# CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

YUDY ADRIANA SALAZAR SANTANA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

# CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

YUDY ADRIANA SALAZAR SANTANA

Tutor

ALEXANDER LARRAHONDO NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2021

## TABLA DE CONTENIDO


INTRODUCCIÓN ..... 11
1. OBJETIVOS ..... 12
1.1. OBJETIVO GENERAL ..... 12
1.2. OBJETIVOS ESPECIFICOS ..... 12
2. PLANTEAMIENTO DEL PROBLEMA ..... 13
2.1. DEFINICIÓN DEL PROBLEMA ..... 13
2.2. JUSTIFICACIÓN ..... 14
3. METODOLOGIA ..... 15
4. MARCO TEORICO ..... 16
4.1. LEGISLACIÓN COLOMBIANA DE DELITOS INFORMÁTICOS PROTECCIÓN DE DATOS PERSONALES ..... 16
4.2. ETAPAS PENTESTING ..... 17
4.2.1. Planificación de Pruebas ..... 17
4.2.2. Realización de actividades para pruebas de Petesting ..... 19
4.2.3. Reconocimiento ..... 20
4.2.4. Escaneo de puertos, servicios y sistemas operativos ..... 20
4.2.5. Establecimiento y análisis de vulnerabilidades ..... 21
4.2.5.1. Análisis de aplicación ..... 21
4.2.5.2. Análisis de tráfico en las aplicaciones ..... 21
4.2.5.3. Plan de Explotación de vulnerabilidades ..... 21
4.2.6. Explotación de vulnerabilidades ..... 22
4.2.7. Informes ..... 22
4.2.8. Emisión, entrega y exposición de Informes ..... 22
4.3. DEFINICIÓN DE HERRAMIENTAS DE CIBERSEGURIDAD ..... 23
5. DESARROLLO DEL INFORME ..... 24
5.1. INSTALACIÓN DEL BANCO DE TRABAJO ..... 24
5.2. COMUNICACIÓN DE LAS MÁQUINAS WINDOWS CON KALI LINUX ..... 25
5.3. MONTAJE BANCO DE TRABAJO Y CARACTERISTICAS TÉCNICAS DE HARDWARE ..... 26
5.4. ANÁLISIS LEGAL Y ETICO DEL ANEXO 2 – ESCENARIO 2 Y ANEXO 3 ..... 30

5.5.ARTICULOS VULNERADOS DE LA LEY 1273 EN LOS ANEXOS .....32
5.6.ARGUMENTACIÓN DE LA APLICACIÓN AL TRABAJO EN THE WHITEHOUSE....33
5.7.PUNTO DE VISTA “OPERACIÓN ANDROMEDA BUGGLY”.....35
5.8.HERRAMIENTAS SOFTWARE UTILIZADAS PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3.....37
5.8.1. Reconocimiento.....38
5.8.2. Escaneo de puertos, servicios y sistemas operativos .....39
5.8.3. Establecimiento y análisis de vulnerabilidades.....41
5.8.4. Plan de Explotación de vulnerabilidades .....42
5.8.5. Explotación de vulnerabilidades .....42
5.9.DATOS ANEXO 4 ESCENARIO 3 QUE APOYARON EL DESCUBRIMIENTO DEL FALLO.....46
5.10.HERRAMIENTAS UTILIZADAS PARA IDENTIFICAR FALLOS EN EL EQUIPO DE WINDOWS 7 Y PUERTO ABIERTO POR APLICACIÓN.....47
5.11.COMO AFECTA EL ATAQUE A LA MÁQUINA WINDOWS 7 X 64 .....48
5.12.PASOS DE EJECUCIÓN PARA EXPLOTACIÓN DE VULNERABILIDAD.....49
5.12.1. Configuración de red .....49
5.12.2. Usando la herramienta metasploit.....50
5.13. ACTIVIDADES E INDAGACIONES A REALIZAR EN CASO DE ENFRENTARSE A UN ATAQUE EN TIEMPO REAL - ARGUMENTOS TÉCNICOS. .....58
5.14.DESDE EL EJERCICIO DE RED TEAM – MEDIDAS DE HARDENIZACIÓN PROPUESTAS PARA MITIGAR LA OCURRENCIA FUTURA DE ESTE ATAQUE. ..60
5.15. ..... DIFERENCIAS ENTRE EQUIPO BLUE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS .....61
5.16.FUNCIONES DEL CIS “CENTER FOR INTERNET SECURITY” DENTRO DEL EQUIPO DE BLUETEAM.....61
5.17.FUNCIONES Y CARACTERISTICAS PRINCIPALES DE UN SIEM .....62
5.18.HERRAMIENTAS DE CONTENCIÓN DE ATAQUES .....63
RECOMENDACIONES ..... 65
CONCLUSIONES..... 67
BIBLIOGRAFÍA ..... 68
ANEXO 1. LINK DEL VIDEO DE SUSTENTACIÓN DEL SEMINARIO ..... 71
ANEXO 2. EVIDENCIA DE TURNITIN 2%..... 71

## TABLA DE FIGURAS

Figura 1. Legislación Colombiana delitos informáticos y protección de datos personales...16
Figura 2. Etapas Pentesting ....17
Figura 3. Inventario de aplicativos web....17
Figura 4. Aplicativos cliente servidor ....18
Figura 5. Activos informáticos....18
Figura 6. Actividades de pruebas Pentesting ....19
Figura 7. Herramientas descargadas e instaladas....24
Figura 8. Se valida la IP configurada en el Kali 192.168.1.13 con el comando Ifconfig.....25
Figura 9. Desde la máquina Win 7-SE2020-X64 se realiza la validación de la IP propia 192.168.1.14 y se realiza el ping exitoso al Kali 192.168.1.13 ....25
Figura 10. Desde la máquina Win 7-SE2020 se realiza la validación de la IP propia 192.168.1.15 y se realiza el ping exitoso al Kali 192.168.1.13 ....26
Figura 11. Configuración equipo Win 7-SE2020-X64 ....27
Figura 12. Configuración equipo Win 7-SE2020....28
Figura 13. Configuración equipo Kali – Linux -2021-2 Virtualbox amd 64 ....29
Figura 14. Actividades de pruebas Pentesting ....37
Figura 15. Ciclo de vida de Windows 7....38
Figura 16. Vulnerabilidades Rejetto HTTP File....38
Figura 17. Escaneo de puertos máquina víctima herramienta nmap....39
Figura 18. Identificación del puerto 80, servicio, versiones ....40
Figura 19. Información del equipo a atacar ....40
Figura 20. Comando Services identifica el servicio del puerto 80 - Http File Server se encuentra activo ....40
Figura 21. Establecimiento de vulnerabilidades puerto 80 – Herramienta Legión ....41
Figura 22. Establecimiento de vulnerabilidades puerto 80 – Herramienta Legión ....41
Figura 23. Información exploitdb para vulnerabilidad identificada en fase anterior ....42
Figura 24. Metasploit herramienta elegida para explotar la vulnerabilidad de Rejetto....43
Figura 25. Búsqueda del módulo Metasploit Rejetto y validación de opciones ....43
Figura 26. Búsqueda del módulo Metasploit Rejetto y validación de opciones ....44
Figura 27. Inicialización y parametrización de variables para el ataque ....44
Figura 28. Variables cargadas en el módulo para efectuar el ataque....44
Figura 29. Explotación de la vulnerabilidad ....45
Figura 30. Creación de usuario desde meterpreter y comando Shell para abrir cmd del equipo atacado....45
Figura 31. Vulnerabilidades Rejetto HTTP File....46
Figura 32. Información Rejetto incibe - cert....47
Figura 33. Explicación del ataque de escalada de privilegios realizado ....49
Figura 34. Windows 7 X 64....49
Figura 35. Kali Linux....50
Figura 36. Nmap en metasploit db_nmap-v-A ip ....50
Figura 37. Identificación puertos abiertos nmap ....50
Figura 38. Identificación puertos 80, servicios y versiones....51

Figura 39. Identificación información PC atacado .....51
Figura 40. Comando services.....52
Figura 41. Consulta vulnerabilidades en Legion.....52
Figura 42. Información vulnerabilidad EDB-ID: 49584.....53
Figura 43. Indicación para explotar vulnerabilidad metasploit .....53
Figura 44. Módulo metasploit para el ataque.....54
Figura 45. Cargue opciones módulo exploit encotrado.....54
Figura 46. Inicialización de variables equipo a atacarFuente: El autor.....55
Figura 47. Inicialización variables equipo atacante.....55
Figura 48. Instrucción options.....55
Figura 49. Ejecución de la vulnerabilidad .....56
Figura 50. Meterpreter creación usuario administrador .....56
Figura 51. Meterpreter creación usuario administrador .....57
Figura 52. Usuario creado en equipo atacado.....57
Figura 53. Estrategia de contención de incidentes .....58
Figura 54. Estrategia de erradicación y recuperación.....59
Figura 55. Diferencias equipo blueteam y equipo de respuesta a incidentes .....61

## LISTA DE TABLAS

Tabla 1. Análisis legal y ético del anexo 2……..30

Tabla 2. Artículos vulnerados de la ley 1273 en los anexos……....32

## GLOSARIO

**BLUE TEAM:** Grupo de especialistas en aspectos de seguridad informática que se orientan de forma defensiva valorando las amenazas y riesgos a los cuales se puede ver enfrentados los sistemas o infraestructura tecnológica, realizando actividades de mitigación y contención de ataques informáticos.

**EXPLOIT:** Puede ser una serie de código o software diseñado para conseguir el control de equipos o apoderarse de datos de red por medio del aprovechamiento de vulnerabilidades o fallas de seguridad existentes en los sistemas.

**EXPLOITDB:** Permite realizar la consulta de la información del código de vulnerabilidad que arrojo Legion, se despliegan datos de la criticidad, explotabilidad, exploit, impacto, vectores de ataque, etc. Adicionalmente allí se ubicó la información de metasploit y el ID que define el comando a utilizar para realizar la explotación de dicha vulnerabilidad.

**HARDENING:** Expresión que se utiliza para describir las actividades de aseguramiento o fortalecimiento en los aspectos de seguridad de una plataforma tecnológica buscando disminuir las posibilidades de ataques informáticos.

**LEGION:** Esta herramienta permite realizar un análisis de las vulnerabilidades arrojando una serie de información como códigos de vulnerabilidad que permiten documentarse frente a la consistencia y explotabilidad de las mismas.

**METASPLOIT:** Esta herramienta está basada en código abierto y tiene posibilidades de: escanear e importar datos, realizar escaneos de descubrimiento, explotar datos, explotación manual, gestionar sesiones, integrar escaneo Nexpose, gestionar credenciales, pivote proxy, módulos post explotación, interfaz web, además es un marco de pruebas de intrusión muy utilizado a nivel mundial; el éxito está en la

colaboración conformada dentro de la comunidad que se encarga no solo de la verificación de vulnerabilidades, administración de validaciones en seguridad y avances en la concienciación respecto a seguridad, sino que también arma y prepara las defensas para siempre estar un paso más allá frente a las amenazas emergentes.

**NMAP:** Instrumento de código abierto con licencia GPL cuya función principal es apoyar la explotación de red y auditar la seguridad de las infraestructuras tecnológicas.

**PENTESTING:** Es una metodología por medio de la cual se ejecutan ataques controlados a sistemas informáticos con el fin de valorar la seguridad e identificar fallos, errores y debilidades a remediar.

**RED TEAM:** Grupo interdisciplinario de expertos en temas de seguridad informática que se orientan en la defensa de forma ofensiva por medio de la simulación de ataques a la infraestructura tecnológica que exploten vulnerabilidades en aplicaciones y sistemas de una compañía.

**VULNERABILIDAD INFORMÁTICA:** debilidad, deterioro o falla en la seguridad en plataformas de software o hardware que puede afectar e impactar la seguridad de la información y la infraestructura tecnológica de una organización.

## RESUMEN

El incremento de ataques informáticos a nivel mundial en los últimos años ha generado popularidad en los términos blueteam y redteam ya que estos equipos interdisciplinarios son reclutados con el ánimo de velar por la protección y seguridad en la infraestructura tecnológica de las organizaciones.

Este trabajo hace un recorrido por diferentes aspectos a tener en cuenta dentro de las capacidades y conocimientos de los especialistas que conforman estos grupos de profesionales; es así como se indica la normatividad Colombiana referente a protección de datos personales y delitos informáticos, se establecen las etapas de un Pentesting para posteriormente aplicarlas en un caso simulado con la ejecución de test a un banco de trabajo implementado dentro del informe, se realiza un acercamiento a las herramientas de ciberseguridad para aplicarlas en la ejecución de un ataque dentro de la infraestructura recreada, se efectúa la evaluación legal y ética de documentos relacionados con la contratación de los equipos, conceptos a tener en cuenta dentro de la información relacionada con los equipos redteam, blueteam, diferencias con los grupos de respuesta a incidentes, conceptos relacionados como SIEM, CIS controls, herramientas para contención de ataques y por último la formulación de recomendaciones y conclusiones del ejercicio realizado dentro del seminario con base a los conocimientos adquiridos.

Palabras clave: Blueteam, Redteam, hardening, Pentesting, Legislación, delitos informáticos, ataque, ciberseguridad, vulnerabilidades, herramientas de contención.

# INTRODUCCIÓN

El surgimiento de nuevas tecnologías, el auge de la computación en la nube, la disponibilidad de redes de alta velocidad, activos de información, datos de aplicaciones corporativas viajando a través de la red, son algunos de los aspectos que en un primer escenario brindan oportunidades de productividad y transformación para las organizaciones a nivel mundial; pero es inevitable un segundo escenario donde se proporciona una amplia oportunidad de ataques cibernéticos aún por desarrollar, conocer y explotar, que generan riesgos inminentes de seguridad, disponibilidad, autenticidad y privacidad de los datos confidenciales y críticos de las compañías.

Estas situaciones que exponen la infraestructura tecnológica a distintas amenazas tanto externas como internas, crean una amplia necesidad de implementación de equipos de seguridad Redteam y Blueteam que generen estrategias para salvaguardar la información con enfoques de revisión, protección, detección, respuesta, mitigación, seguimiento y aseguramiento, en un ciclo continuó que permita la integrabilidad y retroalimentación entre los dos equipos fortaleciendo barreras de seguridad que limiten las posibilidades de ataque y que aborden actividades que permitan contener y responder a posibles materializaciones.

Este informe se realiza en el marco del desarrollo del Seminario Especializado - Equipos Estratégicos en Ciberseguridad - Red Team & Blue Team, en el cual por medio del desarrollo de distintas actividades propuestas se pudieron abordar conocimientos frente a la normatividad, metodologías y herramientas de ciberseguridad que sirven como apoyo para el planteamiento de estrategias ofensivas y defensivas en los contextos de vulnerabilidades y amenazas, conceptos relacionados con el desarrollo de las funciones de estos equipos de defensa y buenas prácticas que aporten al aseguramiento y mitigación de impactos frente a posibles incidentes de seguridad que ocurran en las plataformas tecnológicas a cargo.

# 1. OBJETIVOS

## 1.1. OBJETIVO GENERAL

Elaborar un informe técnico que a partir del análisis ético, legal, creación de un banco de trabajo para la demostración de posibles vulnerabilidades y profundización de conceptos relacionados; permita el establecimiento de estrategias viables para la contención, formulación de recomendaciones y conclusiones que puedan apoyar el desarrollo de las actividades de los equipos Red Team & Blue Team.

## 1.2. OBJETIVOS ESPECIFICOS

- Conocer las actividades de los equipos Red Team & Blue Team en las compañías partiendo de los fundamentos éticos y legales de la normatividad Colombiana.

- Evidenciar las debilidades de una plataforma tecnológica utilizando mecanismos y técnicas de intrusión.

- Proponer estrategias para contener ataques a partir de análisis de riesgos y debilidades de la infraestructura tecnológica de TI.

- Formular recomendaciones que puedan apoyar y fortalecer la función y actividad de endurecimiento y fortalecimiento de las infraestructuras tecnológicas a partir del desarrollo de proyectos blueteam y redteam.

# 2. PLANTEAMIENTO DEL PROBLEMA

## 2.1. DEFINICIÓN DEL PROBLEMA

El estudio de las diferentes ramas relacionadas con la seguridad informática proporciona un amplio horizonte del estado de indefensión en el que se pueden encontrar las organizaciones que carecen de estrategias, conocimiento y equipos interdisciplinarios que aborden actividades de aseguramiento y problemáticas de seguridad a las que se pueda enfrentar la organización.

Con todo esto surgen algunas inquietudes: ¿Están los profesionales de la información y seguridad informática contextualizados con los términos de blueteam y redteam? , ¿Que conocimientos tienen las personas que estudian el área de seguridad informática sobre las funciones y responsabilidades de los equipos blueteam y redteam?, en la experiencia personal, cuando empecé a realizar este seminario de profundización no tenía ni idea del significado de estos términos y por lo tanto tampoco tenía información respecto al perfil profesional y requerimientos necesarios para poder aplicar a una vacante que se relacione con las capacidades y gestión de estos equipos de defensa.

Algunos profesionales con conocimientos en áreas de seguridad informática y de la información, ignoran la existencia de herramientas de ciberseguridad que pueden apoyar el desarrollo de las habilidades necesarias para aportar en la construcción dentro de los equipos de defensa y fortalecimiento de nociones que contribuyan a la labor profesional y a sembrar la inquietud de alcanzar dichas competencias para aplicar a la conformación de uno de estos equipos tan importantes hoy en día para las organizaciones.

## 2.2. JUSTIFICACIÓN

Con la evolución de las tecnologías y el crecimiento constante de niveles de ataques cibernéticos y amenazas emergentes debido a la continua investigación por parte de cibertatacantes que cada vez son más especializados y sofisticados; se acrecienta la necesidad de conocimiento frente al tratamiento de amenazas y vulnerabilidades por parte de los equipos interdisciplinarios que con su actividad pueden apalancar la toma de decisiones de distintas índoles desde la seguridad organizacional hasta la identificación, divulgación y tratamiento de amenazas con los tratados y comunidades que aportan a la ciberseguridad a nivel mundial.

Este trabajo está dirigido a estudiantes y profesionales de áreas de seguridad informática y de la información que desconocen la existencia de herramientas de ciberseguridad y la conformación de grupos de trabajo blueteam y redteam; sus habilidades, funciones, procesos, tecnologías, perfiles profesionales y marco legal entre otros temas de interés y que pueden ser útiles al momento del desarrollo de las actividades estudiantiles, laborales o que pueden aportar conocimientos enfocados desde su labor a distintos caminos no explorados hasta ahora.

El objetivo del informe es comprender las capacidades, funciones, conocimientos y herramientas de los equipos blueteam y redteam para el desarrollo e implementación de estrategias encaminadas al aseguramiento y defensa de la infraestructura tecnológica de las organizaciones partiendo de la ética, legislación y buenas prácticas.

# 3. METODOLOGIA

Este informe se desarrollo por medio de la ejecución de cinco fases en las cuales se distribuyeron las actividades de la siguiente manera:

Etapa 1: Comprendió el conocimiento de la normatividad colombiana frente a delitos informáticos, protección de datos personales; se estudiaron las etapas de Pentesting y definiciones de herramientas de ciberseguridad y por último se configuro un banco de trabajo para las prácticas de las etapas posteriores.

Etapa 2: Se realizó el análisis legal y ético del escenario que comprendía un contrato empresarial para el reclutamiento de los integrantes de equipos redteam y blueteam en una compañía, verificando los artículos vulnerados frente a la ley 1273 de 2009; se expusieron las posiciones frente a la aplicación al cargo que ofrece la empresa y la opinión frente a un caso real denominado “Operación Andrómeda buggly”.

Etapa 3: Frente al escenario de un ataque ocurrido en la compañía se procedió a exponer las herramientas con las cuales se pudo identificar y recopilar la información del ataque enfocados en las etapas de Pentesting estudiadas en la fase 1, se analizó la información que aporto para los descubrimientos del fallo, los impactos de este fallo en la máquina afectada y la explotación de la vulnerabilidad explicada en cada uno de los pasos que se requirieron.

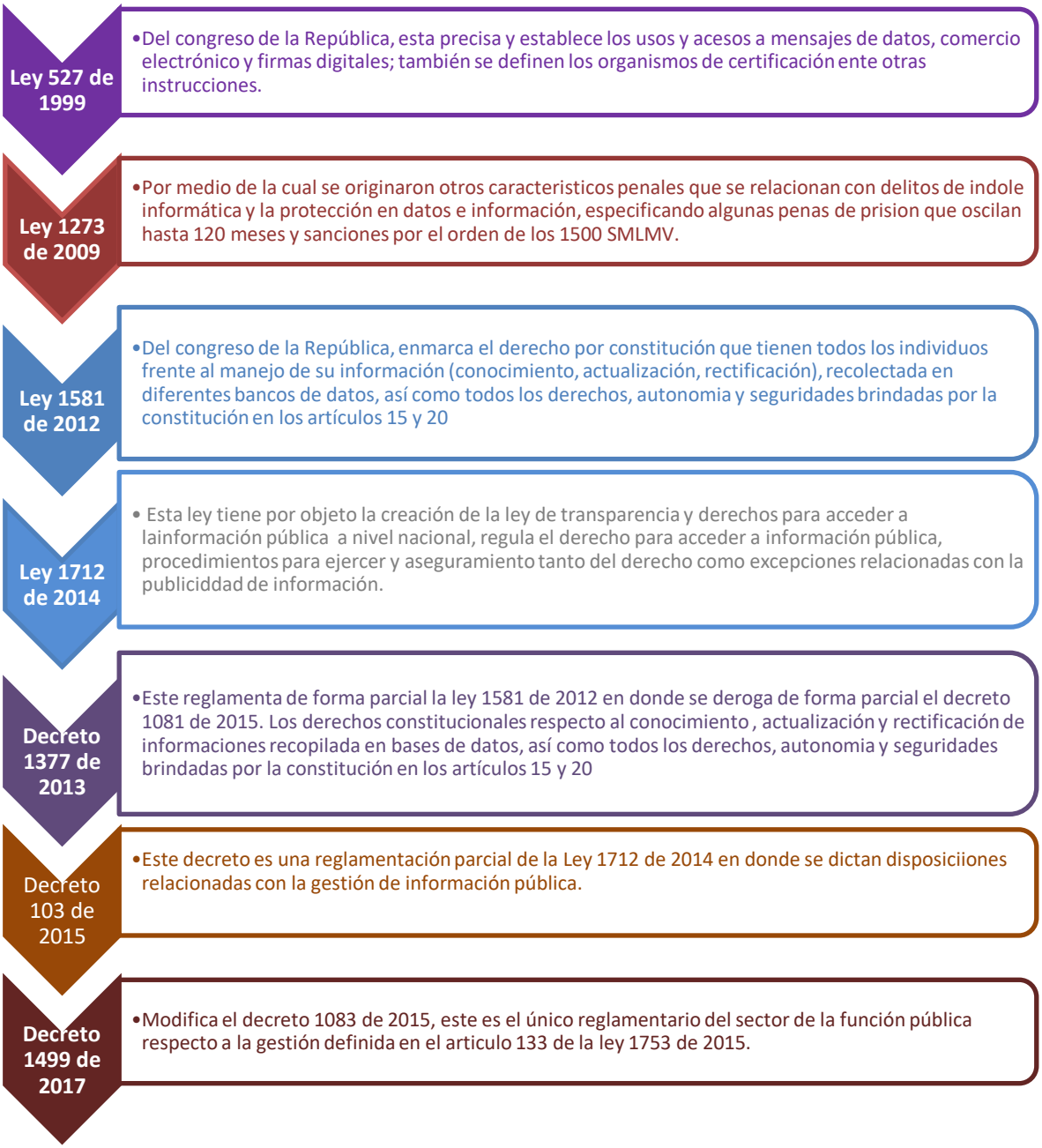
Etapa 4: Se presentaron las indagaciones a realizar en caso de ataques en tiempo real, basados en argumentos técnicos, desde el equipo de redteam se presentaron las medidas de hardenización para mitigar ataques futuros, se establecieron diferencias entre el equipo blueteam y de respuesta a incidentes, la utilización de CIS en el equipo de blueteam y se hizo una profundización frente a términos como SIEM y herramientas de contención de ataques.

Etapa 5: Compilación de las actividades desarrolladas en las anteriores fases en el informe que incluye la formulación de recomendaciones que permitan el establecimiento de estrategias para fortalecer aspectos de seguridad en las organizaciones y conclusiones frente a los conocimientos adquiridos desde la perspectiva de la ciberseguridad.

# 4. MARCO TEORICO

## 4.1. LEGISLACIÓN COLOMBIANA DE DELITOS INFORMÁTICOS PROTECCIÓN DE DATOS PERSONALES

Figura 1. Legislación Colombiana delitos informáticos y protección de datos personales




Fuente: Construcción propia autor

## 4.2. ETAPAS PENTESTING

Para la implementación de metodologías de Pentesting se tendrá en cuenta la referencia de ADALID Corp.[1] que plantea tres etapas principales en las cuales se divide el proceso de ejecución de las pruebas:

Figura 2. Etapas Pentesting


Fuente: Construcción propia autor

### 4.2.1. Planificación de Pruebas

Este procedimiento se realiza con el apoyo de la entidad dueña de la infraestructura a validar, el proveedor o experto asesor que realiza las pruebas se encarga de entregar los requisitos necesarios a la compañía o en su defecto al interventor encargado del proceso. Esta planificación esta a su vez compuesta por las siguientes sub- etapas:

Figura 3. Inventario de aplicativos web


Fuente: http://www.pctltda.com/web/

1. **Inventario de aplicativos Web:** Es necesario que la entidad realice un inventario de aplicativos web que funcionen en la compañía, esta información es un input importante para la realización de las pruebas y debe contener como mínimo lo siguiente:
   - Direcciones IP asignadas y nombres tanto interno como externo de publicación.
   - Lenguajes de programación y bases de datos si aplican.
   - Año de inicio de funcionamiento.
   - Tipos y Procesos que soportan (apoyo, misional).

1 ALCALDÍA DE BOGOTÁ. Guardianes de la información Penetration Testing. [Sitio web]. [Consulta: 25 de agosto de 2021]. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

Figura 4. Aplicativos cliente servidor


Fuente: https://sites.google.com/site/lawedysus fundamentoscompleto/home/cliente---servidor

**2. Aplicativos cliente\servidor:** Como insumo para la realización de las pruebas, la entidad debe entregar este inventario con al menos la siguiente información:

- Direcciones IP asignadas y nombres tanto interno como externo de publicación para los servidores.
- Lenguajes de programación tanto para clientes como servidores y bases de datos si aplican.
- Año de inicio de funcionamiento.
- Tipos y Procesos que soportan (apoyo, misional).

**3. Especificar los activos informáticos para las pruebas:** se gestiona una reunión inicial con la compañía en donde se llevan a cabo las siguientes tareas:

- Resolución de dudas frente a los activos elegidos para la realización de pruebas.
- Evitar aplicativos en los cuales no se pueda gestionar una ventana de tiempo para realización de las pruebas.
- La compañía debe priorizar un orden para las aplicaciones elegidas.
- Establecer posibles riesgos de corrupción, pérdidas de información o disponibilidad en el desarrollo de las pruebas, mitigaciones para estos eventos y planes de continuidad.
- Elegir diferentes tipos de aplicaciones en cuanto a variedad de desarrollos, lenguajes de programación, middleware.
- Definir el cronograma y duración para ejecución de las pruebas.

Figura 5. *Activos informáticos*


Fuente: https://www.dtsecurity.net/enterprise-communications.html

**4. Definición de herramientas a utilizar para las pruebas:** Con la información entregada por la compañía frente a los aplicativos a probar y la aplicación de la cartilla Ámbito 1 “Reconocimiento de área” se identifican las herramientas a utilizar en cada uno de ellos.

**5. Elaboración de propuesta para las pruebas:** Esta propuesta es un informe gerencial en el que se indican los aplicativos que se escogieron para la realización de las pruebas, el cronograma que se llevara a cabo para la realización de las pruebas con la respectiva duración, indicar posibles riesgos de corrupción, pérdidas de información o disponibilidad en el desarrollo de las pruebas, mitigaciones para estos eventos y planes de continuidad. Esta propuesta se presenta a la alta dirección de la compañía quien deberá realizar la aprobación por escrito para dar inicio al proyecto de ejecución de pruebas.

**6. Definición del cronograma:** Este documento técnico contiene:

- El personal involucrado en el acompañamiento en el desarrollo de pruebas.
- El apoyo, permisos, actividades preliminares y después de la ejecución.
- Activos de información seleccionados para las pruebas.
- Información de los costos relacionados con la realización de las pruebas.
- Herramientas que se utilizaran para cada uno de los test.
- Resultado que se espera en los aplicativos frente a la realización de las pruebas.
- Hora y fecha de realización, tiempos de ejecución de pruebas y de indisponibilidad de servicios.

Este documento será entregado a la alta gerencia de la compañía que estará encargada de definir y coordinar la realización de las mismas.

### 4.2.2. Realización de actividades para pruebas de Pentesting

Para la realización de las pruebas se tendrán en cuenta algunas metodologías de referencia como Ec-Council, OSSTM y pruebas de efectividad; las etapas propuestas por ADALID Corp.[2] son las siguientes:

*Figura 6.* Actividades de pruebas Pentesting


Fuente: ALCALDÍA DE BOGOTÁ. Guardianes de la información Penetration Testing. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

[2] Ibíd., p.19

### 4.2.3. Reconocimiento

Para esta etapa se procede a realizar investigaciones en la página web de la compañía, revisando información de utilidad como teléfonos, direcciones de email, proveedores, empresas relacionadas, funcionarios, redes sociales, noticias relacionadas con posible información filtrada sin intensión que posiblemente conocen los empleados pero no es de índole pública.

Validación de mensajes e **información publicada en internet** referenciando a la compañía y que esté relacionada con infraestructura tecnológica utilizada.

Búsqueda de información en **sitios whois** que permitan identificar **datos de contacto y DNS**, en Sur América se puede utilizar **LACNIC** que se encarga de asignación de recursos para numeración en Internet.

Por medio de diferentes buscadores (**Shodan, Bing, Yahoo, etc**.)Y utilización de **Google hacking** se puede tener acceso a información de la entidad y de igual manera se debe validar información de archivos, metadatos y redes sociales (**Facebook, twitter**), entre otros.

### 4.2.4. Escaneo de puertos, servicios y sistemas operativos

Para esta actividad es necesaria la reducción de rangos de IPS a un listado de equipos activos. Para ello es necesario realizar un barrido de ping o escaneo de ICMP para localizar los equipos activos en red limitando los test a host encontrados. Esta etapa se puede realizar con ayuda de **Nmap** utilizando el comando **“-sn”: nmap –sn <Ip a validar>**, esto listara los host que responden al descubrimiento. Para escanear los puertos activos se pueden utilizar esta herramienta también por medio de un escaneo SYN o TCP. También se realiza un banner grabbing que permite establecer información de sistemas operativos que puede dar información sobre la red y equipos, también se puede conseguir información por medio de la huella de la pila TCP/IP que facilita dirigir la configuración de herramientas para análisis de vulnerabilidades.

### 4.2.5. Establecimiento y análisis de vulnerabilidades

Con la plena identificación de sistemas operativos en los equipos, estos resultados sirven para establecer la ruta del análisis de vulnerabilidades. El administrador de contenidos y los pluggins se pudieron haber establecido con el análisis de banners, esto puede dejar al descubierto información de vulnerabilidades existentes que si no han sido remediadas puede ser un riesgo alto para la infraestructura.
Para realizar el escaneo de vulnerabilidades dentro de los dispositivos identificados se pueden utilizar herramientas como **Nessus, OpenVas, Nikto,** entre otras.

#### 4.2.5.1. Análisis de aplicación

Para realizar pruebas de seguridad en las aplicaciones web, puede utilizarse **OWASP ZAP** que se basa en java y a través de una interface gráfica pone a disposición del usuario diferentes funciones para la ejecución de ataques a las aplicaciones con una serie de complementos todo en uno.

#### 4.2.5.2. Análisis de tráfico en las aplicaciones

Esta validación permite establecer como viaja la información de la aplicación, si viajan en claro o cifrados; si la respuesta es la primera puede estar la información de los usuarios comprometida. Para efectuar esta tarea se puede realizar con **Wireshark**, activando la escucha de la interface que pueda acceder al tráfico de la aplicación; con esto la herramienta empieza a realizar capturas de todos los paquetes que viajan por la red y permite realizar los análisis correspondientes.

#### 4.2.5.3. Plan de Explotación de vulnerabilidades

Con el resultado de las vulnerabilidades que se identificaron se debe establecer la clasificación de acuerdo a la criticidad, tipo y la existencia de exploit de acuerdo a la validación en páginas comohttps://www.rapid7.com/db y https://www.exploit-db.com/search/. Las vulnerabilidades que presenten exploit disponible se clasificaran en

cuatro grupos: las que se puedan gestionar remotamente con exploits remotos, los que necesitan acceso local a la máquina, los que explotan debilidades de los aplicativos web y por último las que pueden generar indisponibilidad de servicio. El plan de explotación tendrá como prioridades las vulnerabilidades que involucren un exploit remoto que permita un acceso privilegiado al equipo o uno que permita acceder y ejecutar un exploit local relacionado con vulnerabilidades identificadas en los sistemas; posteriormente se listan las debilidades a explotar en el orden prioritario que se les dio.

### 4.2.6. Explotación de vulnerabilidades

Empieza con la elección de las herramientas y exploits para explotar las debilidades priorizadas; para la realización de estas actividades se elige el Metasploit y exploits a aplicar en base a las vulnerabilidades encontradas y que se plantearon en el plan de explotación. Se configura cada una de las elecciones para atacar que tiene el Metasploit con base a las vulnerabilidades y las versiones tanto de la aplicación como de servicios y sistemas operativos. El exploit es lanzado después de la configuración en el Metasploit al servidor objetivo, se recogen evidencias del resultado del ataque y la información del Metasploit o las capturas que se evidencian en la explotación.

### 4.2.7. Informes

Con base a las evidencias recolectadas en el desarrollo de las pruebas se realiza un informe especificando los resultados que se obtuvieron.

### 4.2.8. Emisión, entrega y exposición de Informes

Esta etapa busca la realización de una presentación técnica y gerencial que muestre los resultados conseguidos en las pruebas de Pentesting que se ejecutaron en los diferentes equipos y entidades seleccionadas y priorizadas.
Se expone un informe elaborado de acuerdo al contexto propuesto por la alta gerencia de la entidad.

## 4.3. DEFINICIÓN DE HERRAMIENTAS DE CIBERSEGURIDAD

Las herramientas que permiten la realización de pruebas de penetración testing son fundamentales para gestionar la seguridad en las organizaciones; permiten abordar problemas algunas veces desconocidos de manera proactiva y oportuna. A continuación se enumeran y explican algunas de ellas:

- **Metasploit:** Esta herramienta es un marco de pruebas de intrusión muy utilizado a nivel mundial; el éxito está en la colaboración conformada dentro de la comunidad que se encarga no solo de la verificación de vulnerabilidades, administración de validaciones en seguridad y avances en la concienciación respecto a seguridad, sino que también arma y prepara las defensas para siempre estar un paso más allá frente a las amenazas emergentes. Esta herramienta está basada en código abierto y tiene posibilidades de: escanear e importar datos, realizar escaneos de descubrimiento, explotar datos, explotación manual, gestionar sesiones, integrar escaneo Nexpose, gestionar credenciales, pivote proxy, módulos post explotación, interfaz web.
- **Nmap:** Su función principal es apoyar la explotación de red y auditar la seguridad de las infraestructuras tecnológicas. Con los comandos disponibles se pueden hacer descubrimiento de servidores, encontrar puertos abiertos en los servidores de destino, puede validar los servicios que se están realizando en el host, puede descubrir sistemas operativos, versiones utilizadas en los servidores y se pueden identificar algunas características de hardware del equipo incluido en la prueba.
- **OpenVas:** Esta herramienta es un marco de integración de servicios y herramientas de scanner que permiten gestionar identificar y gestionar vulnerabilidades de seguridad. Dentro de sus principales características se pueden escanear diferentes host de manera simultánea, tiene soporte SSL para OPT, opcionalmente se puede habilitar el soporte WMI, existe la posibilidad de gestionar notas en el resultado de escaneo, gestionar falsos positivos, programar los escaneos y gestionar usuarios.
- **Servicio en línea ExploitDB:** Este recurso consiste en un almacén de datos de exploits y pruebas de conceptos que la hace más útil para usuarios que requieren información procesable de forma rápida. Contiene una base de datos de piratería de

Google con contenido clasificado en consultas de motores de búsqueda que se ha dispuesto para el descubrimiento de información en algunas ocasiones confidencial puesta al público en internet. La opción Exploit Database en GitHub incluye searchsploit que posibilita tener una copia de Exploit Database disponible en cualquier lugar ya que permite realizar las búsquedas en detalle por medio de la copia del repositorio local que se extrajo.

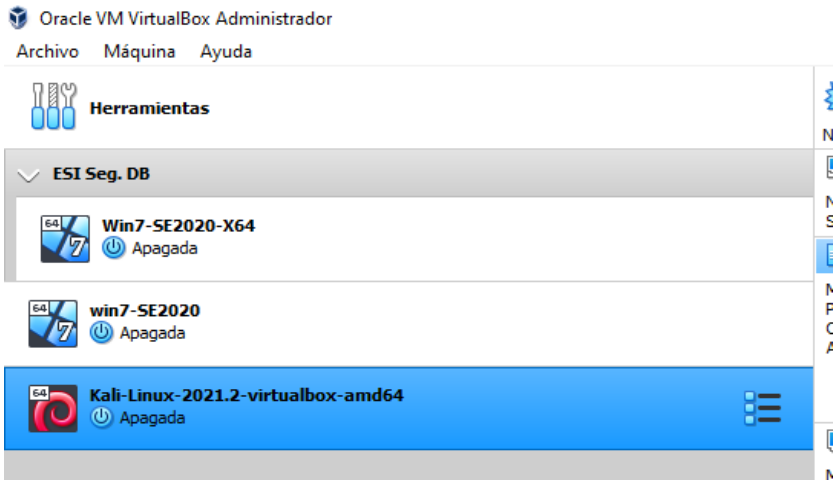
- **Servicio en línea CVE:** Es un proyecto que tiene como misión la identificación, definición y catalogación de vulnerabilidades de ciberseguridad que son de divulgación pública. Se genera un registro CVE para cada debilidad en el catalogo. Los asociados realizan la publicación de registros CVE con el ánimo de comunicar las descripciones de las vulnerabilidades encontradas y los profesionales de tecnología de información y ciberseguridad hacen uso de este catalogo para asegurar el tratamiento de los mismos inconvenientes coordinando los esfuerzos para el abordaje y priorización de vulnerabilidades.

# 5. DESARROLLO DEL INFORME

## 5.1. INSTALACIÓN DEL BANCO DE TRABAJO

Descarga herramienta virtual box y descarga imágenes .ova windows 7 x86, un windows 7 x64, un kali linux.

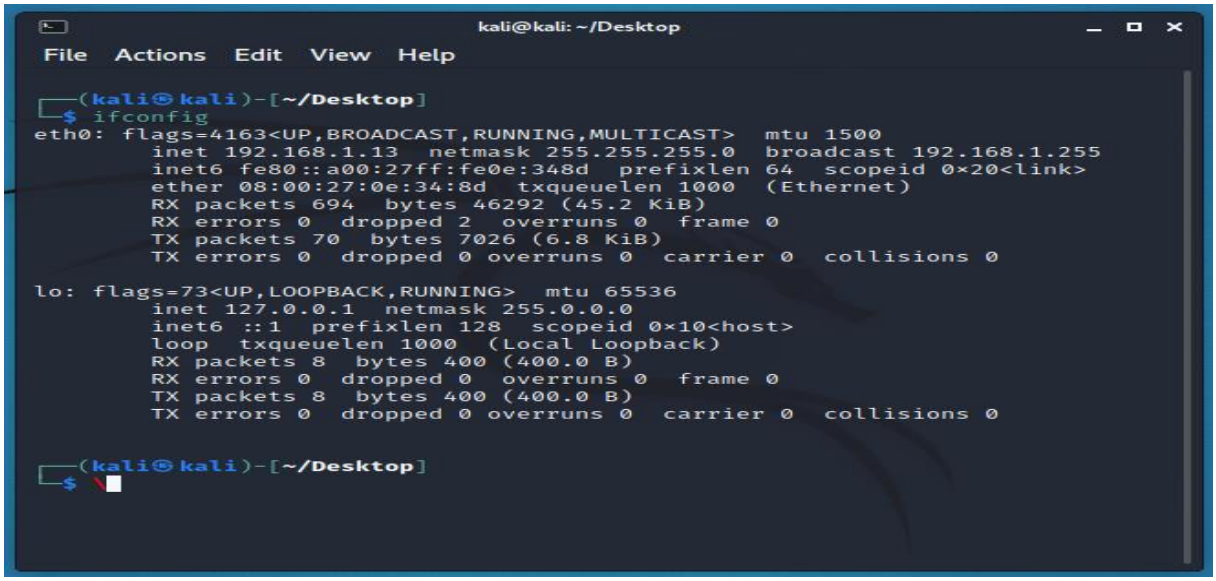
*Figura 7.* Herramientas descargadas e instaladas




Fuente: El autor

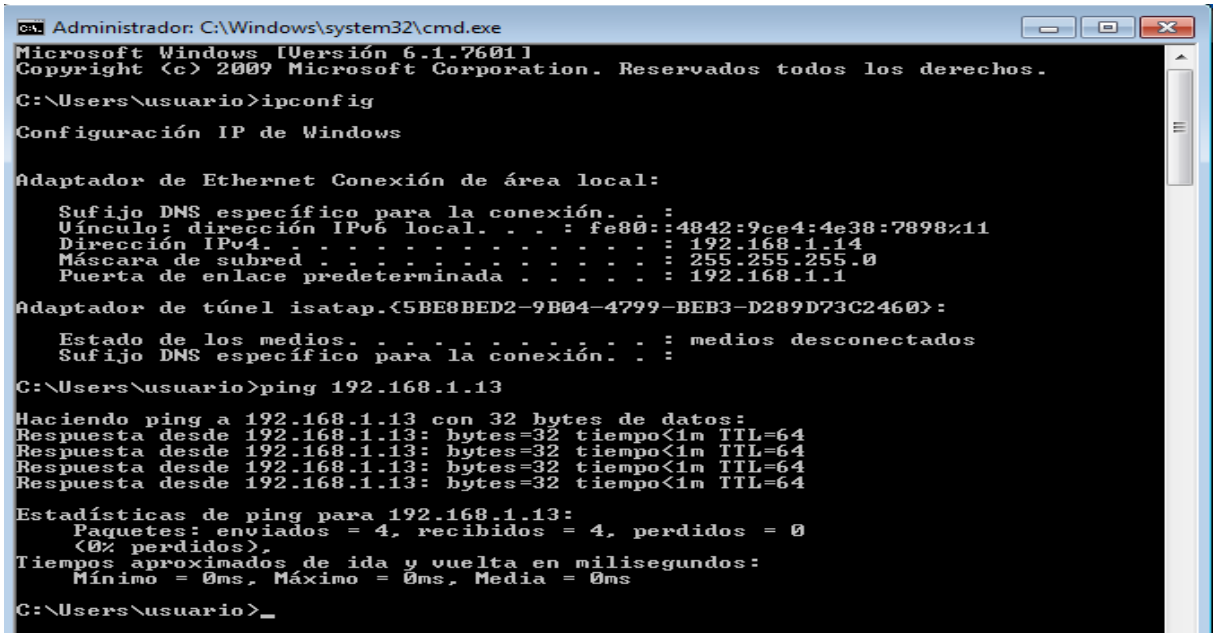
## 5.2. COMUNICACIÓN DE LAS MÁQUINAS WINDOWS CON KALI LINUX

*Figura 8.* Se valida la IP configurada en el Kali 192.168.1.13 con el comando Ifconfig.



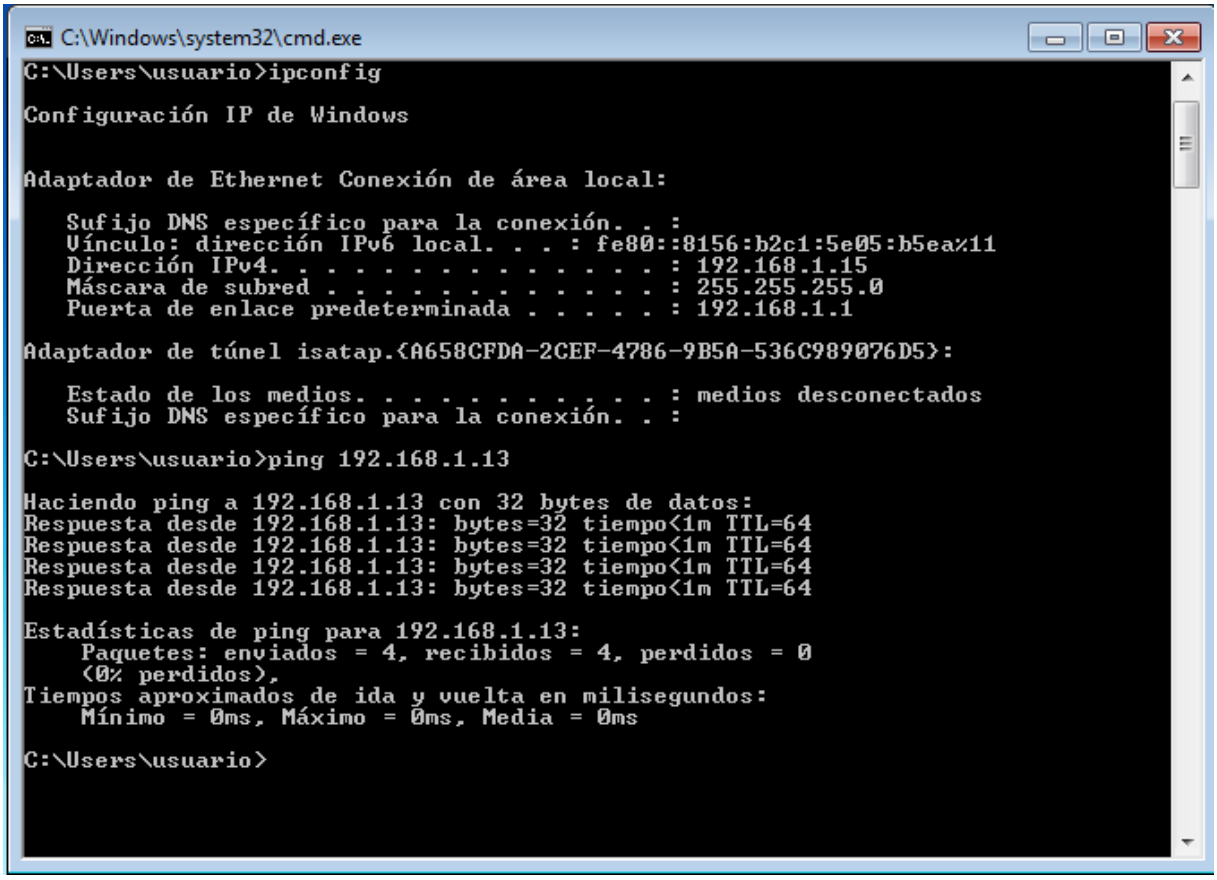

Fuente: El autor

*Figura 9.* Desde la máquina Win 7-SE2020-X64 se realiza la validación de la IP propia 192.168.1.14 y se realiza el ping exitoso al Kali 192.168.1.13




Fuente: El autor

*Figura 10.* Desde la máquina Win 7-SE2020 se realiza la validación de la IP propia 192.168.1.15 y se realiza el ping exitoso al Kali 192.168.1.13




Fuente: El autor

## 5.3. MONTAJE BANCO DE TRABAJO Y CARACTERISTICAS TÉCNICAS DE HARDWARE

El banco de datos se encuentra desplegado con una máquina virtual VirtualBox que enlaza tres equipos con las siguientes características:

**Win 7-SE2020-X64:**

**Sistema operativo:** Windows 7 (64 bit)

**Memoria base:** 4096 MB

**Orden de arranque:** Óptica, disco duro

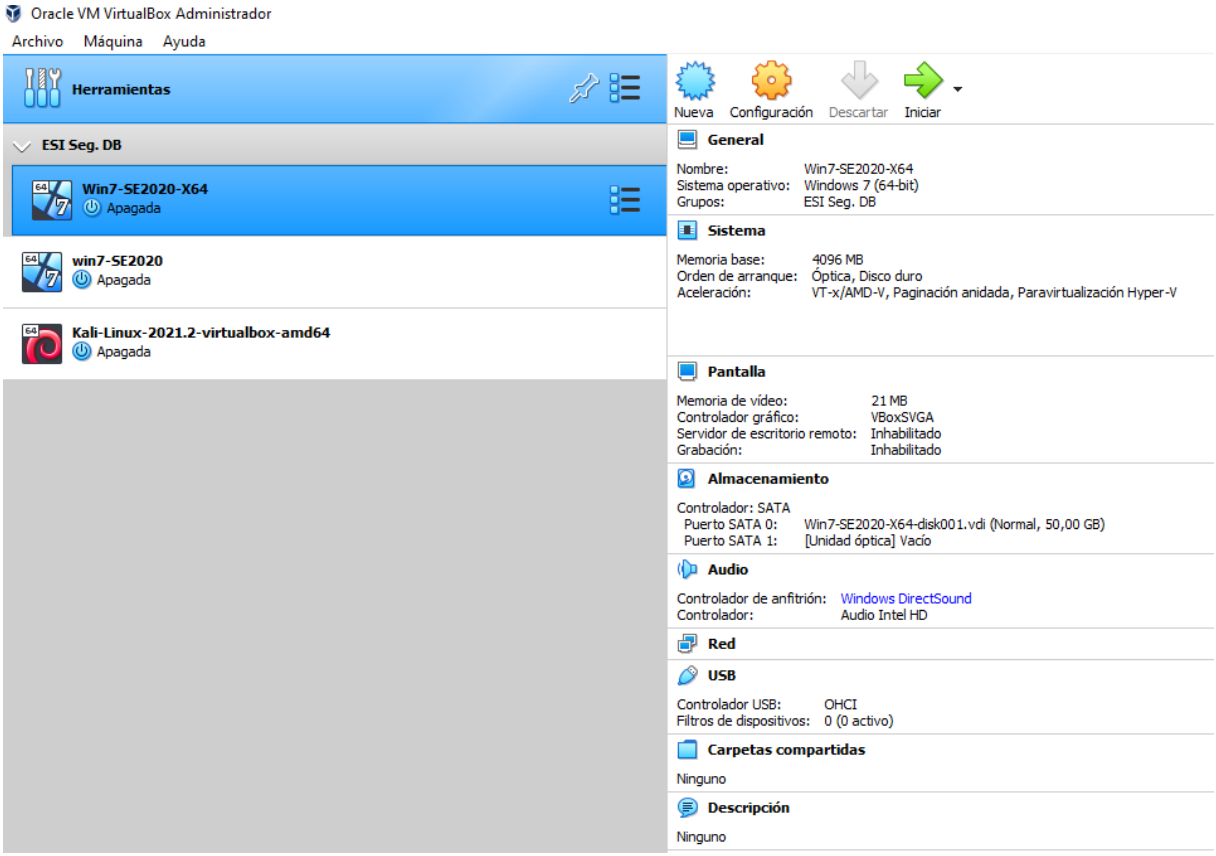
**Memoria video:** 21 MB

**Controlador Gráfico:** VBoxSVGA

**Controlador:** SATA

**Controlador USB:** OHCI

*Figura 11.* Configuración equipo Win 7-SE2020-X64




Fuente: El autor

**Win 7-SE2020:**

**Sistema operativo:** Windows 7 (64 bit)

**Memoria base:** 4096 MB

**Procesadores:** 4

**Orden de arranque:** Disquete, Óptica, disco duro

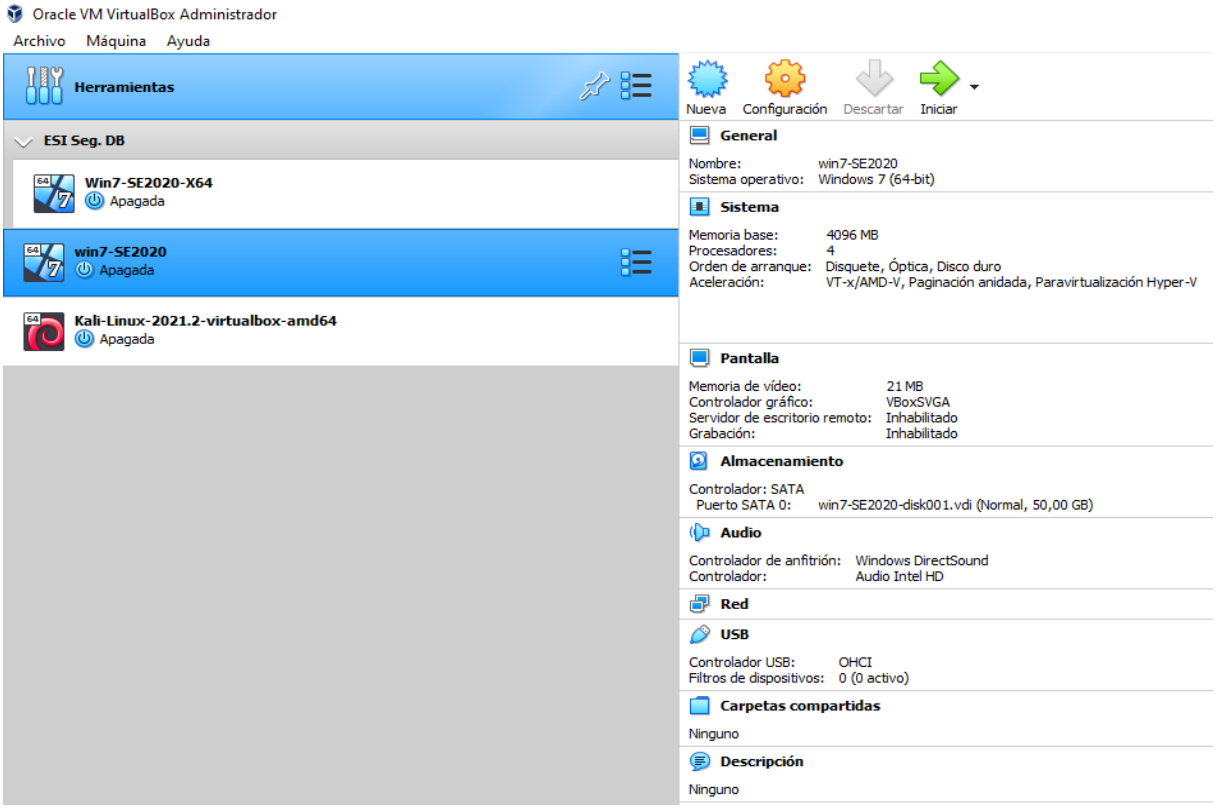
**Memoria video:** 21 MB

**Controlador Gráfico:** VBoxSVGA

**Controlador:** SATA

**Controlador USB:** OHCI

*Figura 12.* Configuración equipo Win 7-SE2020




Fuente: El autor

**Kali – Linux -2021-2 Virtualbox amd 64:**

**Sistema operativo:** Debian (64 bit)

**Memoria base:** 4048 MB

**Procesadores:** 2

**Orden de arranque:** Disco duro, Óptica.

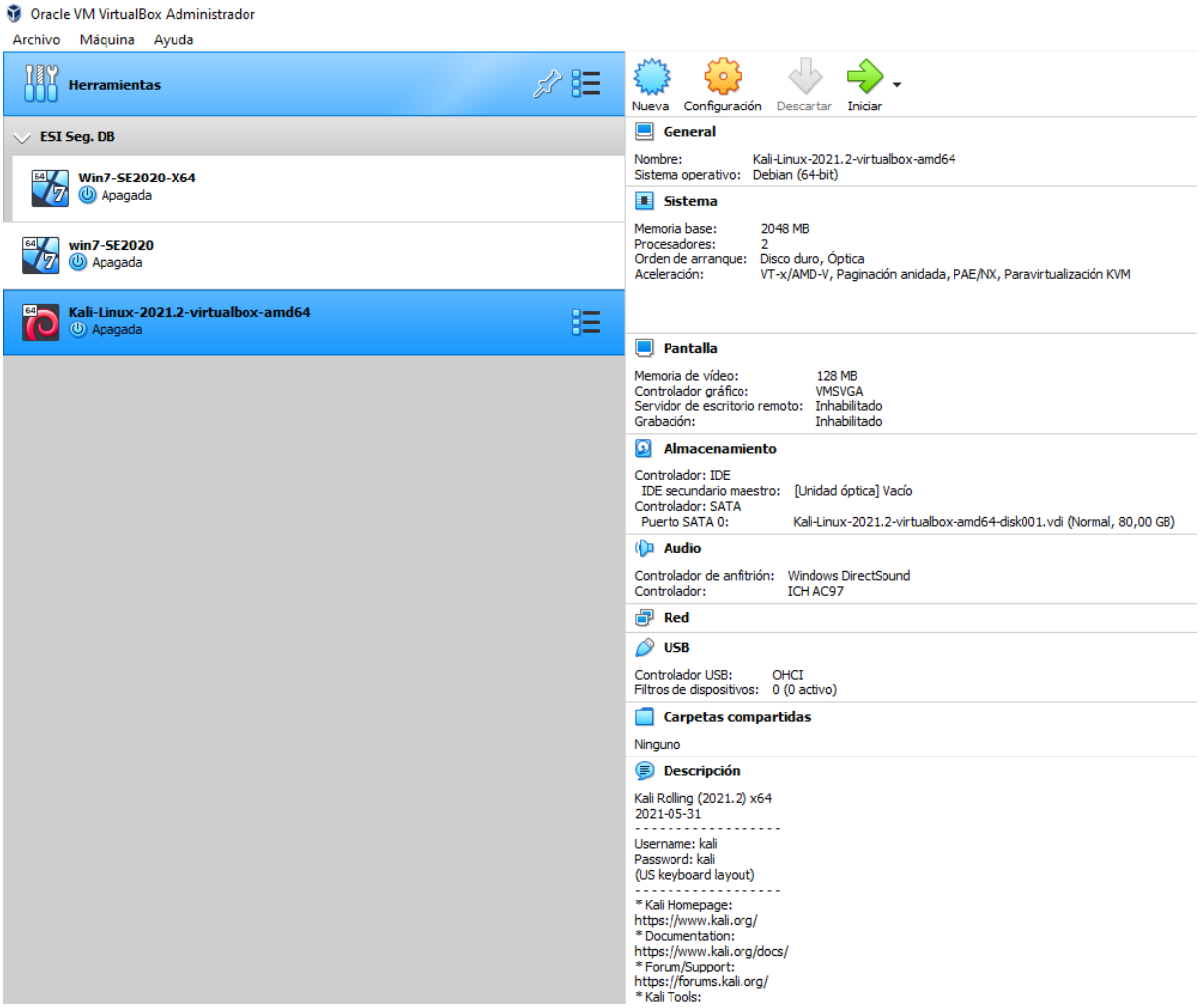
**Memoria video:** 128 MB

**Controlador Gráfico:** VMSVGA

**Controlador:** SATA

**Controlador USB:** OHCI

*Figura 13.* Configuración equipo Kali – Linux -2021-2 Virtualbox amd 64




Fuente: El autor

## 5.4. ANÁLISIS LEGAL Y ETICO DEL ANEXO 2 – ESCENARIO 2 Y ANEXO 3

Tabla 1. Análisis legal y ético del anexo 2

| Documento | Fragmentos Ilegales o no éticos | Argumentos |
|---|---|---|
| **ANEXO 2** | Este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal. | La empresa ha actuado de forma poco ética al desconocer la información del contrato teniendo en cuenta que dentro de las prohibiciones en el código de ética se encuentran permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por la ley, esta situación puede facilitar la participación y patrocinio de actividades ilegales. Por otro lado dentro de los deberes está respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de las profesiones relacionadas con la ingeniería, así como denunciar todas las transgresiones y velar por el buen prestigio de los profesionales; teniendo en cuenta lo anterior y los antecedentes del abogado que asesoró la transcripción de los contratos de la compañía, esta debió ejecutar las revisiones pertinentes para asegurar el cumplimiento de la ley y la ética profesional relacionada. |
| **ANEXO 3** | Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, **se obliga a no divulgar directa, indirecta, próxima o remotamente**, ni a través de ninguna otra persona o de sus subalternos o funcionarios, **autoridades legales**, asesores o **cualquier persona relacionada con ella**, la información confidencial o **sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados**. | En esta clausula se vulneran varios de los deberes y prohibiciones del código de ética, dentro de los que se pueden resaltar: La obligación de la no divulgación de la información no puede estar supeditada a autoridades legales ni a personas relacionadas con ella; lo anterior teniendo en cuenta que el código de ética indica que se debe impedir o evitar el ocultamiento o utilización indebidos de la información y permitir el acceso inmediato a autoridades de policía en caso de investigación y denunciar los delitos, contravenciones y faltas contra el código de ética aportando la información que se tenga sobre los procesos ilegales que se estén llevando a cabo. La ley 1581 de 2012 de datos personales que legisla el derecho que las personas tienen a conocer para este caso la información que sobre ellas se maneje en la compañía. |
| **ANEXO 3** | **Datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".** | Este punto es ilegal teniendo en cuenta que en la ley 1273 de 2009 se contempla dentro de los delitos informáticos el acceso abusivo a los sistemas informáticos y la interceptación de información sin órdenes judiciales o autorización valida. |

| Documento | Fragmentos Ilegales o no éticos | Argumentos |
|---|---|---|
| **ANEXO 3** | No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros. | En el código de ética registra como deber de los profesionales denunciar los delitos, contravenciones y faltas contra la ética y que se puedan registrar dentro del ejercicio de la profesión y el espionaje y la apropiación de la información de terceros está catalogada como delito en la ley 1273 de 2009. |
| **ANEXO 3** | Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas. | Es deber de los profesionales denunciar los delitos, contravenciones y faltas contra la ética registrados en el ejercicio de la profesión y el hecho de conocer que la información tratada en las reuniones corresponde a actos ilegales denota una responsabilidad ética y legal del profesional para con la sociedad y dignidad de la profesión. |
| **ANEXO 3** | Se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security. | La empresa no puede obligar a sus profesionales a ocultar información confidencial y/o ilegal ya que las personas relacionadas con la información tienen derecho legal a conocer la información relacionada con ellas; por otra parte el profesional tiene deber de denunciar los actos ilegales que atenten contra la sociedad y su profesión y los delitos informáticos tienen penas económicas e intramural que pueden afectar la vida de los mismos. |
| **ANEXO 3** | la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas. | Algunos de los delitos informáticos indicados en la ley 1273 de 2009 indican que es un agravante a los hechos, si para consumar los delitos el agente ha reclutado víctimas en la cadena del delito; esto quiere decir que la empresa también tiene responsabilidades frente a los delitos que se llegaran a evidenciar ante cualquier denuncia realizada a las autoridades. |
| **ANEXO 3** | En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security. | Algunos de los delitos informáticos indicados en la ley 1273 de 2009 indican que es un agravante a los hechos, si para consumar los delitos el agente ha reclutado víctimas en la cadena del delito; esto quiere decir que la empresa también tiene responsabilidades frente a los delitos que se llegaran a evidenciar ante cualquier denuncia realizada a las autoridades. |

Fuente: Construcción propia autor

## 5.5. ARTICULOS VULNERADOS DE LA LEY 1273 EN LOS ANEXOS

Tabla 2. Artículos vulnerados de la ley 1273 en los anexos

| Documento | Fragmentos Ilegales o No éticos | Artículos de la ley 1273 vulnerados |
|---|---|---|
| **ANEXO 2** | La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal. | Los artículos 269F violación de datos personales y 269G suplantación de sitios web para capturar datos personales, sentenciados en la ley 1273 de 2009 indican que es un agravante a los hechos, si para consumar los delitos el agente ha reclutado víctimas en la cadena del delito; esto quiere decir que la empresa también tiene responsabilidades frente a los delitos que se llegaran a evidenciar ante cualquier denuncia realizada a las autoridades y que el contrato debió revisarse para mitigar los riesgos derivados de actuaciones ilegales para las que se esté reclutando personas. |
| **ANEXO 3** | **Se obliga a no divulgar directa, indirecta, próxima o remotamente,** ni a través de ninguna otra persona o de sus subalternos o funcionarios, **autoridades legales,** asesores o cualquier **persona relacionada con ella,** la información confidencial **o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.** | Puede estar relacionado con el artículo 269F ya que al no poder divulgar información a personas relacionadas con la misma se puede estar atentando o violentando los datos personales teniendo en cuenta la ley 1581 de 2012 de datos personales que legisla el derecho que las personas tienen a conocer para este caso la información que sobre ellas se maneje en la compañía. |
| **ANEXO 3**<br><br>**ANEXO 3** | **Datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".**<br><br>**No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.** | Este punto es ilegal teniendo en cuenta que en la ley 1273 de 2009 se contempla dentro de los delitos informáticos el acceso abusivo a los sistemas informáticos en el articulo 269A y la interceptación de información 269C sin órdenes judiciales o autorización valida.<br><br>El espionaje puede estar catalogado como el acceso abusivo a datos informáticos 269A y la interceptación en las comunicaciones 269C, en cuanto la apropiación de la información de terceros está decretada en el artículo 269I que habla de hurto de datos por medios informáticos o parecidos. |
| **ANEXO 3** | **Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.** | Esta conducta puede estar cualificada dentro del artículo 269H que registra las circunstancias de agravación punitiva, al indicar que todas las conductas derivadas en delitos informáticos, realizadas por los administradores que tienen a cargo la administración, control o manejo de información pueden desencadenar la inhabilidad en la profesión hasta por 3 años. |

| Documento | Fragmentos Ilegales o No éticos | Artículos de la ley 1273 vulnerados |
|---|---|---|
| **ANEXO 3** | Se obliga a **no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.** | Esta conducta puede estar cualificada dentro del artículo 269H que registra las circunstancias de agravación punitiva, al indicar que todas las conductas derivadas en delitos informáticos, realizadas por los administradores que tienen a cargo la administración, control o manejo de información pueden desencadenar la inhabilidad en la profesión hasta por 3 años. |
| **ANEXO 3** | La parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas. | Los delitos informáticos 269F violación de datos personales y 269G en caso de que se capturen por suplantación de sitio web que se indican en la ley 1273 de 2009 indica que es un agravante a los hechos, si para consumar los delitos el agente ha reclutado víctimas en la cadena del delito; esto quiere decir que la empresa también tiene responsabilidades frente a los delitos que se llegaran a evidenciar ante cualquier denuncia realizada a las autoridades. |
| **ANEXO 3** | En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security. | Los delitos informáticos 269F violación de datos personales y 269G en caso de que se capturen por suplantación de sitio web que se indican en la ley 1273 de 2009 indica que es un agravante a los hechos, si para consumar los delitos el agente ha reclutado víctimas en la cadena del delito; esto quiere decir que la empresa también tiene responsabilidades frente a los delitos que se llegaran a evidenciar ante cualquier denuncia realizada a las autoridades. |

Fuente: Construcción propia autor

## 5.6. ARGUMENTACIÓN DE LA APLICACIÓN AL TRABAJO EN THE WHITEHOUSE

Teniendo en cuenta la situación actual del país y la posición de diferentes frentes de la actualidad Colombiana en los cuales la marrullería y corrupción son el pan de cada día y las oportunidades para los profesionales son cada vez más limitadas, una oportunidad de este calibre podría verse muy alentadora y tentadora; sin embargo, para muchos ingenieros que aún creemos en la dignidad, en la ética y honestidad de la profesión, esta circunstancia está cargada de muchas restricciones de índole moral, ética y legal

que podrían atentar gravemente no solo contra los principios inculcados en la familia, comunidad educativa, laboral y profesional, si no en la posibilidad de perder la habilidad para ejercer la profesión, la estabilidad económica y la libertad.

El código de ética para ingenieros dentro de sus postulados define algunos de los eventos que se transgredirían con la aceptación de la labor en cuestión y las causales por las cuales no sería procedente la aceptación del cargo, teniendo en cuenta el punto de vista moral expuesto en este mismo punto:

1. La violación comprobada de este código puede acarrear la suspensión hasta por 5 años o la cancelación de la matrícula profesional.
2. Dentro de los deberes generales de los profesionales se especifica en el punto b la custodia de la información que se le encomiende evitando el ocultamiento y uso indebido de la misma.
3. En el punto e indica como deber también permitir el acceso por parte de las autoridades de policía a los lugares y documentados dentro de las investigaciones para facilitar la ejecución de la labor.
4. Denunciar los delitos, contravenciones y faltas contra el código a los cuales tenga acceso y conocimiento ejerciendo la profesión, entregando las pruebas y documentos que tenga al alcance, es el punto f de estos mismos deberes.
5. Dentro de las prohibiciones se enuncia el permitir, tolerar o dar facilidad para ejercer de forma ilegal esta profesión.
6. Se prohíbe el ofrecimiento o aceptación de labores en contra de la legislación vigente.
7. En los deberes para con la dignidad de la profesión se indica el respeto por las disposiciones legales y reglamentos que normen los actos de la profesión y la denuncia de todas las infracciones.
8. En caso de obligación legal se debe revelar la información relacionada con el trabajo y que tenga reserva o secreto profesional, lo anterior constituye un deber en pro de la dignidad de la profesión.

## 5.7. PUNTO DE VISTA “OPERACIÓN ANDROMEDA BUGGLY”

El caso de la “OPERACIÓN ANDROMEDA BUGGLY” en donde supuestamente esta fachada servía al Ejercito Nacional de Colombia para actividades de inteligencia que se orientaban a detectar amenazas de ciberseguridad y que con las investigaciones realizadas destapo una serie de incidencias que desencadenaron capturas e investigaciones por parte de la Fiscalía General de la Nación al encontrar acontecimientos aparentemente de índole ilegal y que de acuerdo a la lectura realizada de los acontecimientos que involucraron este escándalo podría tener las siguientes implicaciones legales y éticas:

Implicaciones legales contempladas en la ley 1273 de 2009:

1. Acceso abusivo a sistemas informáticos: esto de acuerdo a las declaraciones que especifican que se inyectaron malware a equipos ajenos para lograr obtener información.
2. Interceptación de datos informáticos: Las llamadas chuzadas, espionaje de correos electrónicos e información de alcaldes de zonas en donde había presencia de guerrilla de forma ilegal pudieron incurrir en este delito.
3. Uso de software malicioso: De acuerdo a las indagaciones se pudo establecer el uso de software malicioso para conseguir datos de personas e interceptar comunicaciones.
4. Violación de datos personales: En esta operación se accedió a información confidencial de las personas incluso sin autorización de las mismas; se habla también de la comercialización y divulgación de información confidencial entre personas civiles y del ejército que hacían parte de los equipos reclutados para esta conspiración.
5. Todos estos delitos tienen dentro de sus penalidades intramural entre 48 y 96 meses y multas económicas entre 100 y 1.000 SMLMV.

6. En el Artículo 269H que trata sobre eventos que agravan punitivamente y las penas se pueden aumentar de la mitad a tres cuartas partes si se prueban, se pueden destacar varios que entrarían a jugar dentro de las conductas observadas:

- Se habla de un posible espionaje a los acuerdos de paz, lo que se podría relacionar con sistemas o redes informáticas gubernamentales.
- Al estar involucrado el personal del ejército nacional, se entiende que estos son servidores públicos ejerciendo las funciones de su cargo.
- Se indicó que algunos de los personajes involucrados recibieron dineros a cambios de información y bases de datos que se consiguieron durante la operación, logrando así beneficios económicos para sí o para terceros.
- En la operación se involucraron personas civiles a algunas de las cuales se les indicó que se estaban construyendo grupos de hacking para compartir conocimientos, aún no es claro si se utilizó como herramienta a personas de buena fe que al parecer no sabían sobre la fachada y objetivos reales de este proyecto.

Implicaciones éticas que se registran en el código de la profesión:

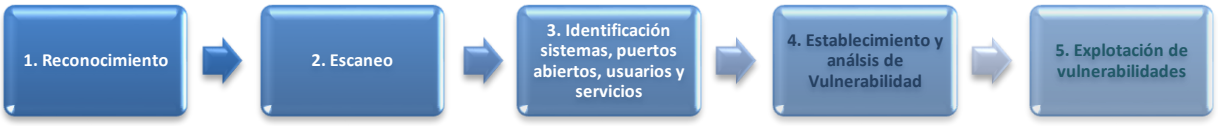
1. Cancelación de matriculas profesionales para los ingenieros involucrados en las actividades ilícitas que se identificaron.
2. Deber de custodiar la información a cargo, evitando la realización de acciones indebidas, esto va relacionado a la venta de información a terceros que se pudo establecer y a la interceptación ilegal de las comunicaciones que se podrían catalogar como acciones indebidas.
3. Al parecer no hubo denuncias por parte de las personas que se involucraron en estos acontecimientos, aún a sabiendas de que posiblemente se trataba de actos ilegales; este es un deber del ingeniero dentro del ejercicio de sus funciones.
4. Es prohibido facilitar, permitir y tolerar la realización de actividades delictivas dentro de la profesión, esto para las personas que se involucraron tanto los militares como los civiles.

5. El hecho del ofrecimiento y aceptación de trabajo que atenta contra la normatividad vigente por medio de funcionarios del ejército nacional o personal civil con conocimientos en la profesión, infringe una de las prohibiciones del código que se está analizando.
6. Para con la dignidad de la profesión se quebrantan el respeto y hacer respetar las normas legales dentro de las actuaciones de los profesionales y la denuncia de actividades que transgredan las mismas.
7. Ninguno de los involucrados ha dejado en alto la profesión, al contrario este tipo de actuaciones la desprestigian.
8. Al realizar la comercialización de información conseguida durante la operación, se falto a los deberes con el público en general, en donde se recomienda mantener el secreto y la reserva de la información a cargo del profesional; al igual que esta misma conducta se veda dentro de las prohibiciones respecto al público en general.

## 5.8. HERRAMIENTAS SOFTWARE UTILIZADAS PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3

Para la enumeración de las herramientas de software utilizadas en la ejecución de las pruebas se establecerán las etapas en las que se utilizaron y los procedimientos especificados:

*Figura 14.* Actividades de pruebas Pentesting




Fuente: ALCALDÍA DE BOGOTÁ. Guardianes de la información Penetration Testing. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

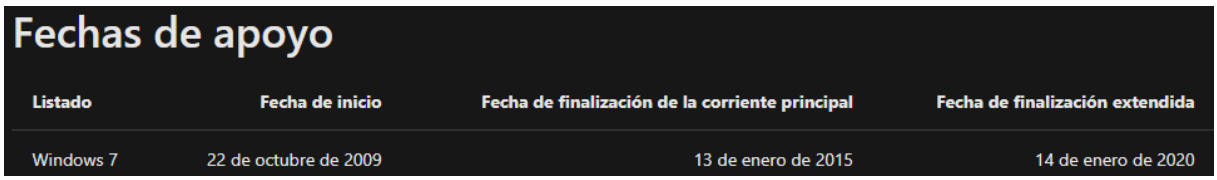
### 5.8.1. Reconocimiento

Para esta etapa se escudriña e investiga toda la información necesaria con el ánimo de orientar y poder desarrollar las pruebas.

De acuerdo a la información recopilada por la compañía se puede establecer que el equipo involucrado cuenta con un sistema operativo Windows 7 X64, tiene instalada una aplicación llamada Rejetto y existen sospechas de una escalada de privilegios dentro del sistema.

**Windows 7 X64:** Esta versión de Windows salió al mercado en 2009, el soporte del proveedor finalizó en 2015 y la extensión del soporte terminó en 2020; esta situación hace que este sistema operativo se convierta en un vector de ataque ya que al no existir soporte del software esta obsolescencia puede traer consigo descubrimiento de nuevas vulnerabilidades y exploits exitosos.

*Figura 15.* Ciclo de vida de Windows 7



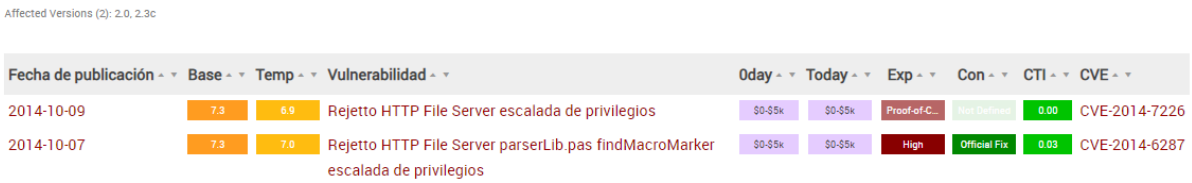
Fechas de apoyo

| Listado | Fecha de inicio | Fecha de finalización de la corriente principal | Fecha de finalización extendida |
|---|---|---|---|
| Windows 7 | 22 de octubre de 2009 | 13 de enero de 2015 | 14 de enero de 2020 |

Fuente: https://docs.microsoft.com/en-us/lifecycle/products/windows-7

**Aplicación Rejetto:** Al validar información en la web sobre esta aplicación se puede establecer que esta se relaciona con vulnerabilidades que permiten que atacantes por medio de una reverse Shell acceder y controlar remotamente al equipo, lo que puede facilitar entre otros una escalada de privilegios.

*Figura 16.* Vulnerabilidades Rejetto HTTP File



Affected Versions (2): 2.0, 2.3c

| Fecha de publicación | Base | Temp | Vulnerabilidad | 0day | Today | Exp | Con | CTI | CVE |
|---|---|---|---|---|---|---|---|---|---|
| 2014-10-09 | 7.3 | 6.9 | Rejetto HTTP File Server escalada de privilegios | $0-$5k | $0-$5k | Proof-of-C... | Not Defined | 0.00 | CVE-2014-7226 |
| 2014-10-07 | 7.3 | 7.0 | Rejetto HTTP File Server parserLib.pas findMacroMarker escalada de privilegios | $0-$5k | $0-$5k | High | Official Fix | 0.03 | CVE-2014-6287 |

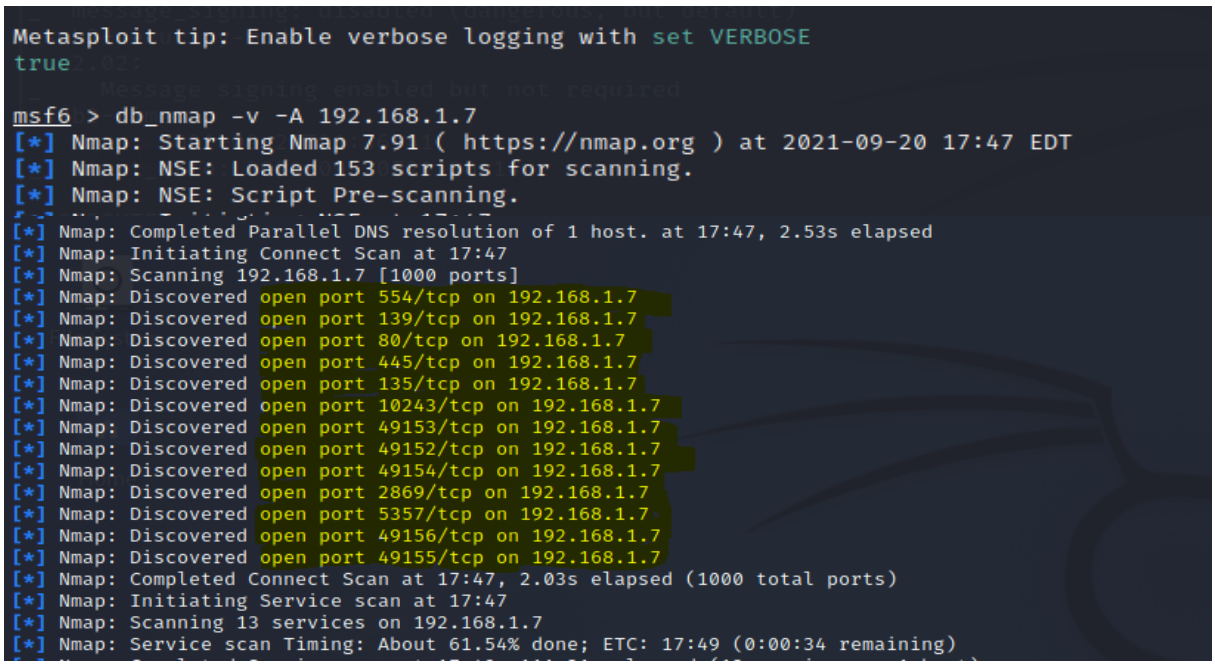
Fuente: https://vuldb.com/es/?product.rejetto:http_file_server Figura 2. Vulnerabilidades Rejetto HTTP File

**Escalada de privilegios:** Este evento se presenta cuando un atacante explota fallos o debilidades de aplicaciones o sistemas, con esto logra acceder a permisos de acceso amplios que de ninguna manera debería tener; estos accesos le pueden permitir ingreso a algunas áreas restringidas que podrían contener información sensible o disponible para ser sustraída. Se conoce también como elevación de privilegios.

### 5.8.2. Escaneo de puertos, servicios y sistemas operativos

Para esta actividad es necesaria la reducción de rangos de IPS a un listado de equipos activos. Para ello es necesario realizar un barrido de ping o escaneo de ICMP para localizar los equipos activos en red limitando los test a host encontrados. Esta etapa se puede realizar con ayuda de **Nmap** utilizando el comando **db_nmap –v-A <Ip a validar>**, para este ejercicio lo haremos desde la herramienta **metasploit** esto listara los puertos abiertos en la máquina víctima.

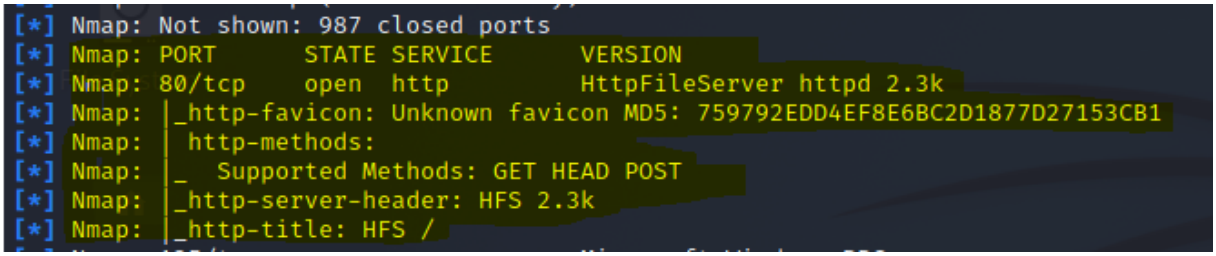
*Figura 17.* Escaneo de puertos máquina víctima herramienta nmap




Fuente: El autor

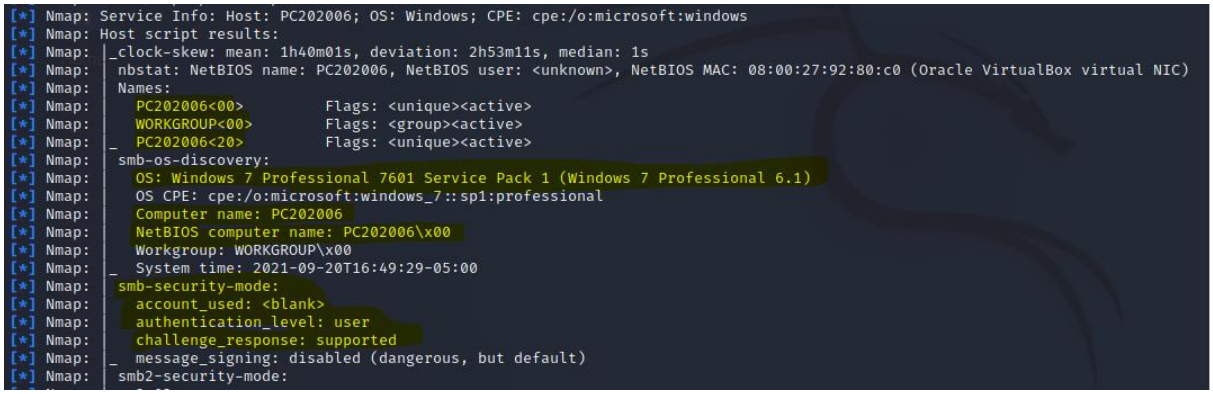
También se realiza un banner grabbing que permite establecer información de sistemas operativos que puede dar información sobre la red y equipos, también se puede conseguir información por medio de la huella de la pila TCP/IP que facilita dirigir la configuración de herramientas para análisis de vulnerabilidades.

*Figura 18.* Identificación del puerto 80, servicio, versiones



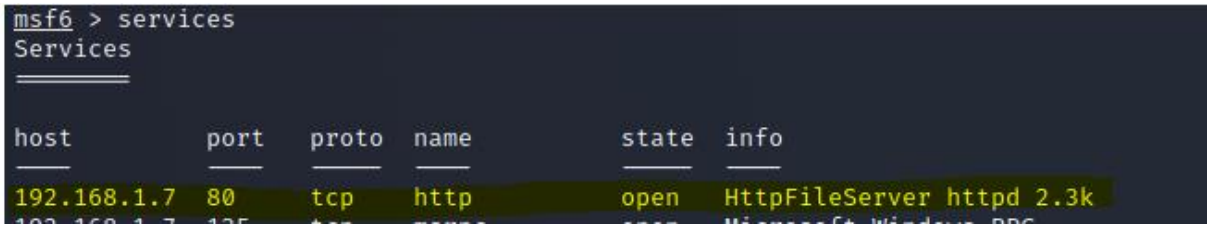

Fuente: El autor

*Figura 19.* Información del equipo a atacar




Fuente: El autor

*Figura 20.* Comando Services identifica el servicio del puerto 80 - Http File Server se encuentra activo



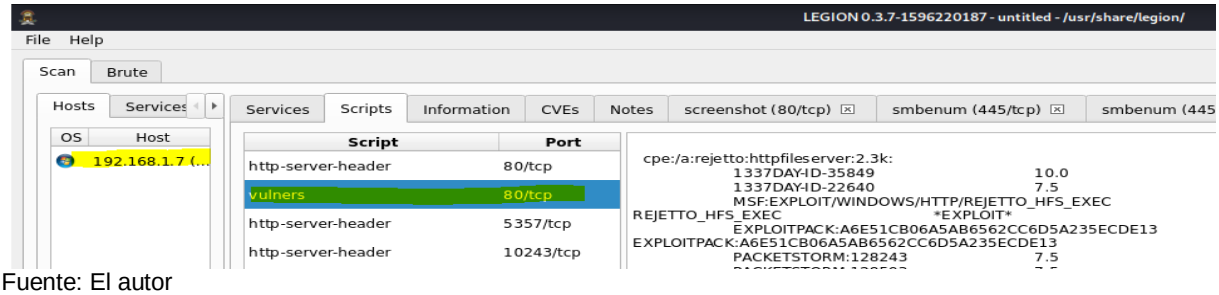

Fuente: El autor

### 5.8.3. Establecimiento y análisis de vulnerabilidades

Con la plena identificación de sistemas operativos en los equipos, estos resultados sirven para establecer la ruta del análisis de vulnerabilidades. El administrador de contenidos y los pluggins se pudieron haber establecido con el análisis de banners, esto puede dejar al descubierto información de vulnerabilidades existentes que si no han sido remediadas puede ser un riesgo alto para la infraestructura.

Para realizar el escaneo de vulnerabilidades dentro de los dispositivos identificados se pueden utilizar diferentes mecanismos, para esta prueba se utilizó la herramienta **Legión**.

*Figura 21.* Establecimiento de vulnerabilidades puerto 80 – Herramienta Legión




Fuente: El autor

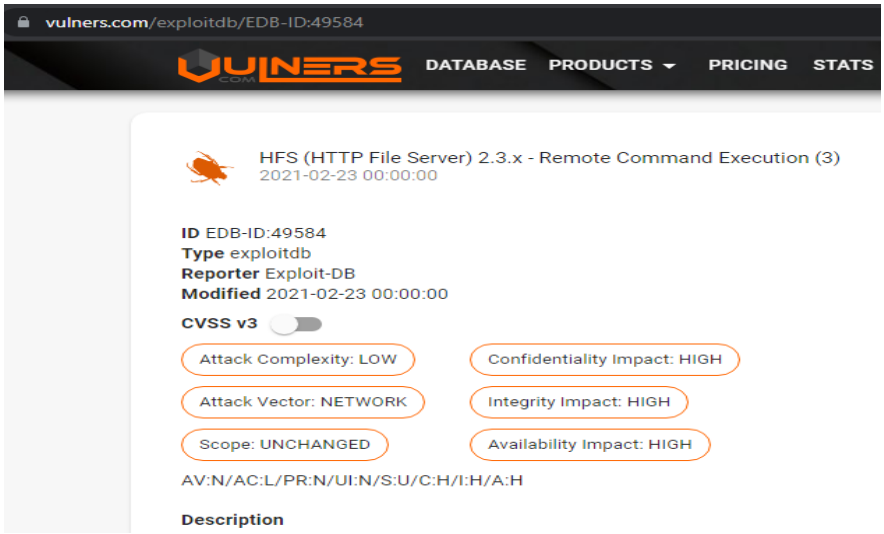
*Figura 22.* Establecimiento de vulnerabilidades puerto 80 – Herramienta Legión


Fuente: El autor

### 5.8.4. Plan de Explotación de vulnerabilidades

Con el resultado de las vulnerabilidades que se identificaron se debe establecer la clasificación de acuerdo a la criticidad, tipo y la existencia de exploit de acuerdo a la validación en páginas como https://www.rapid7.com/db y https://www.exploit-db.com/search/. Las vulnerabilidades que presenten exploit disponible se clasificaran en cuatro grupos: las que se puedan gestionar remotamente con exploits remotos, los que necesitan acceso local a la máquina, los que explotan debilidades de los aplicativos web y por último las que pueden generar indisponibilidad de servicio. En la página exploitdb vulners se puede identificar el exploit para la vulnerabilidad identificada en la etapa anterior con Legión.

*Figura 23.* Información exploitdb para vulnerabilidad identificada en fase anterior



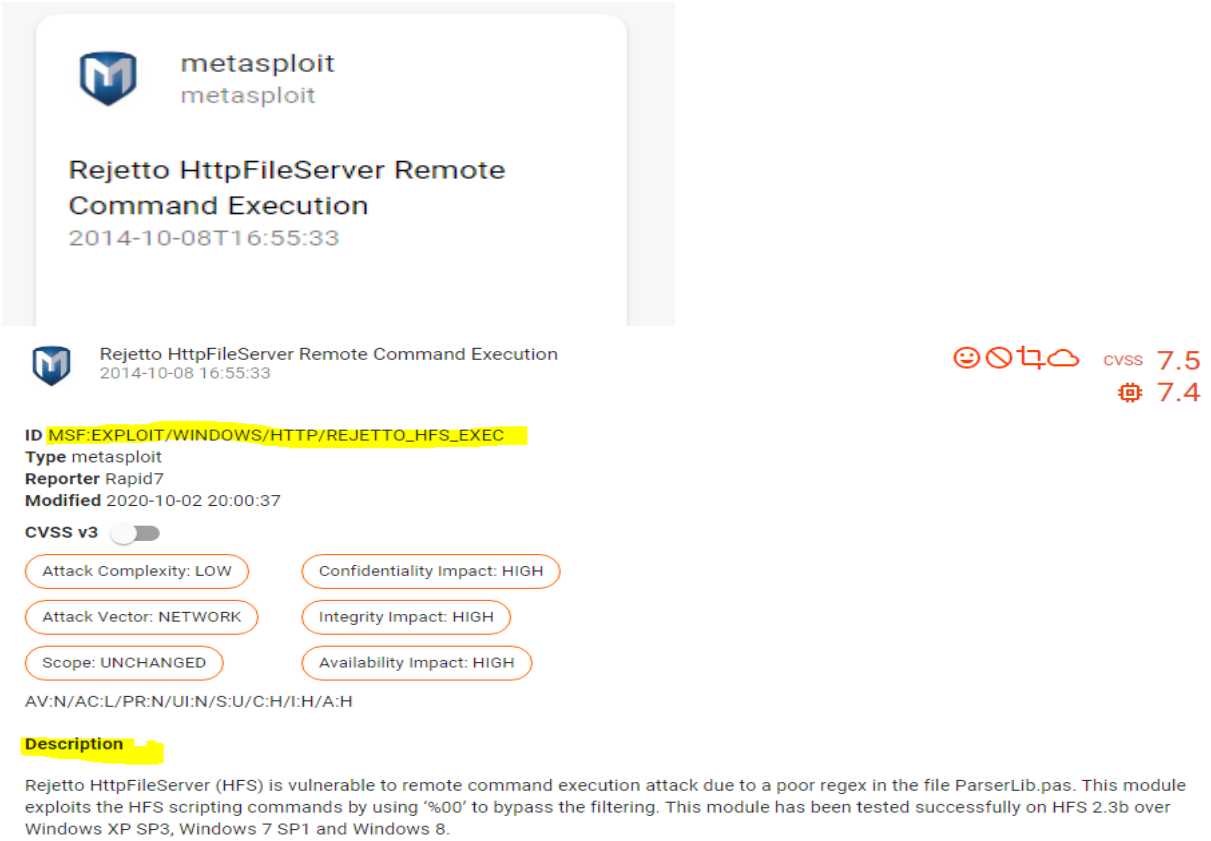

Fuente: El autor

### 5.8.5. Explotación de vulnerabilidades

Empieza con la elección de las herramientas y exploits para explotar las debilidades priorizadas; para la realización de estas actividades se elige el Metasploit y exploits a aplicar en base a las vulnerabilidades encontradas y que se plantearon en el plan de explotación. Se configura cada una de las elecciones para atacar que tiene el

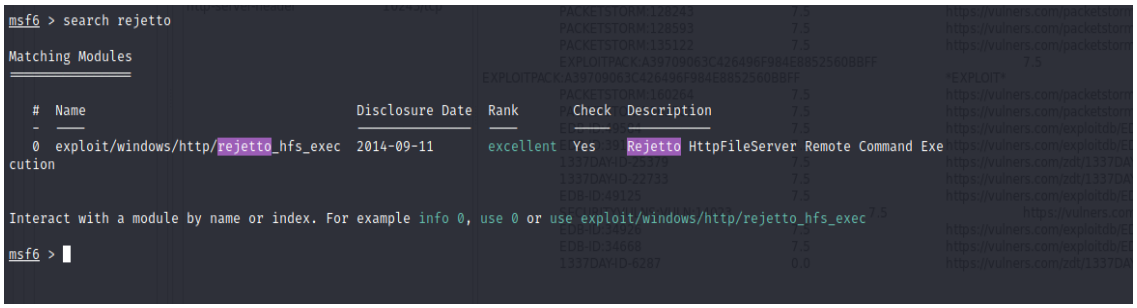
Metasploit con base a las vulnerabilidades y las versiones tanto de la aplicación como de servicios y sistemas operativos. El exploit es lanzado después de la configuración en el Metasploit al servidor objetivo, se recogen evidencias del resultado del ataque y la información del **Metasploit** o las capturas que se evidencian en la explotación.

*Figura 24.* Metasploit herramienta elegida para explotar la vulnerabilidad de Rejetto



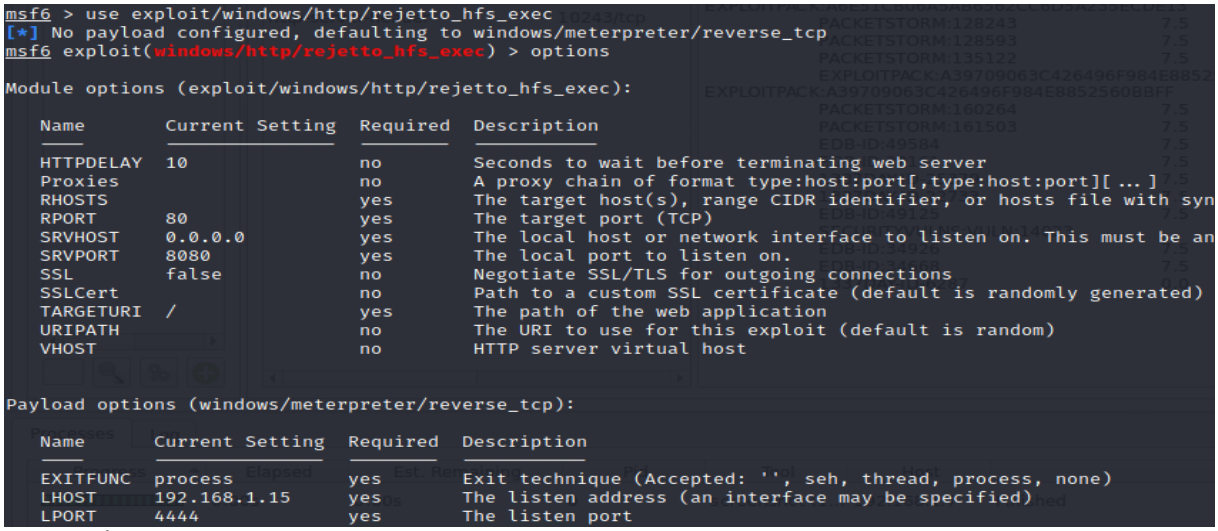

Fuente: El autor

*Figura 25.* Búsqueda del módulo Metasploit Rejetto y validación de opciones



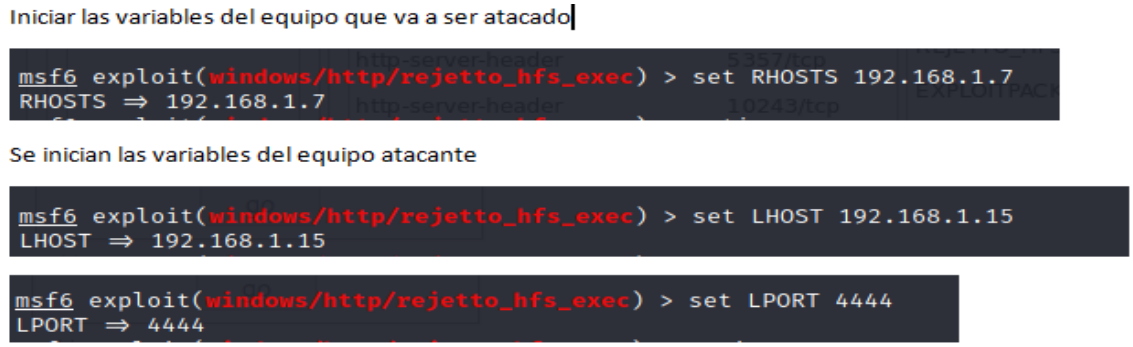

Fuente: El autor

*Figura 26.* Búsqueda del módulo Metasploit  Rejetto y validación de opciones



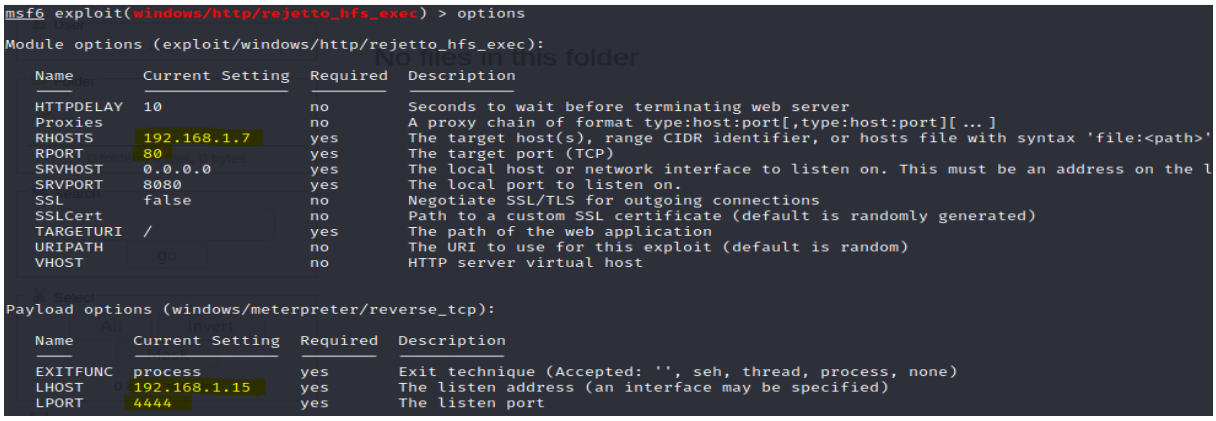

Fuente: El autor

*Figura 27.* Inicialización y parametrización de variables para el ataque



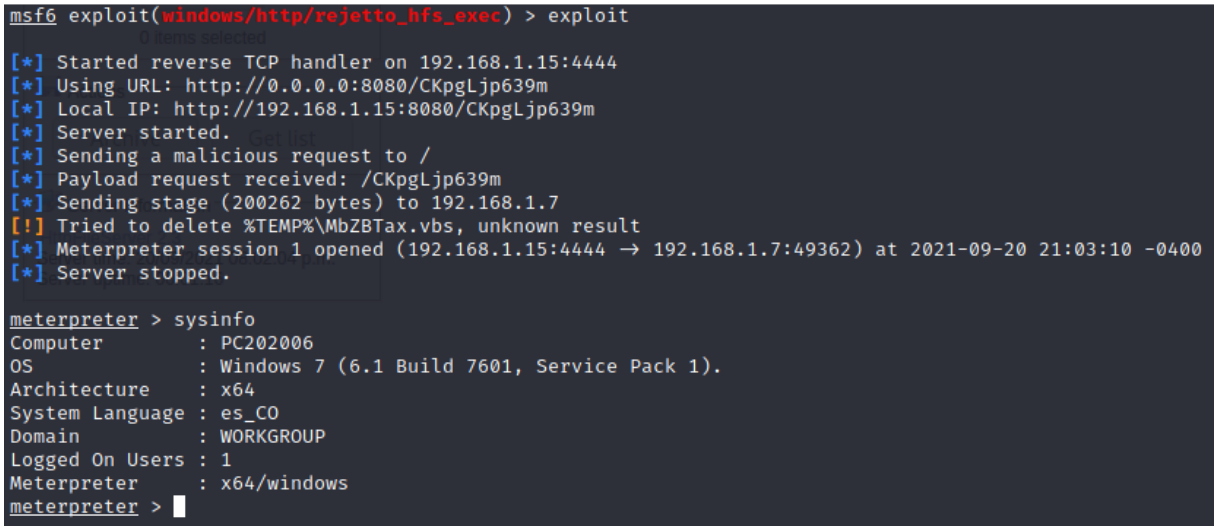

Fuente: El autor

*Figura 28.* Variables cargadas en el módulo para efectuar el ataque



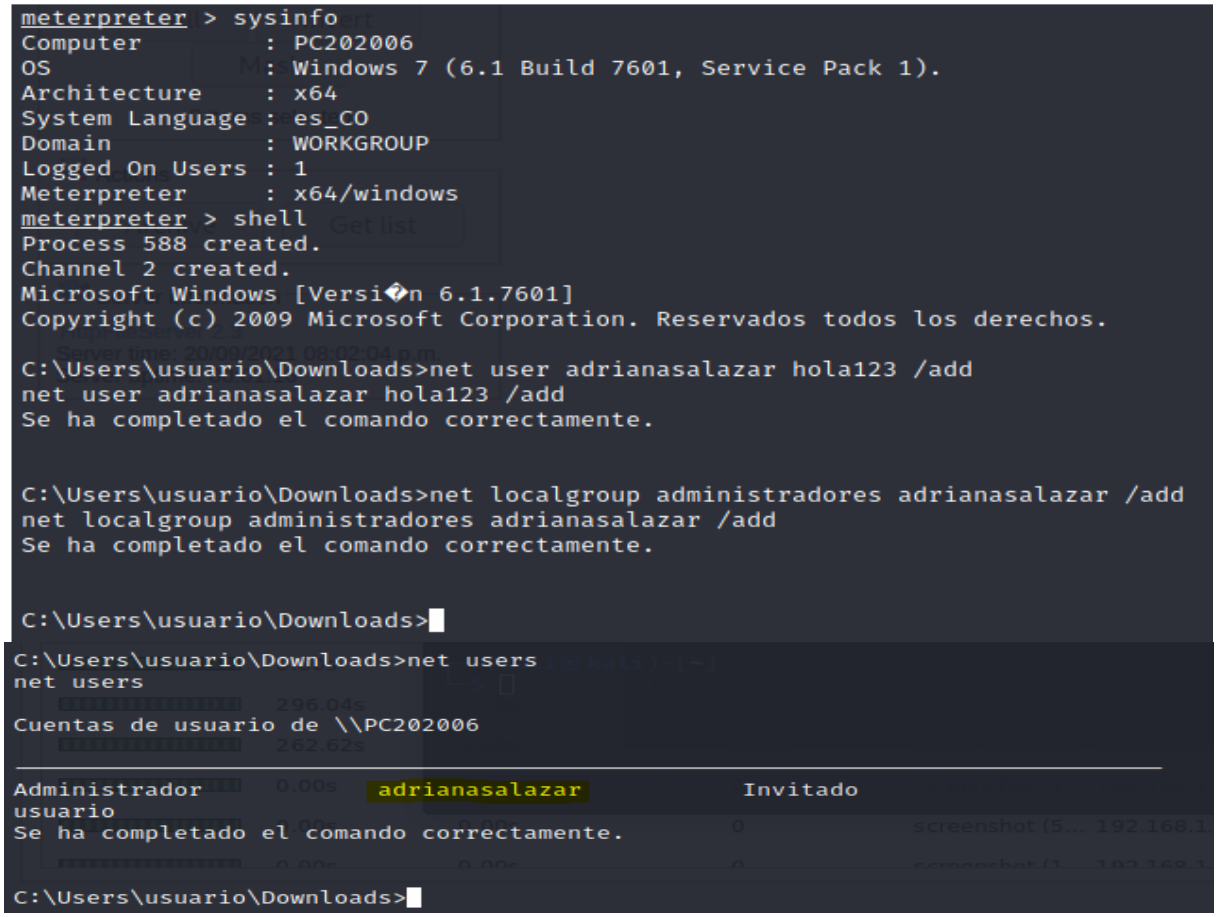

Fuente: El autor

*Figura 29.* Explotación de la vulnerabilidad




Fuente: El autor

*Figura 30.* Creación de usuario desde meterpreter y comando Shell para abrir cmd del equipo atacado




Fuente: El autor

## 5.9. DATOS ANEXO 4 – ESCENARIO 3 QUE APOYARON EL DESCUBRIMIENTO DEL FALLO

De acuerdo a la información recopilada en el anexo 4 del escenario 3 se puede establecer que el equipo involucrado cuenta con un sistema operativo:

**Windows 7 X64**: Esta versión de Windows salió al mercado en 2009, el soporte del proveedor finalizó en 2015 y la extensión del soporte terminó en 2020; esta situación hace que este sistema operativo se convierta en un vector de ataque ya que al no incluir soporte del software esta obsolescencia puede traer consigo descubrimiento de nuevas vulnerabilidades y exploits exitosos.

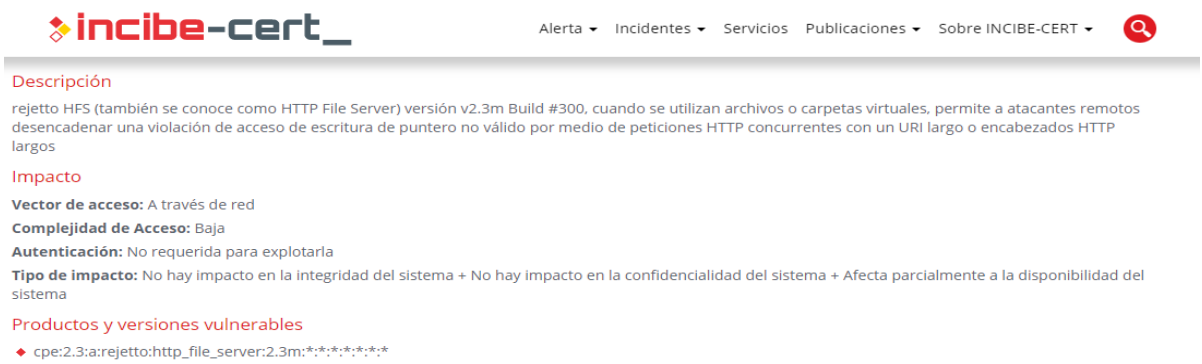
De igual manera se especifica la existencia de una aplicación instalada en la máquina que está presentando fugas de información:

**Aplicación Rejetto**: Al validar información en la web sobre esta aplicación se puede establecer que esta se relaciona con vulnerabilidades que permiten que atacantes por medio de una reverse Shell acceder y controlar remotamente al equipo, lo que puede facilitar entre otros una escalada de privilegios.

*Figura 31.* Vulnerabilidades Rejetto HTTP File


Fuente: https://vuldb.com/es/?product.rejetto:http_file_server Figura 2. Vulnerabilidades Rejetto HTTP File

*Figura 32.* Información Rejetto incibe - cert




Fuente: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

Y se habla de la investigación de un posible ataque de:

**Escalada de privilegios:**

Este evento se presenta cuando un atacante explota fallos o debilidades de aplicaciones o sistemas, con esto logra acceder a permisos de acceso amplios que de ninguna manera debería tener; estos accesos le pueden permitir ingreso a algunas áreas restringidas que podrían contener información sensible o disponible para ser sustraída. Se conoce también como elevación de privilegios.

## 5.10. HERRAMIENTAS UTILIZADAS PARA IDENTIFICAR FALLOS EN EL EQUIPO DE WINDOWS 7 Y PUERTO ABIERTO POR APLICACIÓN

En primera instancia para realizar la identificación de los fallos en la máquina atacada para este ejercicio fueron necesarias las siguientes herramientas desde el equipo Kali Linux en donde se desarrollo el ataque:

**Nmap:** Permitió realizar el escaneo de puertos del equipo para establecer aspectos como: puertos abiertos, estado del servicio, identifica la versión y el puerto por el cual está abierto la aplicación, sistema operativo e información del equipo.
**Esta herramienta descubre que la aplicación rejetto 2.3 abre el puerto 80.**

**Legion:** Esta herramienta permitió realizar un análisis de las **vulnerabilidades presentes en el equipo y puerto 80**, arroja una serie de información como códigos de vulnerabilidad que permiten documentarse frente a la consistencia y explotabilidad de las mismas.

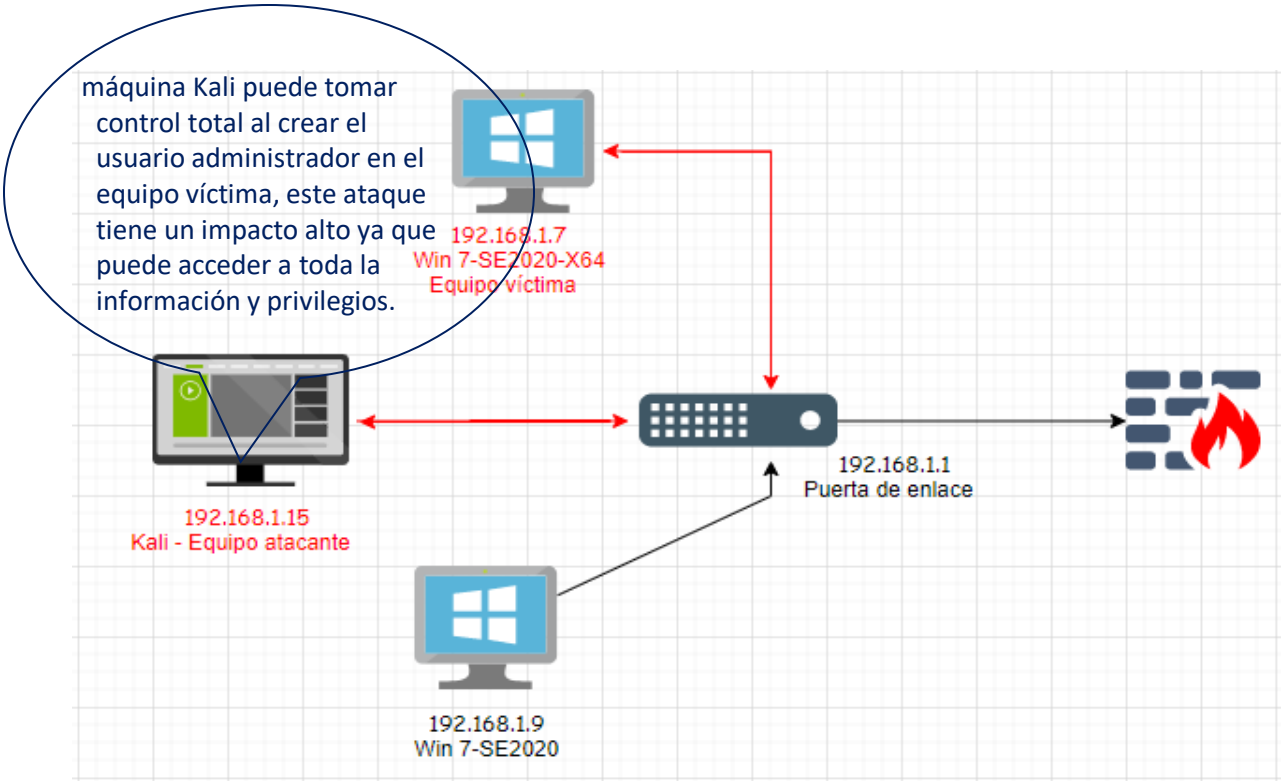
**Exploitdb:** Esta herramienta permite realizar la consulta de la información del código de vulnerabilidad que arrojo Legion, se despliegan datos de la criticidad, explotabilidad, exploit, impacto, vectores de ataque, etc. Adicionalmente allí se ubicó la información de metasploit y el ID que define el comando a utilizar para realizar la explotación de dicha vulnerabilidad.

**Metasploit:** En este módulo se ejecuta el comando que encontramos en Exploitdb, se cargan las opciones del módulo y se inicializan las variables con información de la máquina atacante y el equipo a atacar para gestionar la comunicación entre las máquinas que garantice el éxito del ataque y se lanza el comando que ejecuta el ataque, se consigue el ingreso al equipo y se procede a ejecutar la creación de usuario administrador.

## 5.11. COMO AFECTA EL ATAQUE A LA MÁQUINA WINDOWS 7 X 64

Este ataque permite que el usuario atacante por medio de la identificación de puertos abiertos e información que arroja el escaneo realizado obtenga datos de la vulnerabilidad identificada en el puerto 80 con la aplicación rejetto; con esta información accede al equipo víctima remotamente utilizando lo investigado y explotando la vulnerabilidad. Ya dentro de la máquina a atacar se crea un usuario administrador, desde el meterpreter ejecutando el comando Shell. Ya con esta actividad realizada puede ejecutar diferentes acciones (borrar usuarios, crear cuentas, acceder a la información del equipo, tener privilegios de administrador para realizar cualquier tarea). Es un ataque de alto impacto ya que puede tomar todo el control de la máquina y adicionalmente acceder a privilegios restringidos para usuarios diferentes al propietario de la misma.

*Figura 33.* Explicación del ataque de escalada de privilegios realizado

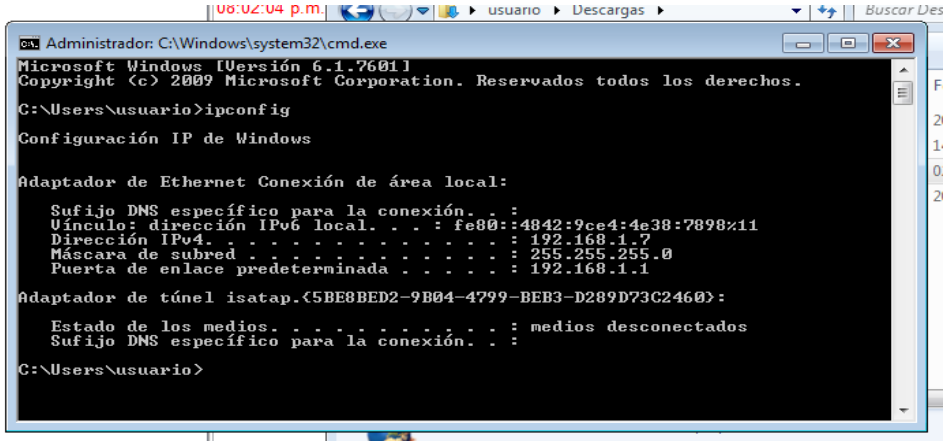



Fuente: Construcción propia autor

## 5.12. PASOS DE EJECUCIÓN PARA EXPLOTACIÓN DE VULNERABILIDAD

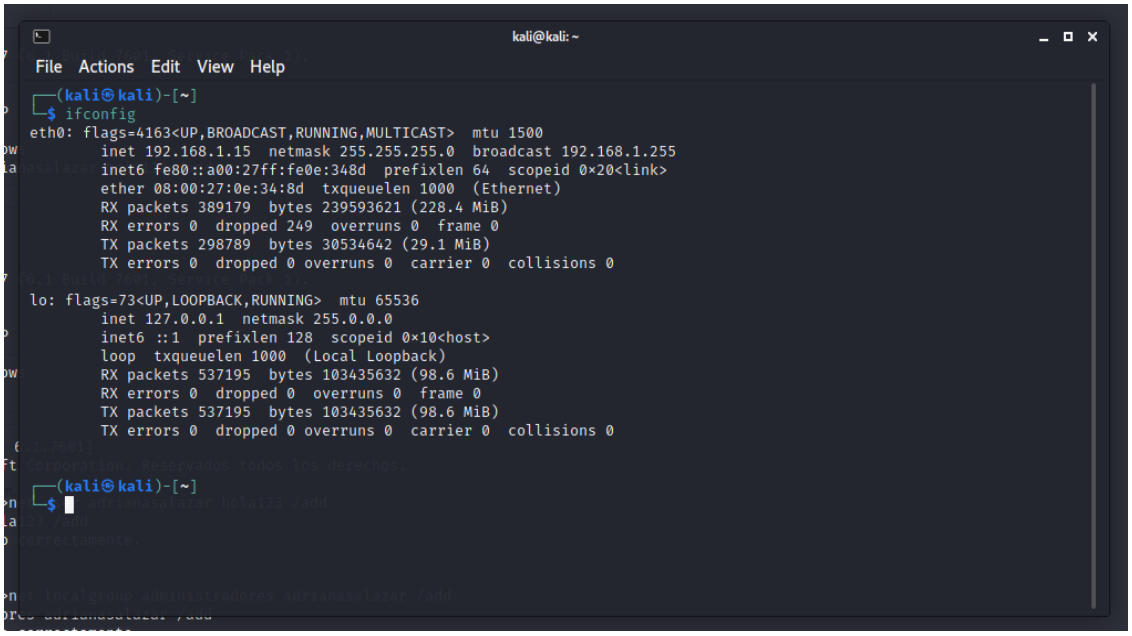
### 5.12.1. Configuración de red

*Figura 34.* Windows 7 X 64




Fuente: El autor

*Figura 35.* Kali Linux

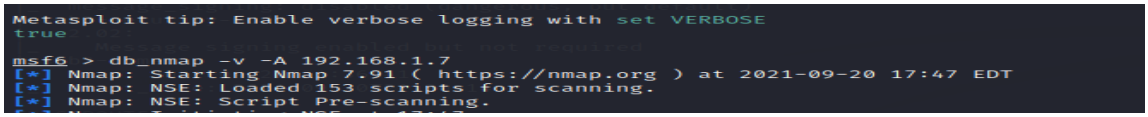



Fuente: El autor

### 5.12.2. Usando la herramienta metasploit

a. Utilización de nmap dentro de metasploit para identificar los puertos abiertos en la maquina atacada se realiza con el comando db_nmap –v –A 192.168.1.7

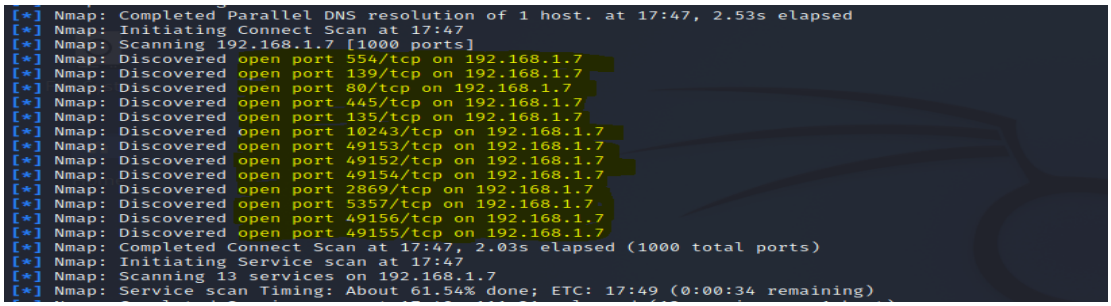
*Figura 36.* Nmap en metasploit db_nmap-v-A ip




Fuente: El autor

b. Como resultado se pueden identificar los puertos abiertos

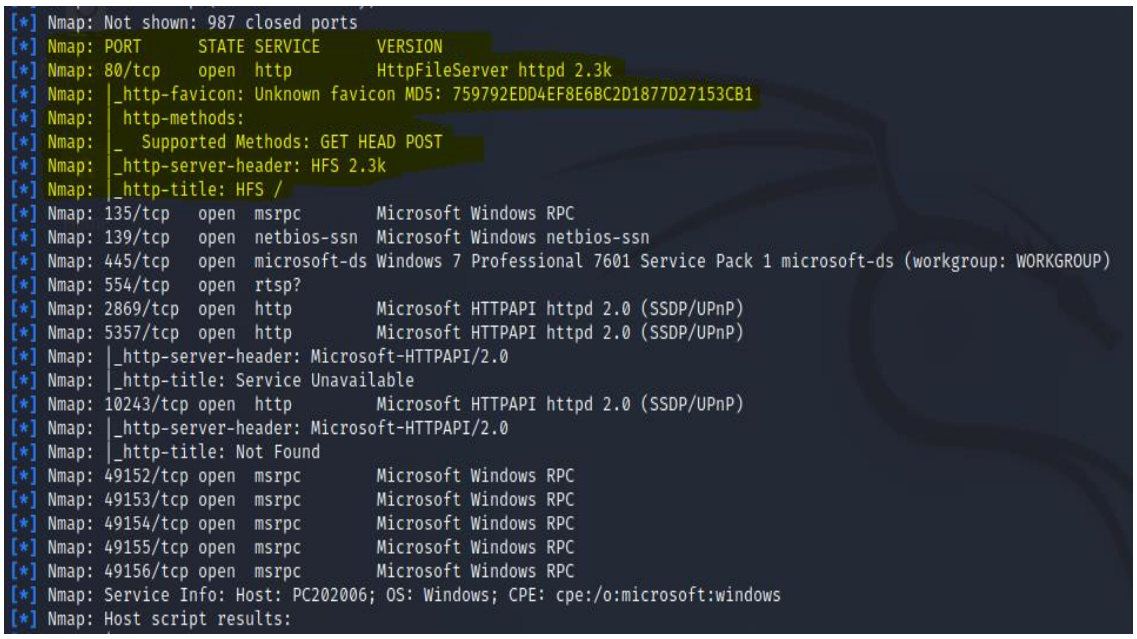
*Figura 37.* Identificación puertos abiertos nmap




Fuente: El autor

c. Se identifica el puerto abierto por el programa HTTP File server de rejetto, puerto 80.

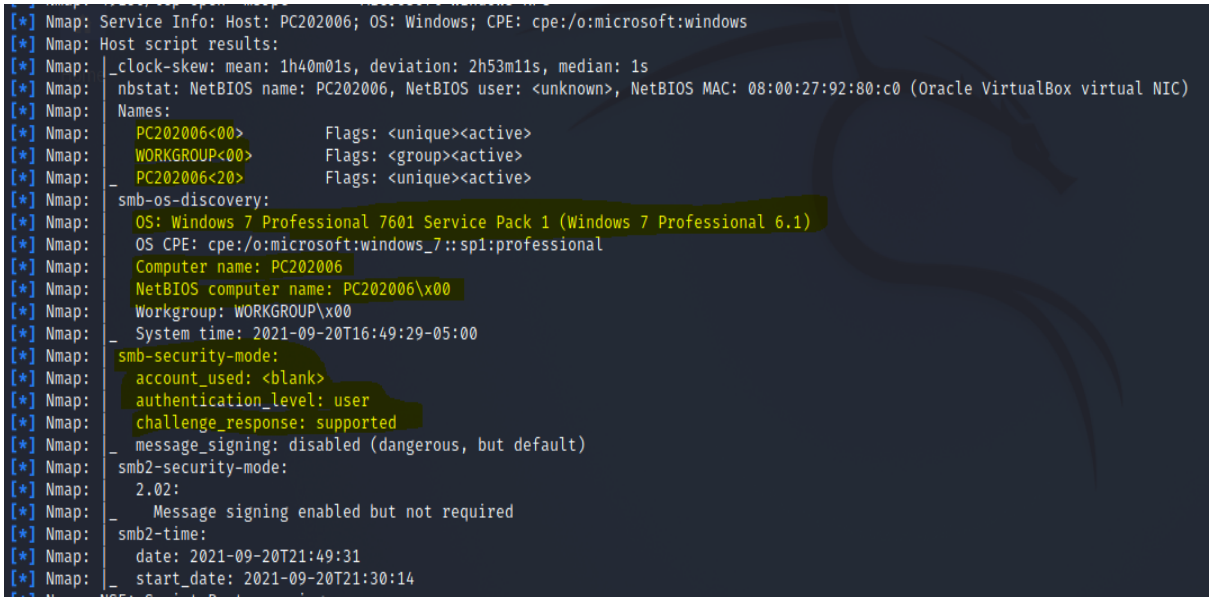
*Figura 38.* Identificación puertos 80, servicios y versiones




Fuente: El autor

d. Se identifica la información del PC atacado

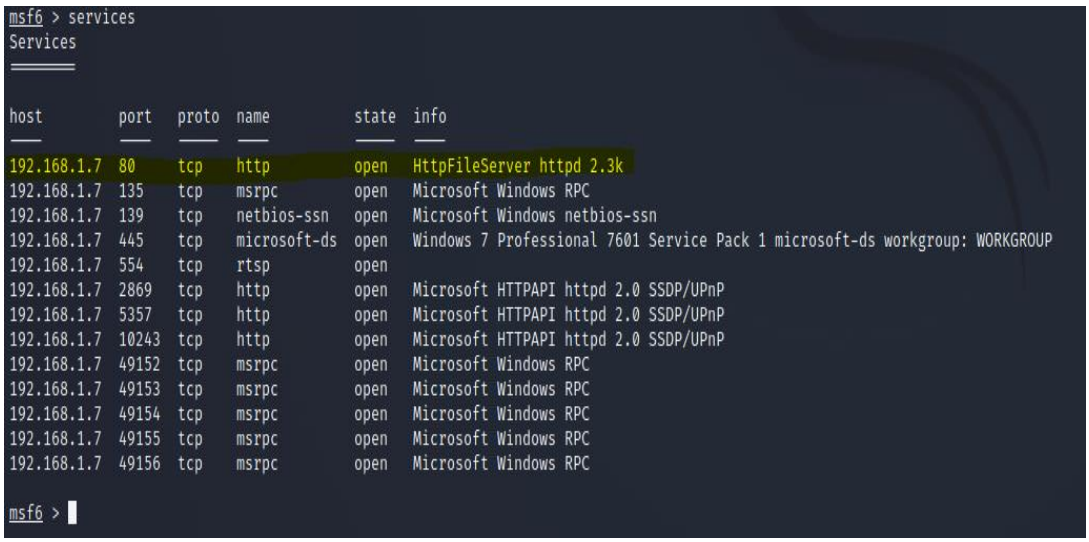
*Figura 39.* Identificación información PC atacado




Fuente: El autor

e. Con el comando services se identifica que el servicio del puerto 80 del programa Http File Server se encuentra activo

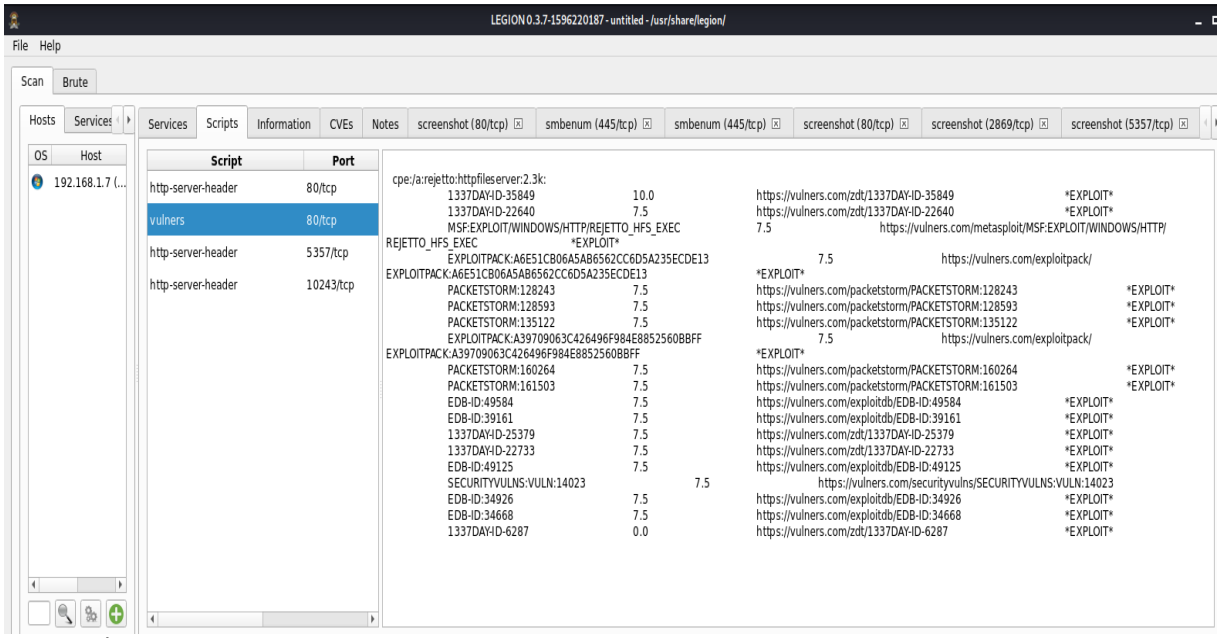
*Figura 40.* Comando services




Fuente: El autor

f. Validar información de las vulnerabilidades en el puerto 80 que genera el programa Http File Server con la herramienta Legion

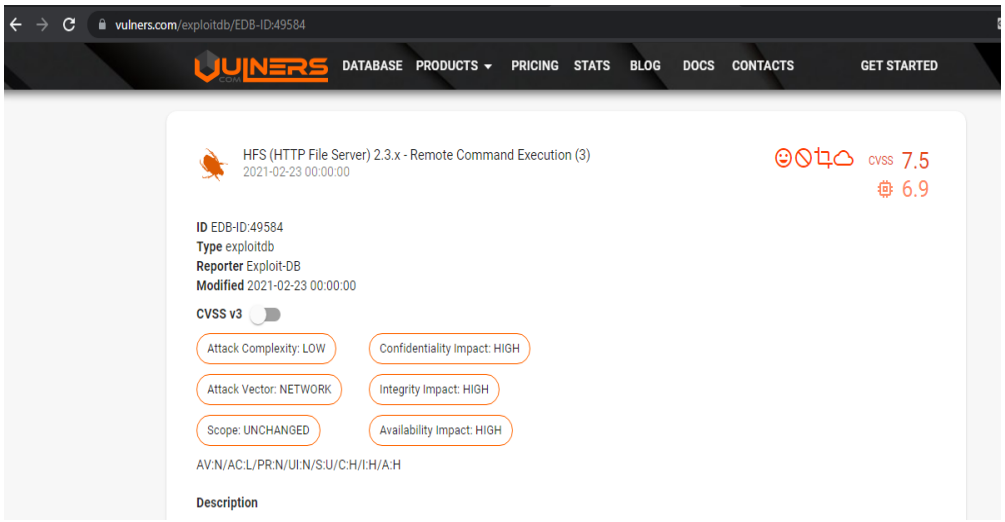
*Figura 41.* Consulta vulnerabilidades en Legion




Fuente: El autor

g. Se busca la información de la vulnerabilidad EDB-ID:49584 que aparece dentro de las vulnerabilidades arrojadas por legión

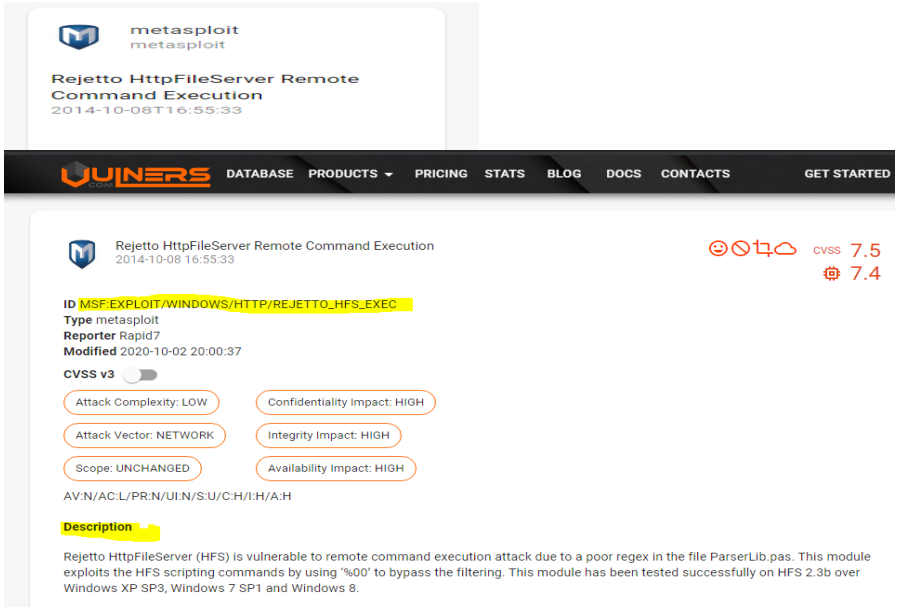
*Figura 42.* Información vulnerabilidad EDB-ID: 49584




Fuente: El autor

h. Información relacionada con la forma de explotar la vulnerabilidad en metasploit, comando a ejecutar en el módulo indicado.

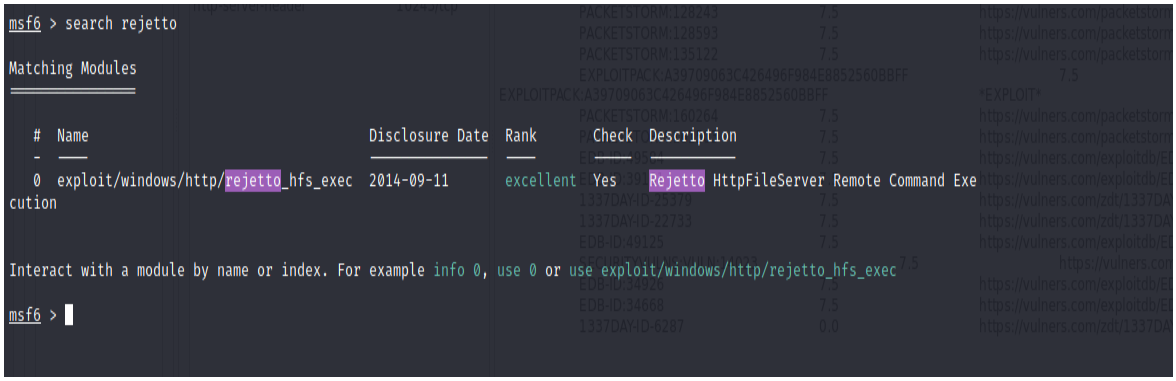
*Figura 43.* Indicación para explotar vulnerabilidad metasploit




Fuente: El autor

i. Se busca el módulo de metasploit para atacar las vulnerabilidades encontradas

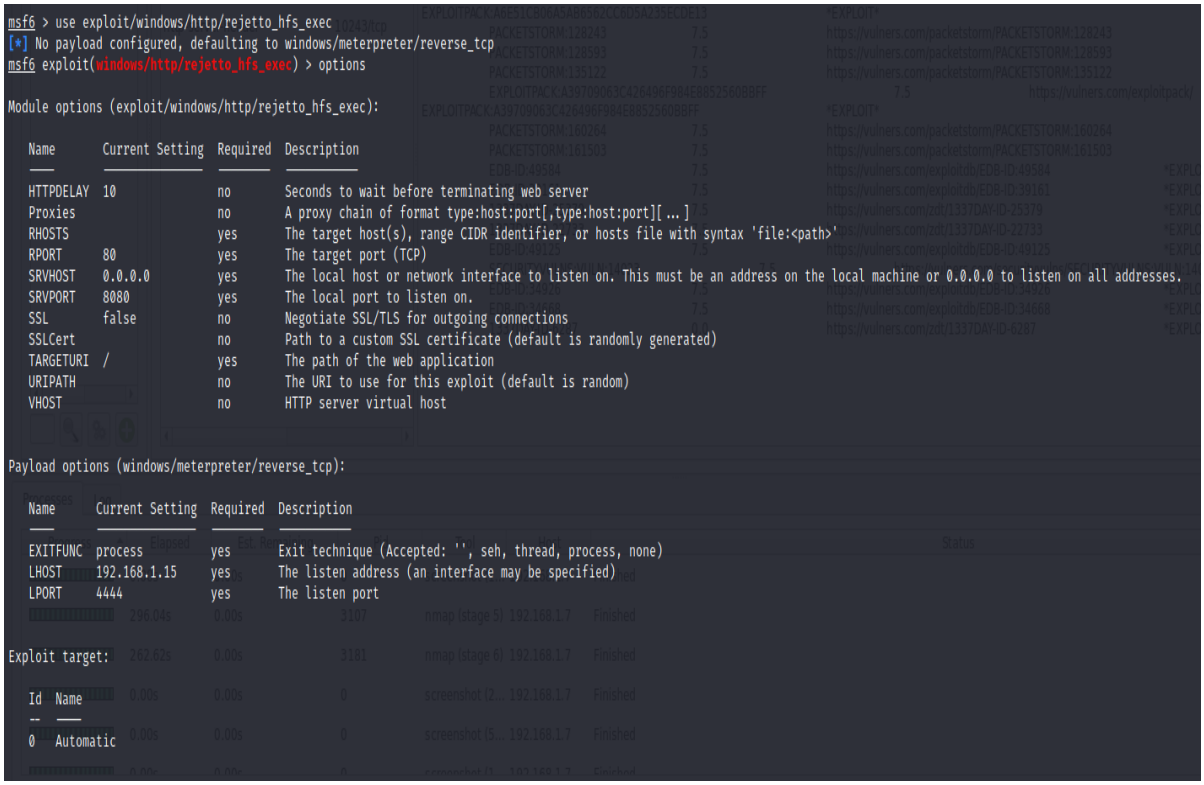
*Figura 44.* Módulo metasploit para el ataque




Fuente: El autor

j. Se carga y revisan las opciones del modulo con la información del exploit encontrada

*Figura 45.* Cargue opciones módulo exploit encotrado




Fuente: El autor

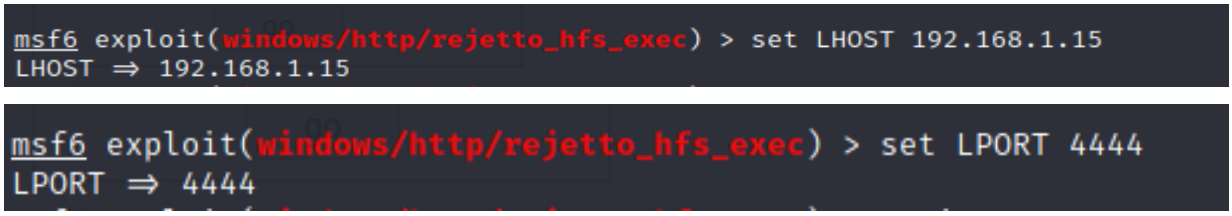
k. Iniciar las variables del equipo que va a ser atacado

*Figura 46.* Inicialización de variables equipo a atacar


Fuente: El autor

l. Se inician las variables del equipo atacante, se utiliza un puerto que no se esté utilizando para entablar la conexión con la máquina atacada

*Figura 47.* Inicialización variables equipo atacante




Fuente: El autor

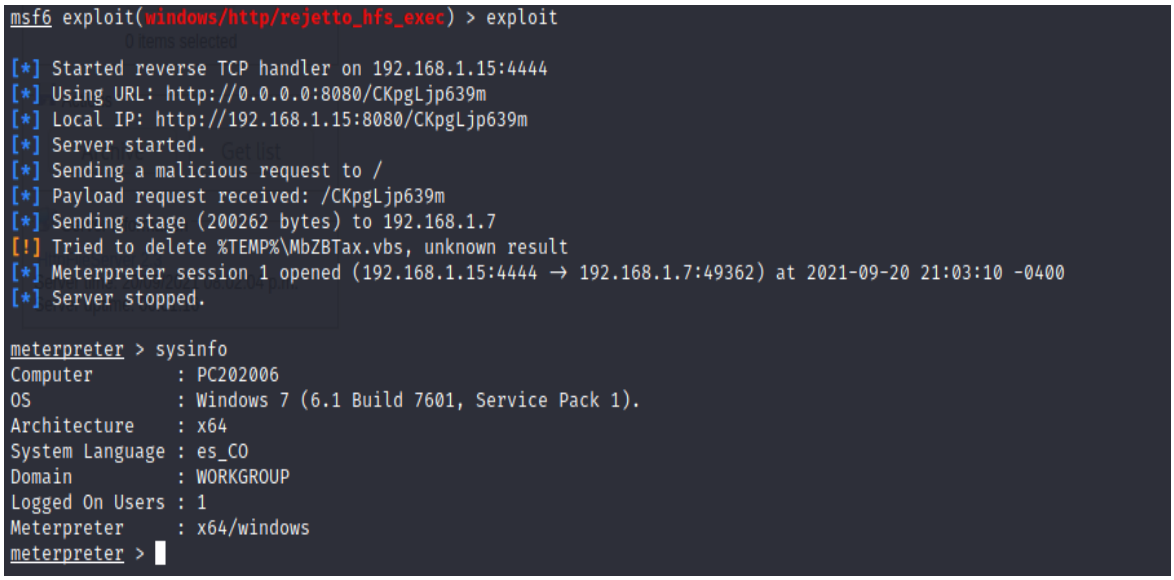
m. Las opciones del modulo cargadas se validan con la instrucción options

*Figura 48.* Instrucción options


Fuente: El autor

n. Se ejecuta la vulnerabilidad

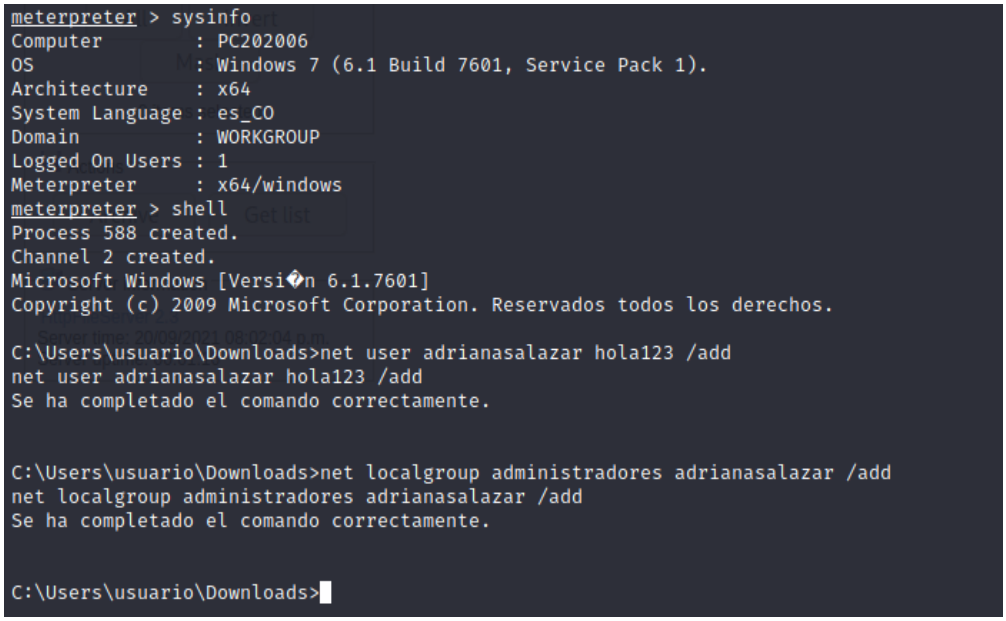
*Figura 49.* Ejecución de la vulnerabilidad




Fuente: El autor

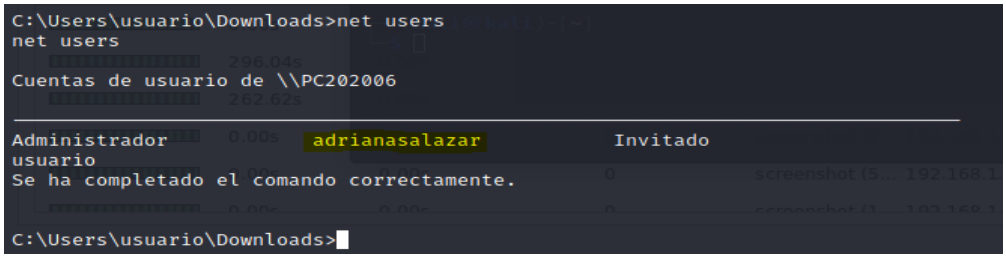
o. Se crea el usuario administrador, desde el meterpreter se ejecuta el comando Shell para abrir el cmd del equipo atacado.

*Figura 50.* Meterpreter creación usuario administrador




Fuente: El autor

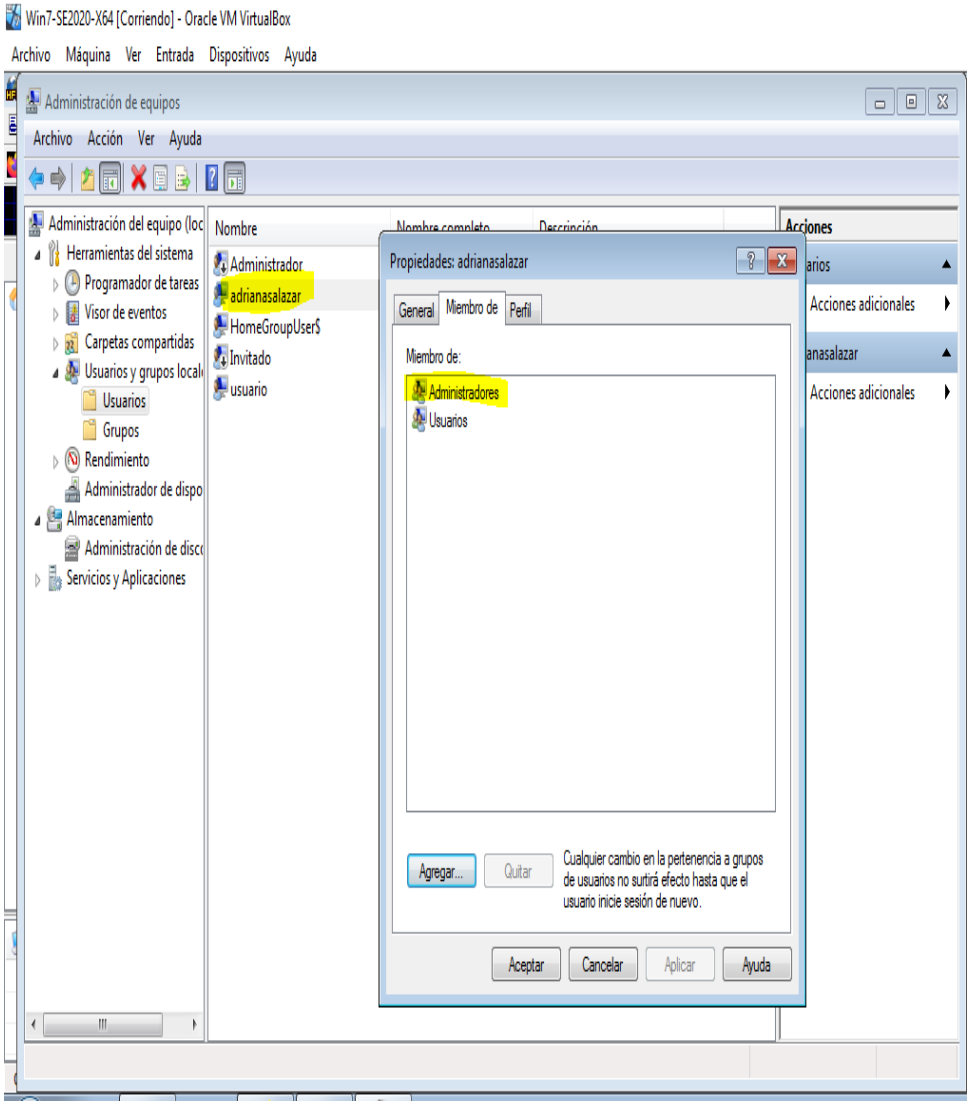
*Figura 51.* Meterpreter creación usuario administrador




Fuente: El autor

p. En el equipo atacado se puede ver la cuenta creada

*Figura 52.* Usuario creado en equipo atacado




Fuente: El autor

## 5.13. ACTIVIDADES E INDAGACIONES A REALIZAR EN CASO DE ENFRENTARSE A UN ATAQUE EN TIEMPO REAL - ARGUMENTOS TÉCNICOS.

De acuerdo al Instituto Nacional de Estándares y Tecnología NIST[3] en su guía de manejo de incidentes, establece que con frecuencia las violaciones de seguridad ponen en juego información personal y comercial por lo cual es prioritario tener opciones de respuestas rápidas y eficientes durante la identificación de estos ataques. De este tipo de situaciones nace la necesidad de tener establecidos procedimientos de respuesta a incidentes de seguridad; es decir: una metodología que permita de forma sistémica responder y manejar los incidentes en forma consistente para tomar las decisiones y acciones que más se apropien a los tipos de eventos enfrentados. Está práctica ayuda a minimizar las perdidas, robo de información y la interrupción de servicios que se pueden ocasionar por los incidentes; también trae como beneficio la capacidad de valerse de la información que se obtiene durante el manejo del incidente para utilizar posteriormente en el manejo de los mismos. Teniendo en cuenta lo anterior es fundamental dentro de los procedimientos de tratamiento de incidentes de seguridad definir una estrategia que facilite la toma de decisiones de forma oportuna de manera que evite la propagación y disminuya daños de los recursos de TI y afectación en la integridad, confidencialidad o disponibilidad de la información.

*Figura 53.* Estrategia de contención de incidentes

| Incidente | Detección | Contención |
|---|---|---|
| Acceso no autorizado | Sucesivos intentos fallidos de login | Bloqueo de cuenta |
| Código Malicioso | Infección con virus | Desconexión de la red del equipo afectado |
| Acceso no autorizado | Compromiso del Root | Apagado del sistema |
| Reconocimiento | Scanning de puertos | Incorporación de reglas de filtrado en el firewall |

Fuente: El autor, basado en Seguridad y privacidad de la Información: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la información. MINTIC.2018. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf. Pg. 21.

3 *Computer SecurityIncident Handling Guide: Recommendations of the National Institute of Standards and Technology.* National Institute of Standards and Technology (NIST). U.S. Department of Commerce.2012. Special Publication 800-61 Revisión 2. Pg. 6.

Estas estrategias para contener las incidencias pueden ser variables y se deben documentar para apoyar la gestión eficaz y rápida de las decisiones; los aspectos que se pueden tener como base pueden ser: potencial daño o robo de los activos, disponibilidad de servicio, tiempo y recursos para la ejecución de estrategias, duración y efectividad del procedimiento, entre otros.

Después de lograr contener el ataque se debe proceder a erradicar y recuperar; esta fase consiste en la eliminación de rastros del incidente y proceder a la recuperación por medio de restituir los sistemas o servicios afectados, restableciendo las funcionalidades en los sistemas que tuvieron algún impacto y efectuar la securización de los sistemas que prevenga incidentes parecidos en el futuro.

*Figura 54.* Estrategia de erradicación y recuperación

| Incidente | Detección | Erradicación | Recuperación |
|---|---|---|---|
| DoS (denegación de servicio) | SYN Flood | Restitución del servicio caído | Restitución del servicio caído |
| Virus | Gusano en la red | Corrección de efectos producidos. Restauración de backups | Corrección de efectos producidos. Restauración de |
| Vandalismo | Defacement a un sitio web | Reparar el sitio web | Reparar el sitio web |
| Intrusión | Instalación de un rootkit | Reinstalación del equipo y recuperación de datos | Reinstalación del equipo y recuperación de datos |

Fuente: El autor, basado en Seguridad y privacidad de la Información: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la información. MINTIC.2018. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf. Pg. 21.

Para algunos casos en estas fases de respuesta a incidentes, como son: contención, erradicación y recuperación, cuando la afectación es a sistemas críticos de la organización puede activarse el BCP – Plan de continuidad del negocio o DRP –Plan de recuperación de desastres.

## 5.14. DESDE EL EJERCICIO DE RED TEAM – MEDIDAS DE HARDENIZACIÓN PROPUESTAS PARA MITIGAR LA OCURRENCIA FUTURA DE ESTE ATAQUE.

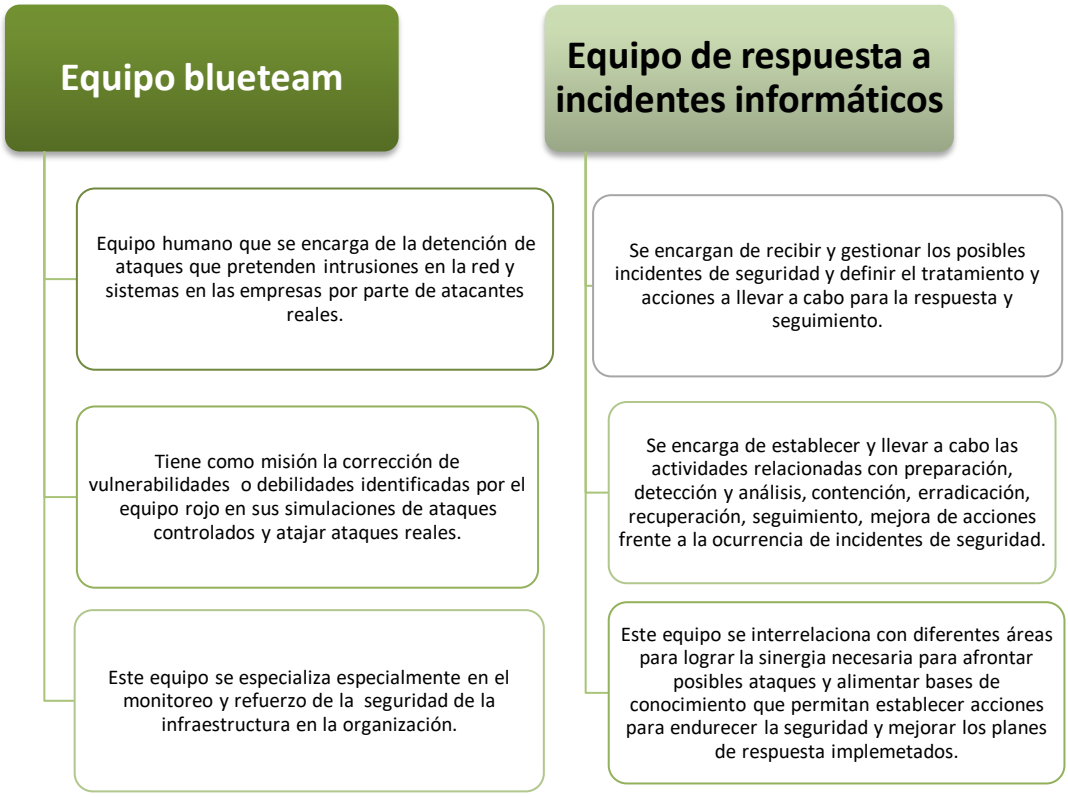
Para mitigar la ocurrencia del ataque presentado desde el ejercicio de red team, las medidas para securizar la infraestructura y evitar la ocurrencia en ocasiones futuras de esta situación, se presentan las siguientes recomendaciones:

- Verificar la necesidad de apertura de puertos existentes en la infraestructura tecnológica garantizando únicamente los servicios necesarios para la funcionalidad requerida en los equipos específicos.
- Habilitar la funcionalidad del rejetto en un puerto diferente al que viene por defecto establecido, preferiblemente arriba del puerto 4000.
- Utilizar el software siempre actualizado en la última versión, para este caso si se requiere el software rejetto, instalar versiones actualizadas en las cuales se hayan remediado las vulnerabilidades conocidas; esta aplicación tiene solucionada la vulnerabilidad explotada a partir de la versión 2.3b.
- Limitar la descarga e instalación de programas únicamente al personal administrador, de tal manera que los usuarios finales no tengan este tipo de privilegios y se garantice por parte del área de TI la instalación de aplicaciones confiables y controles compensatorios para excepciones que se presenten.
- Verificar periódicamente los usuarios existentes frente a los funcionarios vigentes, roles y perfiles asignados de acuerdo a las funciones de los cargos.
- Establecer una matriz de segregación de responsabilidades en donde se garantice que los usuarios administradores solo van a ser asignados al personal idóneo.
- Establecer procedimientos de creación y des habilitación de usuarios.
- Mantener las herramientas de seguridad activas y actualizadas como antivirus y firewall en todos loe equipo disponibles en la red.
- Limitar accesos a servicios de red
- Inhabilitar servicios que no se utilizan o son innecesarios en los equipos de red.
- Modificar el procedimiento de banner predefinido en los equipos para ocultar información como versiones; esta información se puede personaliza de tal manera

que se eliminen anuncios e información que puede ser de utilidad para los atacantes.

## 5.15. DIFERENCIAS ENTRE EQUIPO BLUE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

*Figura 55.* Diferencias equipo blueteam y equipo de respuesta a incidentes




*Fuente: Construcción propia autor*

## 5.16. FUNCIONES DEL CIS "CENTER FOR INTERNET SECURITY" DENTRO DEL EQUIPO DE BLUETEAM

El equipo de blueteam puede apoyarse enormemente con las herramientas que proporciona el CIS, dentro de este equipo esta herramienta se puede utilizar para:

- Consulta y actualización en línea de las mejores prácticas de seguridad recomendadas por expertos a nivel del mundo.

- Los CIS Controls pueden proporcionar guías para complementar y mapear la seguridad protegiendo la entidad de posibles ataques cibernéticos.
- Con los CIS Benchmarks se obtiene información de la configuración de seguridad para diferentes productos de proveedores de sistemas TI que pueden ser aplicadas a los dispositivos que forman parte de la infraestructura organizacional.
- Si la empresa cuenta con presupuesto, se puede adquirir una membrecía CIS SecureSuite que proporciona recursos y herramientas diseñadas con pautas referentes a CIS y CIS Controls.
- MS-ISAC permite tener acceso a instrumentos útiles para prevención, protección, respuesta y recuperación ante posibles amenazas identificadas; este producto se enfoca principalmente hacia organizaciones gubernamentales.

## 5.17. FUNCIONES Y CARACTERISTICAS PRINCIPALES DE UN SIEM

- Este sistema para gestionar eventos e información de seguridad se conoce como una solución central que engloba y centra toda gestión de seguridad y eventos; esta tecnología suministra análisis en línea frente a las alertas de seguridad que generan diferentes dispositivos tanto de software como de hardware dentro de la red.
- Dentro de la recolección de registros de actividades o logs de los distintos dispositivos identifica situaciones de seguridad o actividades inesperadas, atípicas o sospechosas que pueden representar el inicio de un incidente y eliminando resultados extraños o falsos positivos y entregando respuestas de acuerdo a informes y evaluaciones registradas.
- Permite visualizar fácilmente el estatus de todos los mecanismos de seguridad implementados, lo cual es útil para los administradores de los sistemas de información.
- Con la combinación de las funciones que enrolan el manejo de información de seguridad recopilando los registros de sucesos a largo plazo para enriquecer la exploración y notificación de datos de seguridad y el sistema de tratamiento de

situaciones relacionadas con la seguridad que se encarga de correlacionar eventos, notificarlos y revisarlos en tiempo real.

- Sistematización de actividades o tareas.
- Respuesta de forma automática de amenazas y eventos.
- Eficiencia en la identificación de ataques.
- Gestión de evidencia rápida para la realización de análisis forense.
- Seguimiento a diferentes eventos.
- Optimización en el manejo y tratamiento de riesgos.
- Implementación y manejo de métricas de seguridad.
- Evaluación de debilidades o vulnerabilidades.
- Monitoreo de comportamientos.
- Identificación de violaciones de seguridad
- Documentación de registros de auditoría con eventos identificados y resolución.
- Escalamiento al analista o administrador de eventos depurados para gestionar acciones y tomar decisiones.

## 5.18. HERRAMIENTAS DE CONTENCIÓN DE ATAQUES

**Cisco FireSIGHT** : Es un escáner de actividad en red, posee sensores con inteligencias de actualización constante con las últimas alertas que permiten realizar en los sistemas de la empresa búsquedas relacionadas con códigos prohibidos o maliciosos con base en políticas de seguridad preestablecidas. Esta herramienta también tiene módulos de monitoreo de la conexión de usuarios y equipos para identificar la conexión a dominios comprometidos como bonets. Estos sensores al detectar actividades no consentidas notifican a la consola y al motor de servicios de identidad (ISE) que se encarga de alertar a herramientas de seguridad de la red sobre posible actividad sospechosa. En este punto y de acuerdo a las políticas implementadas la solución Cisco TrustSec se encarga de aislar dispositivos sospechosos en caso de compromiso incluyéndolos en la opción de cuarentena o red virtual, restricción del equipo para accesos a la red, aplicaciones y datos.

**Symantec Advanced Threat Protection (ATP):** Esta solución tiene la posibilidad de detectar y contener las amenazas por medio de puntos de control que se comunican a una única consola en donde se puede realizar la correlación de actividad sospechosa en los puntos de control, priorizando situaciones que pueden presentar mayores riesgos para la compañía. Cuando se identifican amenazas críticas se contienen rápidamente y las instancias se bloquean. La herramienta correlaciona acciones posiblemente sospechosa en todos los puestos de inspección y da prelación a los sucesos que pueden representar niveles altos de riesgo para la compañía. Tan pronto se identifican las amenazas con mayor criticidad se procede a contenerlas rápidamente posibilitando el bloqueo a nuevas. Esta herramienta tiene posibilidad de identificar diferentes amenazas como ataques de día cero, o APT por medio de los puntos de control en la red, correo electrónico, endpoints haciendo detecciones cruzadas entre puntos de control y búsquedas en los entornos. Con los datos globales correlacionados y funciones de telemetría este sistema permite priorizar por importancia y contener los endpoints y bloquear instancias en puntos de control.

**Anti-Spam:** Este sistema permite filtrar los mensajes de correo electrónico, el filtrado se puede realizar tanto para correos entrantes como salientes, algunos además de filtrado de contenido tienen escaneo de malware y restricciones en los tipos de archivos. Tiene la posibilidad de definir reglas para reenviar, poner en cuarentena, estacionar, limpiar, bloquear o eliminar cualquier información que pase por los servidores de acuerdo a los análisis. Las funcionalidades incluyen filtrado de contenido en datos enviados desde los correos corporativos que pueden prevenir temas de litigios o fuga de información. Tiene un sistema de listas negras y listas blancas que permite validar los remitentes de correos entrantes y se pueden definir distintas políticas dentro de sus reglas de configuración.

## RECOMENDACIONES

Para mitigar la ocurrencia de ataques dentro de la infraestructura tecnológica de las organizaciones es necesario plantear estrategias que permitan prevenir, identificar, responder, mitigar, asegurar y hacer seguimiento a los aspectos relacionados con la seguridad en las compañías, algunas de las recomendaciones a tener en cuenta:

- Evaluar de acuerdo al tamaño de la organización, volúmenes de información, análisis de riesgos previos, incidentes de seguridad; la implementación y reclutamiento de expertos especialistas que conformen los equipos redteam y blueteam que le aporten la cuota de seguridad necesaria a la infraestructura de la organización.
- Es un punto fundamental para la organización que los equipos de defensa blueteam y redteam se interrelacionen y tengan una comunicación fluida, esto puede asegurar ejercicios de prueba exitosos y el aseguramiento frecuente de las plataformas.
- Los equipos blueteam deben actualizarse frecuentemente sobre las herramientas que pueden apoyar el aseguramiento de los sistemas y compartir la información con el redteam para la realización de pruebas de ataque; de igual manera el redteam debe actualizarse frente a las amenazas emergentes para cooperar con el blueteam en temas de prevención.
- Establecer políticas de seguridad conocidas y aprobadas por la alta dirección que faciliten el conocimiento por parte de los empleados frente a las buenas prácticas y mitiguen de cierta forma la ocurrencia de incidentes de seguridad.
- Verificar la necesidad de apertura de puertos existentes en la infraestructura tecnológica garantizando únicamente los servicios necesarios para la funcionalidad requerida en los equipos específicos.
- Cambio de puertos comunes vulnerables según la aplicación que se utilice.
- Utilizar el software siempre actualizado en la última versión.

- Implementar controles de detección, prevención y recuperación para protección contra códigos maliciosos; adicionalmente realizar capacitaciones dirigidas a los empleados respecto a las amenazas que se pueden presentar como robo de identidad, virus, spyware, hackers, phishing, entre otros.
- Verificar que los registros de eventos estén activos para todos los roles dentro de la organización de manera que se puedan validar y monitorear con regularidad.
- Restringir la instalación de software a usuarios finales, solo los administradores deben tener estos privilegios.
- Limitar la descarga e instalación de programas únicamente al personal administrador, de tal manera que los usuarios finales no tengan este tipo de privilegios y se garantice por parte del área de TI la instalación de aplicaciones confiables y controles compensatorios para excepciones que se presenten.
- Verificar periódicamente los usuarios existentes frente a los funcionarios vigentes, roles y perfiles asignados de acuerdo a las funciones de los cargos.
- Establecer una matriz de segregación de responsabilidades en donde se garantice que los usuarios administradores solo van a ser asignados al personal idóneo.
- Establecer procedimientos de creación y des habilitación de usuarios.
- Mantener las herramientas de seguridad activas y actualizadas como antivirus y firewall en todos loe equipo disponibles en la red.
- Limitar accesos a servicios de red.
- Inhabilitar servicios que no se utilizan o son innecesarios en los equipos de red.
- Modificar el procedimiento de banner predefinido en los equipos para ocultar información como versiones; esta información se puede personaliza de tal manera que se eliminen anuncios e información que puede ser de utilidad para los atacantes.
- Los documentos utilizados por la organización deben estar avalados por abogados especializados que garanticen la concordancia y afinidad con la ética, normatividad y legislación vigente de manera que no valla en contradicción y vulnere ninguno de estos aspectos.

## CONCLUSIONES

- Los equipos redteam y blueteam le aportan a la organización tranquilidad, mejora continúa en la seguridad, seguimiento constante con análisis de patrones y comportamientos que pueden identificar posibles amenazas, emulación de posibles ataques que pueden ayudar a identificar la capacidad que tienen las organizaciones para proteger sus activos críticos.
- La realización de Pentesting es una práctica que si se evalúa a largo plazo puede resultar económica teniendo en cuenta el sin número de herramientas de código abierto y publicaciones de entidades idóneas y conocedoras creadas para la cooperación mundial en la mitigación de riesgos de ataques, que se pueden utilizar de manera frecuente, gratuita y periódica para la actualización y generación de estrategias de defensa en las organizaciones.
- Los profesionales de la seguridad informática tenemos altos niveles de responsabilidad frente a la continua actualización de conocimientos que debemos realizar para estar a la vanguardia de las amenazas, herramientas para el apoyo de cierre de brechas de seguridad y el aporte que como individuos podemos realizar con nuestro trabajo ético y en concordancia con la normatividad y legislación vigente frente al trabajo que se nos encomiende.
- Los aspectos de la seguridad informática no son de ninguna manera estáticos, contrariamente día a día traen consigo retos importantes frente a la solución de la vulnerabilidades de las tecnologías, identificación de vectores de ataque y amenazas emergentes, actualización de herramientas para la identificación y mitigación de posibles incidentes de seguridad, entre otros; de ahí la importancia de la constante actualización por parte de los equipos expertos que manejan la seguridad informática en las empresas para garantizar el adecuado tratamiento, aseguramiento y seguimiento de manera que limite y mitigue la ocurrencia de eventos adversos que afecten la seguridad en la organización.

## BIBLIOGRAFÍA


ADALID. Anexo técnico. Buenas prácticas y marco normativo de la seguridad digital. Security, Legal and Forensic Corporation. [Sitio web]. [Consulta: 25 de agosto de 2021].Disponible en: https://tic.bogota.gov.co/sites/default/files/seguridad-de-la-informacion/Buenas_practicas_marco_normativo_0.pdf

ALCALDÍA DE BOGOTÁ. Guardianes de la información Penetration Testing. [Sitio web]. [Consulta: 25 de agosto de 2021]. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

CIS SECURITY. CIS Center for Internet Security. [Sitio web]. [Consulta: 28 de septiembre de 2021]. Disponible en: https://www.cisecurity.org/

*Computer SecurityIncident Handling Guide: Recommendations of the National Institute of Standards and Technology.* National Institute of Standards and Technology (NIST). U.S. Department of Commerce. 2012. Special Publication 800-61 Revisión 2

CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [Sitio web]. [Consulta: 08 de septiembre de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COPNIA. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. 2015. (pp. 3-26). [Sitio web]. [Consultado: 10 de septiembre de 2021]. Disponible en:https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE. About CVE. . [Sitio web]. [Consulta: 29 de agosto de 2021]. Disponible en: https://cve.mitre.org/about/index.html

DATACOM. Global. Cisco FireSight, solución de Contención Rápida de Amenazas Cisco. [Sitio web]. [Consulta: 29 de septiembre de 2021]. Disponible en: https://datacom.global/cisco-seguridad-deteccion-de-amenazas-en-las-organizaciones/

DEBCO TECH. Your comunication system. [Sitio web]. Houston. DEBCO TECH. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.dtsecurity.net/enterprise-communications.html

EL TIEMPO. [Sitio web]. [Consulta: 12 de septiembre de 2021]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

ENTER.CO. Detrás de buggly: la historia de la fachada Andrómeda. [Sitio web]. [Consultado: 11 de septiembre de 2021]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

EXPLOIT DATABASE. [Sitio web]. [Consulta: 29 de agosto de 2021]. Disponible en: https://www.exploit-db.com/

*Guidelines on Electronic Mail Security: Recommendations of the National Institute of Standards and Technology.* National Institute of Standards and Technology (NIST). U.S. Department of Commerce. 2007. Special Publication 800-45 Versión 2

INCIBE. Glosario de términos de Ciberseguridad. Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad. [Sitio web]. [Consulta: 26 de septiembre de 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

INCIBE. ¿Qué son y para qué sirven los SIEM, IDS e IPS? Instituto Nacional de Ciberseguridad. [Sitio web]. [Consulta: 26 de septiembre de 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

LA WEB. La web y sus fundamentos completos. [Sitio web]. [Consultado: 11 de septiembre de 2021]. Disponible en: https://sites.google.com/site/lawedysusfundamentoscompleto/

MINTIC. Ley 1581 [LEY_1581_2012]. Mintic. (2012). (pp. 1-11). [Sitio web]. [Consultado: 11 de septiembre de 2021]. Disponible en: https://www.mintic.gov.co/arquitecturati/630/articles-9011_documento.pdf

PCT LTDA. Casa de Software. "Soluciones informáticas para el sector público. Bogotá. [Sitio web]. [Consulta: 26 de septiembre de 2021]. Disponible en: http://www.pctltda.com/web/

RAPID 7 METASPLOIT. Metasploit the world's most used penetration testing framework. [Sitio web]. [Consulta: 29 de agosto de 2021]. Disponible en: https://www.metasploit.com/

Seguridad y privacidad de la Información: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la información. [Sitio web] Ministerio de Tecnologías de la Información y las Comunicaciones.2018. [Fecha de consulta: 27 de septiembre de 2021].Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

SYMANTEC. Symantec presenta la nueva era de Advanced Threat Protection. [Sitio web]. [Consulta: 29 de septiembre de 2021]. Disponible en: https://www.interempresas.net/Ciberseguridad/Articulos/175545-Symantec-presenta-la-nueva-era-de-Advanced-Threat-Protection.html

Rejetto http file server hasta 2.x parserlib.pas findmacromarker escalada privilegios. [Sitio web]. [Fecha de consulta: 27 de septiembre de 2021]. Disponible en: https://vuldb.com/es/?id.71861

## ANEXO 1. LINK DEL VIDEO DE SUSTENTACIÓN DEL SEMINARIO

https://youtu.be/h8PWnGGly1w

## ANEXO 2. EVIDENCIA DE TURNITIN 2%

| | Título de la Entrega | Identificador del trabajo de Turnitin | Entregado | Similitud | Calificación | Nota general |
|---|---|---|---|---|---|---|
| Ver recibo digital | final | 1670256231 | 10/10/2021 16:17 | 2% | N/A | -- |