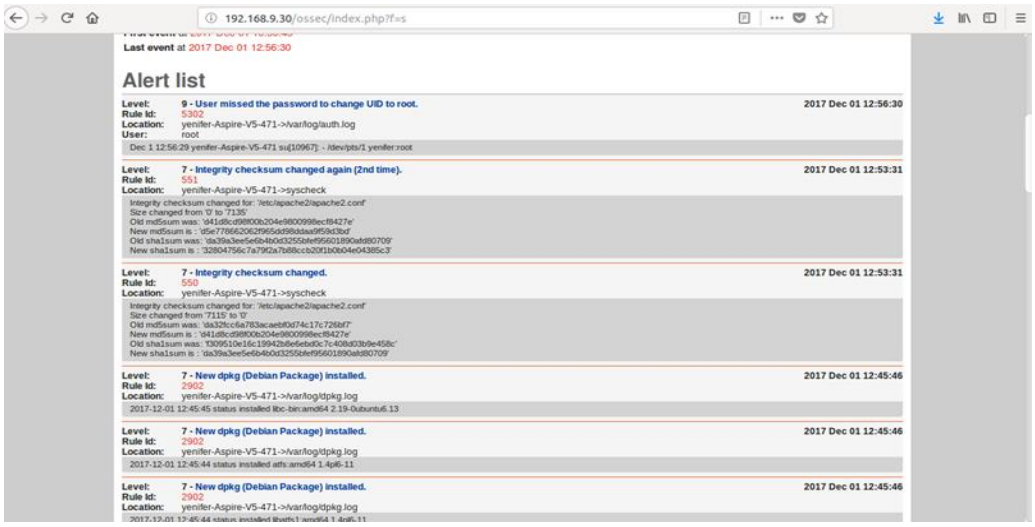
Ilustración 67



Estas son las estadísticas que genera Tripwire cuando se hace un cambio en los archivos.

Ahora, en las ilustraciones 68, se apreciara la lista de alerta que genera OSSEC cuando se ha realizado un cambio en un archivo.

Ilustración 68



Y por último en esta ilustración 69, ossec muestra una estadística de las alertas de las ultimas hora que se realizaron un cambio a un archivo,

para esta prueba se registra la a alerta de la hora 11 ya que, en ese rango de horas se estaba realizando las pruebas, con este producto.

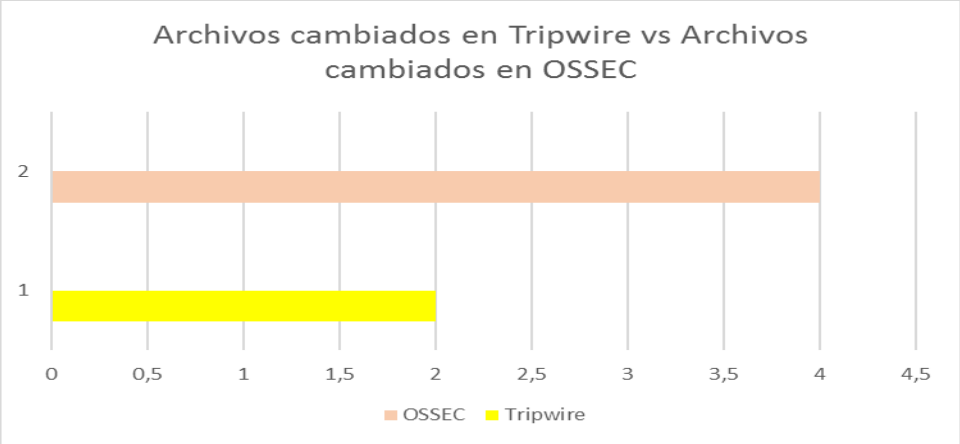
Ilustración 69

Total values per hour

Hour	Alerts	Alerts %	Syscheck	Syscheck %	Firewall	Firewall %	Total	Total %
Hour 0	504	24.8%	5,050	49.4%	0	0.0%	5,577	28.8%
Hour 10	593	29.2%	5,131	50.2%	0	0.0%	7,829	40.4%
Hour 11	244	12.0%	23	0.2%	0	0.0%	4,138	21.4%
Hour 12	529	26.0%	10	0.1%	0	0.0%	1,465	7.6%
Hour 13	164	8.1%	0	0.0%	0	0.0%	355	1.8%

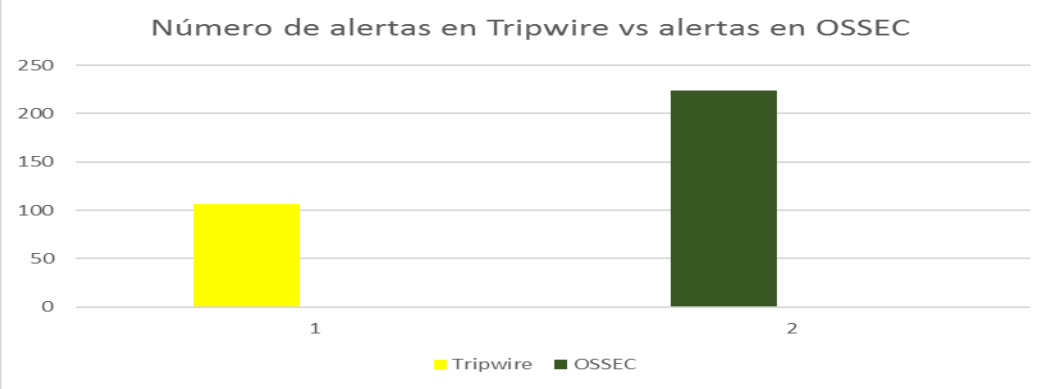
Ahora se realizará una comparación entre Tripwire con OSSEC respecto a los archivos cambiados.

Ilustración 70



Ahora, se apreciará una comparación entre Tripwire y OSSEC con respecto a las alarmas activadas.

Ilustración 71



Se puede notar que ossec genero más alertas que Tripwire, esto puede pasar por lo que decía anteriormente, que los IDS se les atribuye a los falsos positivos que se generan en la red (Ver capítulo 7.1.3.1).

Cabe resaltar que en caso que se quieran ver las alertas que estos productos genera se puede acceder al localhost, hay se podrá ver todos los registro y alertas que se guarda por defecto.

A continuación, se podrá analizar la ilustración 69, de la comparación que se hace entre Tripwire con OSSEC, basado en la estrategia de medición de los productos basados en HIDS, respecto a los archivos analizados ver ilustración 72, donde se apreciara el reporte que hace Tripwire, respecto a los archivos analizados,

Ilustración 72

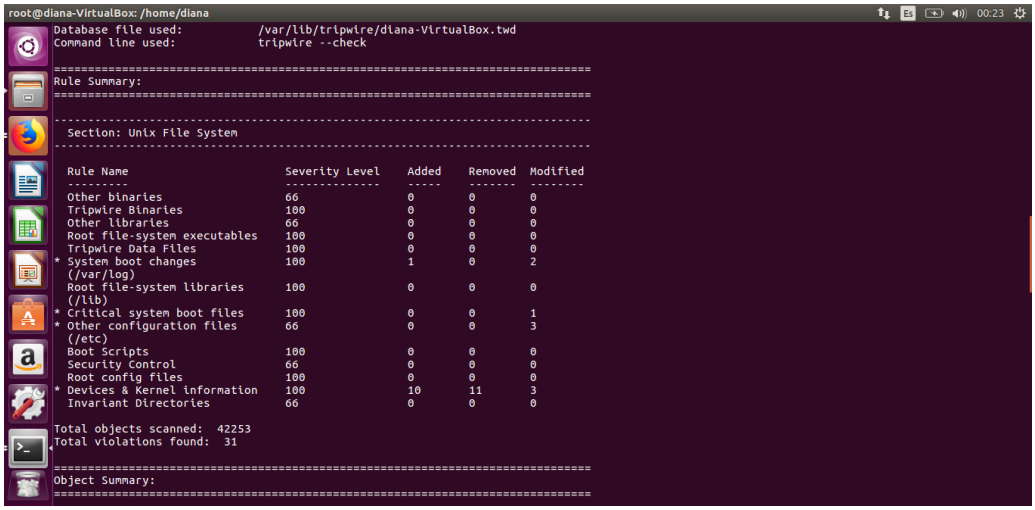
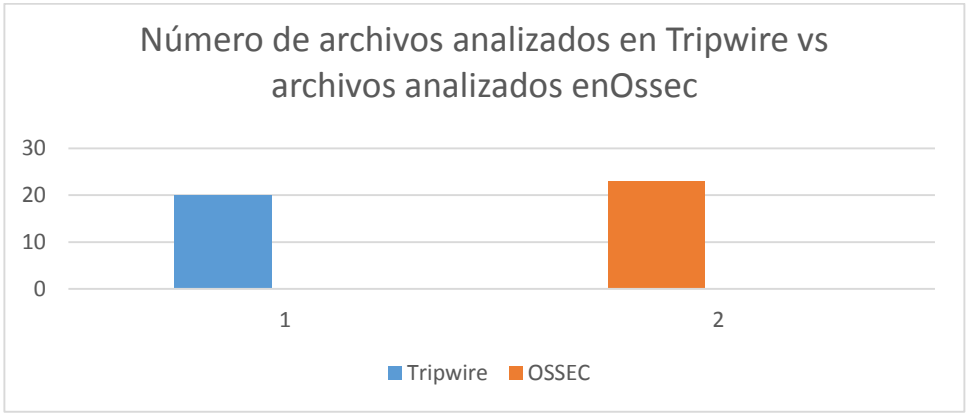
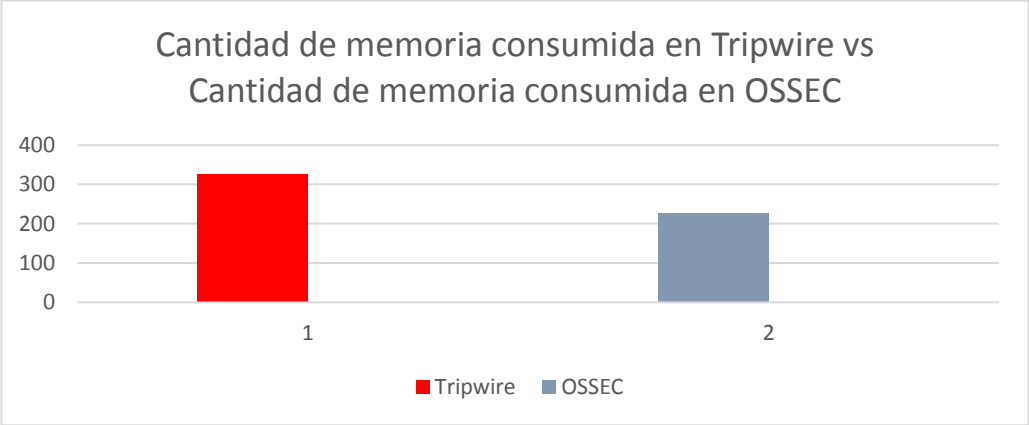


Ilustración 73



Ahora, se podrá ver la comparación entre la cantidad de memoria que consume OSSEC con Tripwire. Para analizar la cantidad de memoria que consumió ossec, al realizar la inspección de los archivos se utilizo Top esta herramienta ya se había utilizado en las pruebas que se realizaron anterior mente, y para ver cuanta memoria consumió Tripwire, ver ilustración 64.

Ilustración 74



Se puede notar que OSSEC le lleva una ventaja a Tripwire, ya que este analizo más cantidad de archivos para proteger la integridad de estos, y no consumió tanta memoria al realizar este tipo de análisis.

Metodología

Los pasos que se llevaron a cabo para realizar una metodología de evaluación de los IDS son:

- Identificar las posibles vulnerabilidades en la red.
- Documentar los ataques ARP Spoofing y DNS Spoofing.
- Diseñar una topología de red donde se puedan instalar IDS sin inconvenientes legales, (ver ilustración 46).
- El tipo de IDS que se necesita en la red, si se quiere que toda la red esté protegida se debe utilizar un NIDS.
- Si se quiere proteger cada host y tener un control más adecuado de la integridad de cada sistema, es recomendable utilizar un HIDS.
- Se implementaron dos productos basado en NIDS (Snort, Suricata). Si se desea proteger la red de ataques ARP Spoofing, es recomendable utilizar Snort, o al contrario si se quiere

proteger la red frente ataques DNS Spoofing se recomienda utilizar Suricata.

De estas herramientas (Snort, Suricata), se analizaron las siguientes características, ya que se consideraban importantes a la hora de detectar un ataque ARP Spoofing y DNS Spoofing:

- La cantidad de paquetes procesados.
- Los protocolos analizados.
- Si se tiene alguna IP sospechosa.
- Que puertos no se están utilizando y se deben deshabilitar.
- Flexibilidad a la hora de generar nuevas reglas.

Por otra parte, una de las ventajas de estas herramientas es que sean open source ya que la comunidad puede generar nuevas reglas y compartirla con otros usuarios.

Además, estos sistemas de detección proveen herramientas útiles para detectar comportamientos anormales considerados sospechosos por lo tanto es importante tener en cuenta la cantidad de alertas detectadas por cada IDS.

Por otra parte, se implementaron dos productos basado en HIDS (OSSEC, Tripwire). para proteger los hosts de la red uno con Tripwire y el otro OSSEC considerando como estado inicial del sistema al momento de su instalación y a partir de allí comparar el estado actual con el inicial para ver cambios importantes en los archivos considerados críticos. Hay que tener en cuenta que los dos productos basado en HIDS seleccionados para estas pruebas, no detectan ataques ARP Spoofing y DNS Spoofing, pero si pueden dar información importante para detectar que algo no van bien con el sistema.

15. CONCLUSION

Durante este proyecto se pudo hacer un análisis y saber más a fondo cómo funcionan los IDS, y así hacer una implementación de ellos, a su vez, se pudo instalar exitosamente un sistema de detección de intrusos en una sala de la Universidad Tecnológica de Pereira, aunque pesar de que los IDS basado en NIDS Suricata y Snort no detectaron los mismos tipos de ataques que se realizaron a ambos productos; ya que Snort no detecta ataques DNS Spoofing y Suricata no detecta ataques ARP Spoofing. Ya que no cuentan o poseen dentro de su arquitectura reglas para detectar estos ataques, más aun, Se pudo observar que Suricata es más potente en cuanto a velocidad de procesamiento en paquetes, número de alertas generadas y cantidad de memoria consumida comparado con Snort.

Respecto a los productos basados en HIDS, estos monitorean cada máquina realizando una copia de toda la base de datos actual del sistema. Cuando se hizo la práctica y se analizó los resultados que estos arrojaron durante las pruebas se pudo observar o interpretar que OSSEC es más potente en cuanto proteger la integridad de los archivos ya que realiza un monitoreo en tiempo real por el contrario Tripwire no es capaz de detectar una intrusión si el sistema ya ha sido atacado previo a su instalación.

La instalación de estos productos requiere un conocimiento previo de estas herramientas y del sistema operativo Linux lo que dificulto la realización de las pruebas y una amplificación en el tiempo de su realización.

A la hora de medir la efectividad de un IDS se debe tener en cuenta en donde la red es más vulnerable, a que ataques se está más expuesto y escoger el IDS con base en esto, ya que la arquitectura de cualquier IDS que tome decisiones en función de su base de firmas tiene unas reglas para cada tipo de ataques, y de antemano no se conoce a que se está expuesto y por lo general se utiliza cualquiera y no funciona, lo que se puede catalogar como malo cuando en realidad no estaba diseñado para ese tipo de ataques.

16. GLOSARIO

DNS: Es una tecnología basada en una base de datos que nos permite conocer la dirección IP de la maquina donde está alojado el dominio al que queremos acceder.

IDS: Es un sistema de detección de intrusos que supervisa la red en busca de actividad maliciosa y realiza una acción si detecta algo sospechoso por lo general bloquea los paquetes sospechosos de la ip de origen, no está diseñado para detener ataques.

I**PS**: Es un sistema de prevención de intrusos que se encarga de controlar la red pueden registrar y detener un ataque en el mismo momento que se está realizando antes de que tenga éxito.

HIDS: Es un tipo de IDS que protege a un solo computador y lo monitorea en busca de comportamiento sospechosos

NIDS: Es un tipo de IDS que monitorea toda la red analizando todo el tráfico que hay en la red en busca de comportamiento sospechoso.

ICMP: Es un protocolo que permite administrar información relacionada con los errores en el procesamiento de datagramas es decir de la IP.

TCP: Protocolo de la capa de transporte del modelo TCP/IP

UDP: User Datagram Protocol es un protocolo mínimo de nivel de transporte orientado a mensajes documentado en el RFC 768 de la IETF. En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación.

FIREWALL: Es un sistema que permite proteger a una o varias computadoras filtrando los paquetes que pueden entrar a nuestra red desde una red externa como internet.

T.I: Tecnologías de la información

RED: Conjunto de computadoras interconectadas que comparten información, recursos y servicios.

ARP: Es un protocolo de comunicaciones de la capa de enlace responsable de encontrar la dirección MAC de una determinada IP.

LAN: Local Area Network es una red que conecta los computadores en un área pequeña como un edificio

IP: Internet Protocol es un número único que identifica de manera lógica y jerárquica un dispositivo en una red

SSH: Secure SHell es un protocolo que facilita la comunicación segura entre dos sistemas permite a los usuarios conectarse a un host de manera remota encripta la conexión.

PUERTO: Interfaz a través de la cual se permite transmitir datos entre diferentes computadoras.

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red permite que varias redes u ordenadores se conecten entre sí.

HOST: Es un ordenador conectado a una red cada host consta de una dirección IP y un nombre de dominio único.

SNIFFER: Es un programa informático que permite capturar todos los paquetes que viajan por una red.

RED CONMUTADA: Es aquella en la cual la comunicación entre un host origen y host destino se realiza mediante nodos de comunicación intermedios.

VPN: Virtual Private Network es un túnel seguro que permite a una red privada extenderse a través de una red pública se usan para proteger el tráfico privado por internet.

GGI: Common Gateway Interface es una tecnología que permite a un cliente solicitar datos de un programa ejecutado en un servidor.

EXPLOIT: Es un programa que explota una vulnerabilidad del sistema para aprovechar esta deficiencia a beneficio de su creador.

SCTP: Stream Transmission Control Protocol es un protocolo de comunicación de la capa de transporte orientado a mensajes.

Ethernet: Es un estándar que define no sólo las características físicas del cableado para establecer la conectividad sino que también brinda los formatos de las tramas de datos del nivel de enlace de datos del modelo OSI.

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física

HTTP: Es un protocolo utilizado para solicitar y transmitir archivos a través de Internet u otra red informática, especialmente páginas web y componentes de páginas web, está orientado a transacciones y opera a través de un esquema petición-respuesta, entre un “cliente” y un “servidor”.

TLS: Transport Layer Security es un protocolo criptográfico que garantiza las comunicaciones en Internet proporciona cifrado de datos y autenticación de aplicaciones entre cliente/servidor.

SSL: Secure Sockets Layer Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet .

SMTP: Simple Mail Transfer Protocol es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, impresoras, etc).

SPAM: Mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

WORLD WIDE WEB: Es un sistema de distribución de documentos de hipertexto interconectados y accesibles vía internet

PCAP: Es una interfaz de una aplicación de programación para captura de paquetes. La implementación del pcap para sistemas basados en Unix se conoce como libpcap; el port para Windows del libpcap recibe el nombre de WinPcap syslog

FIM: Es un control para validar la integridad del sistema operativo y los archivos del software de la aplicación utilizando un método de verificación entre el estado actual del archivo y una línea de base conocida y buena . Este método de comparación a menudo implica el cálculo de una suma de comprobación criptográfica conocida de la línea

base original del archivo y la comparación con la suma de comprobación calculada del estado actual del archivo

ROOTKITS: Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

DKIM: DomainKeys Identified Mail es un mecanismo de autenticación de correo electrónico que permite a una organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado por un destinatario,comprobando de forma inequívoca que el origen del mismo es realmente el que aparece en las cabeceras del email.

MAC: Es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (4 bits)) que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo

DHCP: Dynamic Host Configuration Protocol es un protocolo de configuración dinámica del host, permite a un equipo unirse a una red basada en direcciones IP sin tener pre-configurado una dirección IP.

SWITCH: Es un dispositivo que sirve para conectar varios elementos dentro de una red.

PGP: Pretty Good Privacy programa desarrollado que sirve para cifrar contenido y acceder a él mediante una clave pública y firmar documentos digitalmente para autentificarlos

GNuPG: Es una herramienta de cifrado y firmas digitales desarrollado por Werner Koch, que viene a ser un reemplazo del PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL.

MITM: Man-In-The-Middle es un tipo de ataque informático en el que el atacante tiene conexiones independientes con las víctimas y transmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación es controlada por el atacante.

PAQUETE: Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas. está compuesto de tres elementos: una cabecera (header): que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor,el área de datos (payload): que contiene los datos que se desean trasladar,y la cola (trailer): que comúnmente incluye código de detección de errores.

SPOOFING: Uso de técnicas de suplantación de identidad generalmente para usos maliciosos. Se pueden clasificar sus ataques en función de la tecnología utilizada. Entre ellos el más extendido es el IP spoofing, aunque también existe el ARP spoofing, DNS spoofing, Web spoofing o email spoofing.

17 BIBLOGRAFIA

[1] Ashoor, Asmaa Shaker, y Prof. Sharad Gore. «Difference between Intrusion Detection System (IDS) & Intrusion Prevention System (IPS).» Pune University, India. Julio de 2011.

[2] Pablo Muñiz Botello Cholula, Puebla, México. «Modelado de un sistema de detección de intrusos.» Udlap. 13 de Mayo de 2010. http://catarina.udlap.mx/u_dl_a/tales/documentos/mcc/muniz_b_p/portada.html (último acceso: 8 de Noviembre de 2016).

[3] Scarfone, Karen. «The basics of network intrusion prevention systems.» Octubre de 2015.

[4] Victor Manuel Mendoza Anaya, Jose Alberto Chacon Prieto. Intrusiones Informaticas. 13 de mayo de 2017. https://intrusionesinformaticas.wikispaces.com/Clasificaci%C3%B3n+de+IDS (último acceso: 2 de junio de 2017).

[5] Alfonso, Jimenez. Maestros del web. 19 de Agosto de 2003. http://www.maestrosdelweb.com/snort/.

[6] Suricata. *Suricata IDS.* s.f. https://suricata-ids.org/.

[7] Alfonso, Jimenez. *Maestros del web.* Agosto 19, 2003. http://www.maestrosdelweb.com/snort/.

[8] Alonso. *El lado del mal.* febrero 16, 2016. http://www.elladodelmal.com/2016/02/hacer-e-mail-spoofing-con-smtp-sobre.html (accessed marzo 20, 2016).

[9] Ashoor, Asmaa Shaker, and Prof. Sharad Gore. n.d.

[10] Garcia, Carlos. *Hacking Etico.* agosto 26, 2010. https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/ (accessed marzo 20, 2016).

[11] Gumucio, Jose R. Torrico. *Cisco.* febrero 05, 2016. https://supportforums.cisco.com/t5/routing-y-switching-

blogs/configurando-dhcp-snooping/ba-p/3101169 (accessed noviembre 23, 2016).

[12] jonhatan. *SYSADMIN .* Octubre 21, 2010. https://jonhatan.wordpress.com/2010/10/21/implementacion-de-un-nids-con-easyids/.

[13] lsilva. *En linux.* mayo 20, 2012. https://www.enlinux.org/hacking-un-sitio-web-con-backtrack-5/ (accessed marzo 12, 2016).

[14] Sandra A. Moore, John Ha. *Red Hat Enterprise Linux 4.* USA, 2005.

[15] Soto, Marvin G. *Mediun.* junio 27, 2016. https://medium.com/@marvin.soto/qu%C3%A9-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-c%C3%B3mo-funciona-7f1e174850f2 (accessed marzo 23, 2016).

[16] TRT. *wonder how to.* diciembre 01, 2016. ttps://null-byte.wonderhowto.com/how-to/tutorial-dns-spoofing-0167796/ (accessed noviembre 29, 2107).

[17] Velasco, Rubén. *Redes sone.* noviembre 12, 2016. https://www.redeszone.net/2016/11/12/ataque-arp-poisoning-con-kali-linux/ (accessed novimebre 20, 2017).

[18] Velásquez, F. J. Díaz Jiménez y J.G. Palacio. *Disección de un ataque MITM mediante ARP Spoofing y Técnicas de Protección Existentes.* Barranquilla, Ed. Coruniamericana, Vol. I, 2012. 9-24.

[19] vieites, Alvaro Gomez. "Tipos de ataques e intrusos en las redes informaticas." n.d.

[20] Martin Roesch, Chris Green,Sourcefire, Inc, Cisco and/or its affiliates. All rights reserved. *manual snort.* 2017. http://manual-snort-org.s3-website-us-east-1.amazonaws.com/.