Capacidades Técnicas, Legales Y De Gestión Para Equipos Blue Team Y Red Team.

Cristhian Giovanny Morales Real

Asesor:
Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias Basicas, Tecnologia E Ingenieria - ECBTI

Especialización En Seguridad Informática

Bogotá

2025

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ATAQUE CIBERNÉTICO: cualquier intento sin consentimiento previo de exponer deshabilitar, alterar, destruir, robar u obtener acceso a cualquier tipo de información sin importar el dispositivo o plataforma que la custodie.

BLUE TEAM: equipo de seguridad encargado de proteger de manera activa los Ataques cibernéticos. Realizan un monitoreo frecuente, realizando análisis de patrones y comportamientos que se salen de lo habitual, tanto a nivel de aplicaciones y sistemas, como también de las personas, en lo relacionado a la seguridad de la información.

KALI LINUX: distribución de Linux cuyo objetivo principal es la de auditoría de sistemas informáticos.

PENTESTING: ejercicio de ataque sobre un sistema informático, con el objetivo de hallar vulnerabilidades de seguridad y tener acceso a ellas.

RED TEAM: equipo encargado de simular a los atacantes, dando uso herramientas similares o las mismas que la de los atacantes, con el objetivo de explotar las vulnerabilidades de seguridad informática, dando así las bases de información al equipo de blue team, para que este pueda saber cómo defenderse ante eventuales ataques.

RIESGO: incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los activos de información o a la información propiamente.

VULNERABILIDAD: debilidad o falencia que presenta un sistema de información, y que pone en riesgo los activos de información y a la información misma de las compañías, admitiendo que un atacante afecte la integridad, disponibilidad o confidencialidad de esta.

RESUMEN

En el presente documento se relacionará un informe en donde se darán a conocer estrategias técnicas con actividades propuestas durante el desarrollo del seminario especializado en seguridad informática, con experiencias de equipos de seguridad Red Team & Blue Team, mediante un ambiente controlado y una serie de situaciones de estudio, enfocados en la seguridad de la información.

Palabras clave: Blue Team, Red Team, seguridad de la información, vulnerabilidad.

1. INTRODUCCIÓN

A través de los hallazgos suministrados por los equipos Red Team y Blue Team, se puede establecer el impacto en cada incidente de seguridad sobre activos de información, donde a través de la socialización de las herramientas utilizadas por el equipo Red Team en los ambientes de pruebas controlados, se indica la viabilidad y necesidad de mitigar el impacto sobre los riesgos de seguridad encontrados, ya que se establece los puntos críticos y niveles de criticidad de la vulnerabilidad, para así establecer controles efectivos y planes de trabajo para el resguardo de los datos. Apalancados por variadas fuentes bibliográficas, se logra mantener una actualización constante de las vulnerabilidades más conocidas en los sistemas de información, sistema operativo, aplicativos, etc., donde a través de estos referentes, se puede certificar y garantizar una mitigación, como también la remediación de vulnerabilidades, evitando riesgos potenciales, y protegiendo el activo más importante de las compañías que es la información.

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

De acuerdo con el último informe presentado por la Fiscalía General de la Nación, Colombia sufrió 12.000 millones de intentos de ciberataques en 2023. El uso de nuevas tecnologías en las organizaciones está cada vez más presente, y por ello cada vez se está más vulnerable a ataques cibernéticos que buscan vulnerar el activo más importante que es la información.

2.2 FORMULACIÓN DEL PROBLEMA

¿A través de un informe técnico con los enfoques de Red Team y Blue Team se pueden atender las falencias en seguridad y mejorar los niveles de protección de los activos de información en la organización CyberFort Technologies?

Lo veremos a continuación.

3. OBJETIVOS

4.1 OBJETIVOS GENERAL

Construir un informe técnico mediante los enfoques de Red Team y Blue Team, con el fin de mejorar los niveles de protección de los activos de información de la organización de estudio.

4.2 OBJETIVOS ESPECÍFICOS

Realizar un diagnóstico del estado actual respecto a medidas de seguridad de la información y definir el grupo de herramientas de seguridad adecuadas para emplear en procesos de prevención y contención frente a amenazas informáticas.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión de Blue Team y Red Team, apoyados con la herramienta Kali Linux.

Describir de manera detallada a través del informe técnico las estrategias de Red Team y Blue Team implementados, mediante técnicas de pentesting.

5 DESARROLLO DEL INFORME

5.1 HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS POR EL EQUIPO RED TEAM PARA EL ANÁLISIS Y EXPLOTACIÓN DE LAS VULNERABILIDADES EN EL ESCENARIO PROPUESTO.

Para el desarrollo de este ejercicio se procedió de la siguiente forma, así:

RECONOCIMIENTO

Para esta fase, desde la maquina Kali Linux que se encuentra dentro de la misma red, ejecutamos el comando Netdiscover que nos permitirá reconocer direcciones activas y pasivas. Se usa para descubrir hosts conectados en un segmento de red.

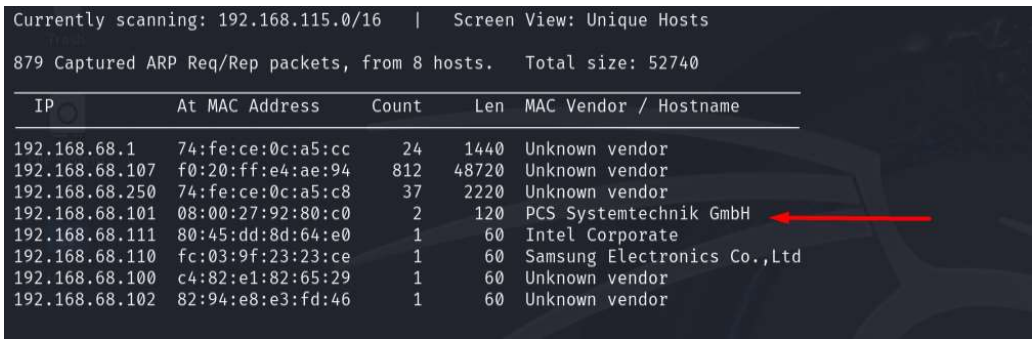

Figura 1 Mapeo de direcciones en segmento de red

Verificamos y coincide con nuestra dirección IP y MAC de la maquina Windows objetivo. Se trató de un reconocimiento pasivo al no tener contacto con el objetivo.

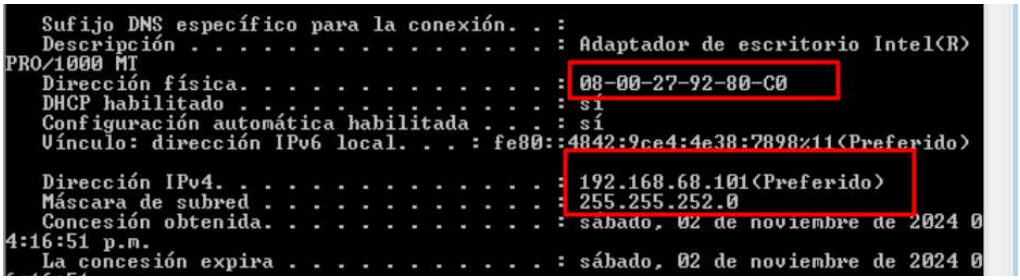

Figura 2 Configuración de tarjeta de red maquina Windows

ESCANEO

Con el uso de la herramienta Nmap, ejecutamos el comando nmap -sV, que nos permitirá detectar versiones en los puertos especificados de la maquina objetivo:

Figura 3 Verificación estado de puertos

También podemos obtener más información con el comando nmap -A que nos permite capturar información avanzada del host objetivo, como lo son el sistema operativo y de igual manera los puertos expuestos:

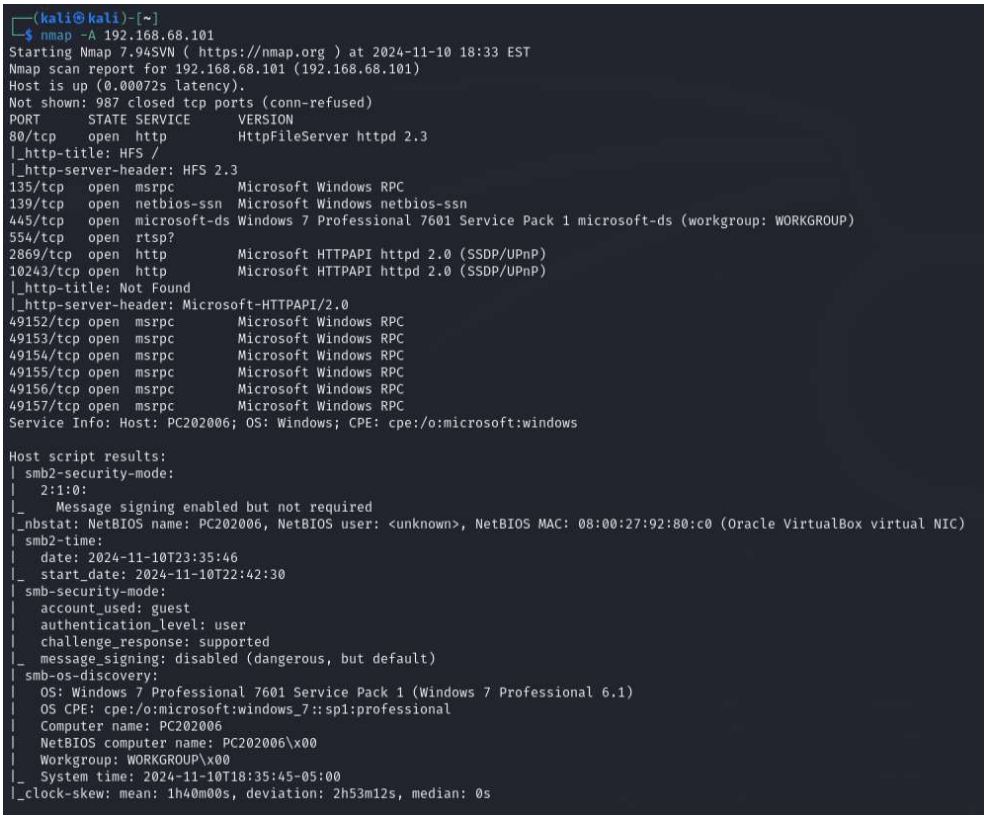

Figura 4 Escaneo de puerto y sistema operativo.

Finalmente, con el comando nmap --script smb-vuln* podemos detectar las vulnerabilidades en un sistema utilizando scripts de detección de vulnerabilidades que veremos más adelante:

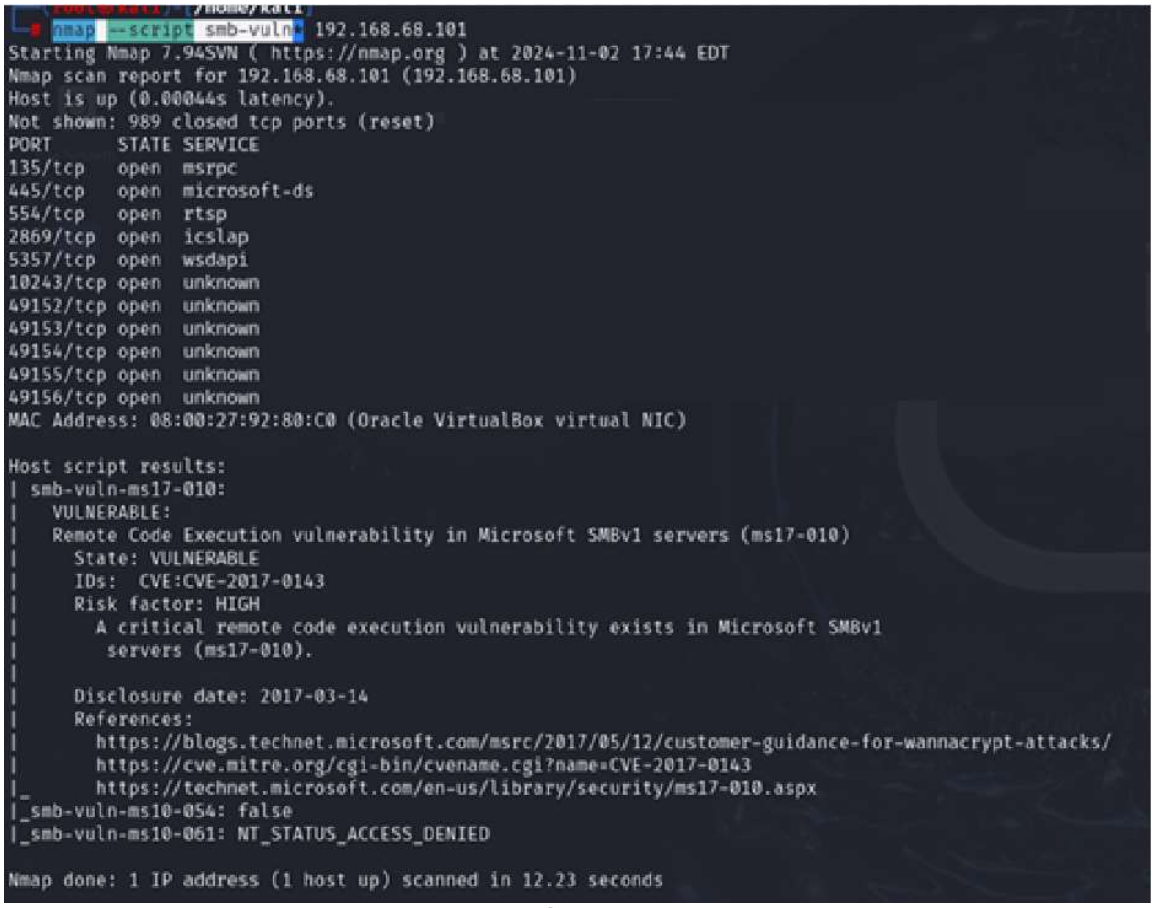

Figura 5 Detección de vulnerabilidades

Es importante tener en cuenta la información de la vulnerabilidad detectada, que más adelante usaremos para intentar explotarla:

smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

EXPLOTACIÓN

Ejecutamos el Metasploit Framework que viene precargado en el Kali Linux con el comando msfconsole, y que nos permitirá interactuar con el Metasploit:

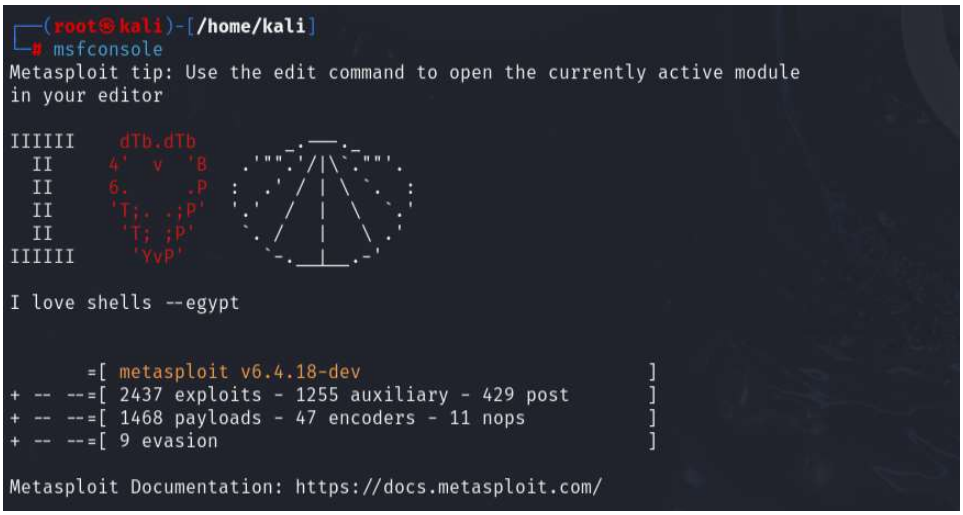

Figura 6 Apertura de Metasploit

Una vez iniciado el metasploit, buscaremos una de las vulnerabilidades anteriormente encontrada, la ms17-010.

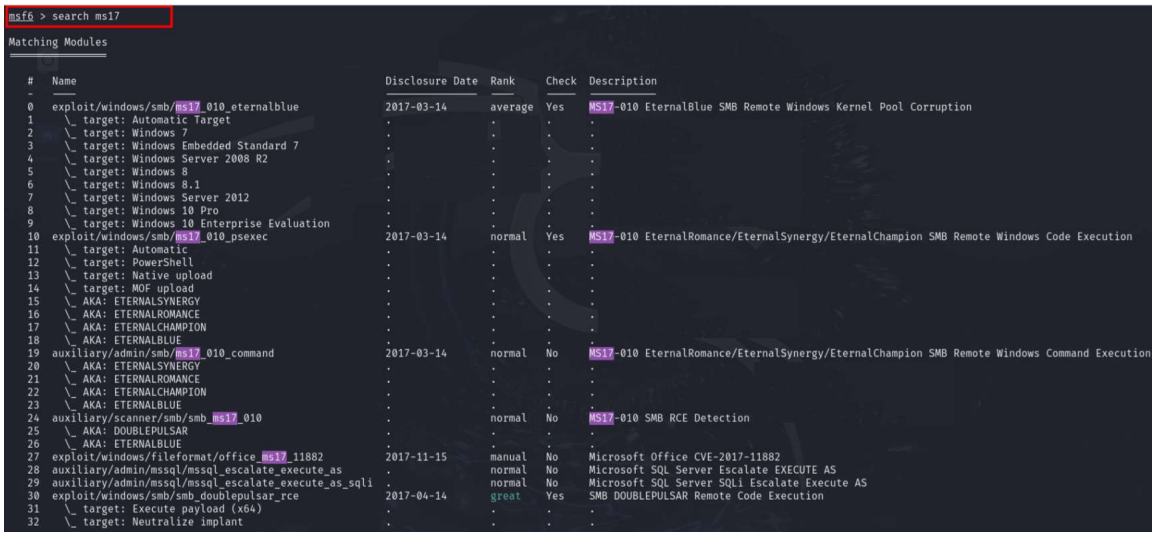

Figura 7 Búsqueda de vulnerabilidad en Metasploit.

Aquí vemos en la descripción el nombre de la vulnerabilidad detectada EternalBlue SMB Remote Windows Kernel Pool Corruption, por lo que ahora nos resta ejecutar la explotación de esta.

En el listado anterior, el numeral “0” es la que nos aplica para la explotación de la vulnerabilidad, por lo que procedemos a seleccionarla:

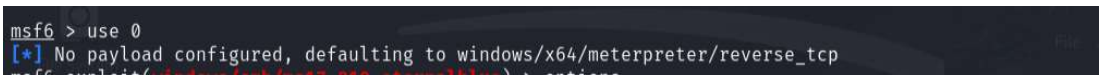

Figura 8 Ejecución en la consola de la vulnerabilidad Eternal Blue.

En este punto para la ejecución del exploit, aun nos falta suministrar información del destino:

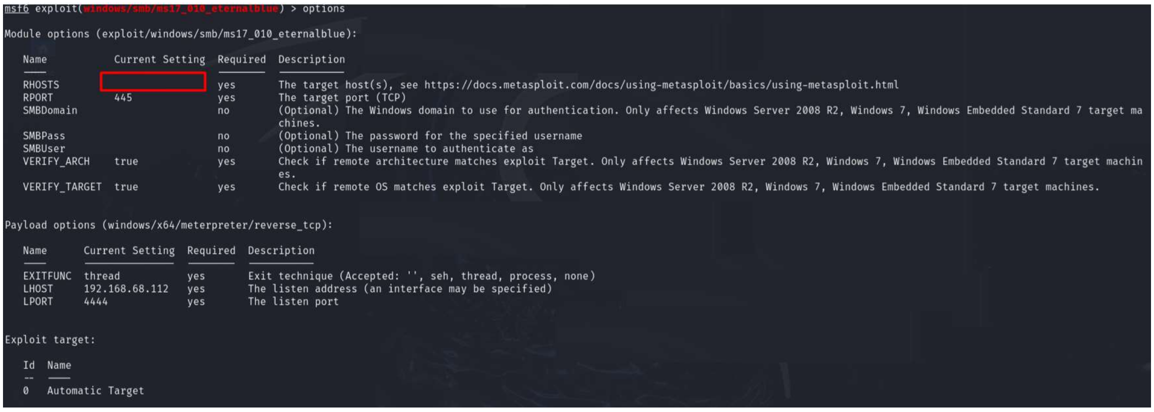

Figura 9 Visualización de la configuración del exploit

Asociamos la información del remote host con el comando set rhost <Ip destino>:

Figura 10 Parametrización del remote host del exploit.

A continuación, con la información suministrada y parametrizada, podemos proceder con la ejecución del exploit:

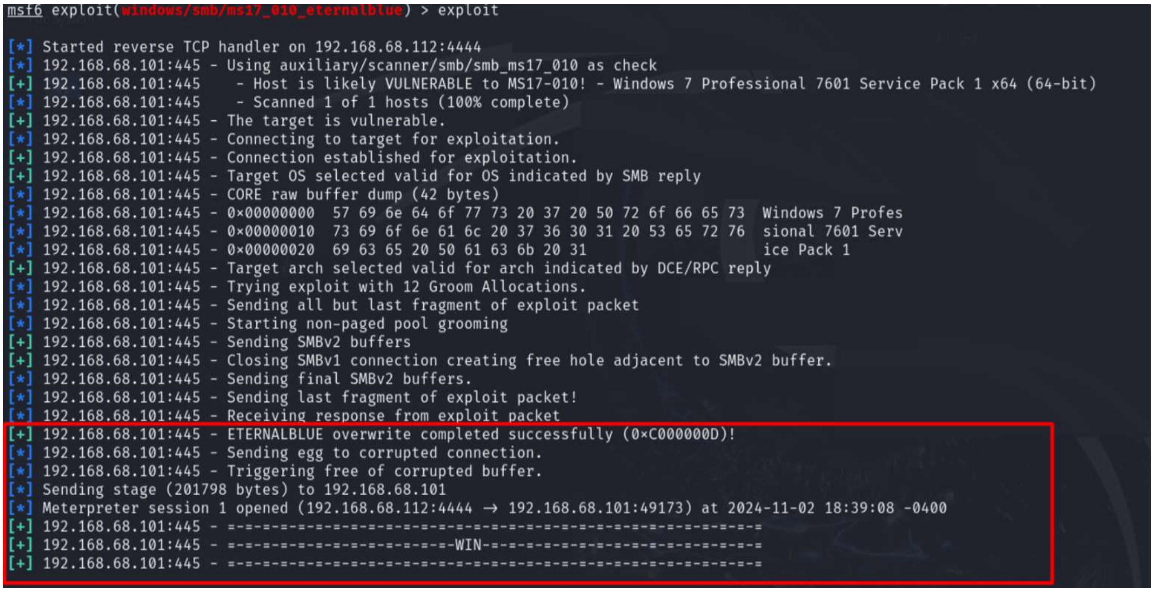

Figura 11 Ejecución del Exploit.

Se confirma la ejecución exitosa del exploit, confirmando igualmente que nos encontramos de manera remota dentro del objetivo con el comando sysinfo:

```
meterpreter > sysinfo
Computer        : PC202006
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_CO
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
meterpreter > cd ..
meterpreter > dir
Listing: C:\Windows
```

Figura 12 Confirmación de acceso remoto.

Verificamos, por ejemplo, la ejecución de los procesos actuales en la maquina:

```
meterpreter > ps

Process List

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x64   0
 248   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 260   460   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 320   312   csrss.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 368   312   wininit.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 376   360   csrss.exe         x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 404   360   winlogon.exe      x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 460   368   services.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 476   368   lsass.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 484   368   lsm.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 580   460   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 640   460   VBoxService.exe   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 696   460   svchost.exe       x64   0        NT AUTHORITY\Servicio de red
 796   460   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 836   460   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 860   460   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 940   460   svchost.exe       x64   0        NT AUTHORITY\Servicio de red
 1152  836   dwm.exe           x64   1        PC202006\usuario              C:\Windows\system32\Dwm.exe
 1180  1140  explorer.exe      x64   1        PC202006\usuario              C:\Windows\Explorer.EXE
 1248  460   spoolsv.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1264  460   taskhost.exe      x64   1        PC202006\usuario              C:\Windows\system32\taskhost.exe
 1316  460   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 1332  460   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 1420  460   SearchIndexer.exe x64   0        NT AUTHORITY\SYSTEM
 1428  460   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 1520  1180  VBoxTray.exe      x64   1        PC202006\usuario              C:\Windows\System32\VBoxTray.exe
 1608  376   conhost.exe       x64   1        PC202006\usuario              C:\Windows\system32\conhost.exe
 1644  460   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 1856  460   wmpnetwk.exe      x64   0        NT AUTHORITY\Servicio de red
 1872  460   sppsvc.exe        x64   0        NT AUTHORITY\Servicio de red
 2000  1180  cmd.exe           x64   1        PC202006\usuario              C:\Windows\system32\cmd.exe
 2592  460   svchost.exe       x64   0        NT AUTHORITY\Servicio de red
```

Figura 13 Verificación de ejecución de procesos maquina objetivo.

Por otro lado, en una línea de comandos por aparte, vamos a trabajar la vulnerabilidad asociada al hfs descubierta en la fase de escaneo. Primero, una vez ingresado en la consola

msfconsole, buscamos los módulos asociados a la vulnerabilidad y que alberga la información para la explotación de la vulnerabilidad:

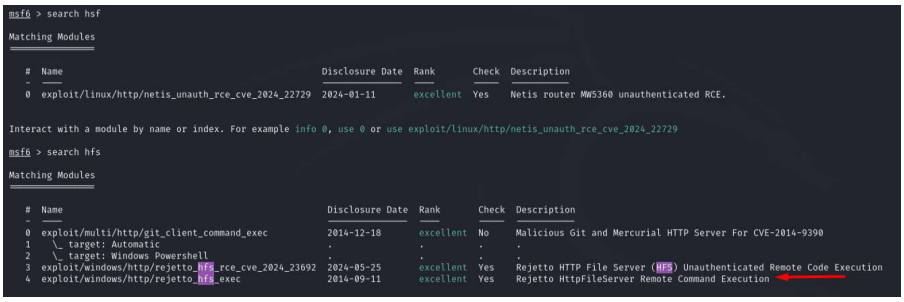

Figura 14 Búsqueda de módulo de explotación asociado a vulnerabilidad hsf.

En el resultado de la búsqueda, el modulo que nos aplica es el del numeral 4 de la anterior imagen, por lo que seguido a ello debemos proceder a ajustar el payload con la información correspondiente, como lo es nuevamente el host destino:

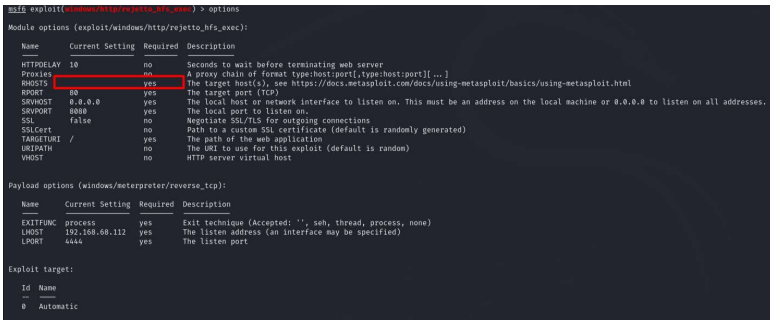

Figura 15 Payload antes del registro de la información.

Con el comando antes visto, ejecutamos el registro de la información, y también el exploit:

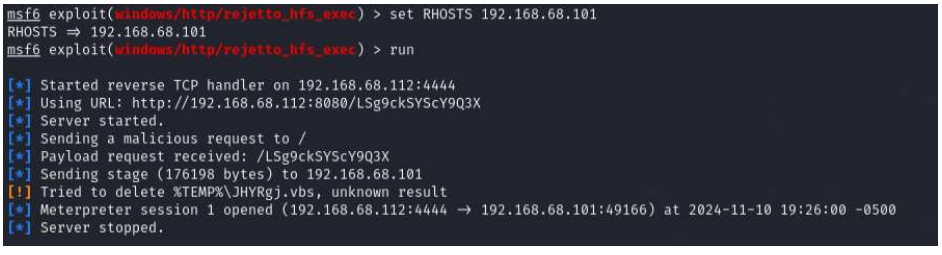

Figura 16 Ejecución de exploit HFS.

Una vez dentro del sistema, podemos verificar el privilegio del usuario con el que se accedió al sistema y así mismo, escalar privilegios con los comandos getuid y getsystem

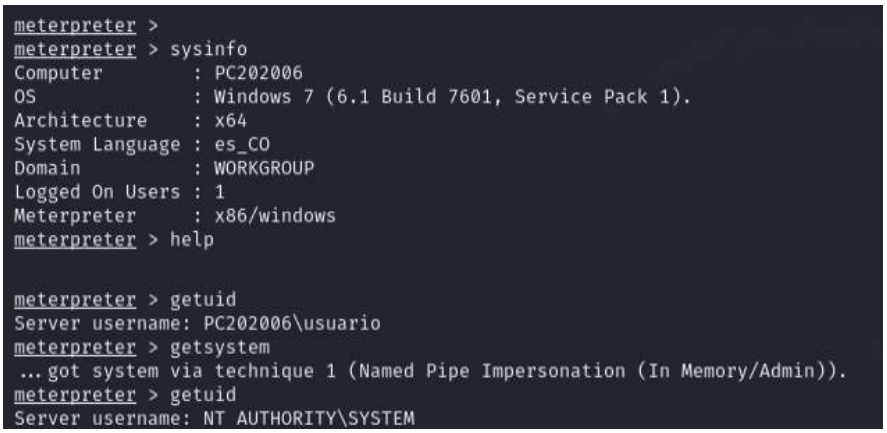

Figura 17 Escalamiento de privilegios.

5.2 PROCEDIMIENTO UTILIZADO POR EL EQUIPO BLUE TEAM PARA CONTENER Y EVITAR LA EXPLOTACIÓN DE VULNERABILIDADES EN EL ESCENARIO PROPUESTO.

Partiendo del informe anterior, donde se contaron con dos frentes de ataque, se propone por cada uno:

EternalBlue

Explota la vulnerabilidad en el protocolo SMBv1 en sistemas Windows no parcheados, de manera preventiva se recomienda implementar.

- Parches de Seguridad: Instalar todas las actualizaciones de seguridad proporcionadas por Microsoft, principalmente el parche MS17-010, ya que corrige la vulnerabilidad que permite el uso del exploit.

- Deshabilitar SMBv1: Deshabilitar el protocolo SMBv1 en todos los sistemas, ya que es obsoleto y propenso a múltiples vulnerabilidades. Como reemplazo, se recomienda el uso de protocolos SMBv2 o SMBv3.

HFS (Rejetto Http File Server)

Estos ataques suelen explotar vulnerabilidades de ejecución remota de comandos (RCE), se recomienda implementar las siguientes medidas:

- Actualizar a la última versión: Instalar la versión más reciente y segura de HFS, o considerar reemplazarlo por otro servidor más de mayor confianza, ya que las versiones antiguas son susceptibles a vulnerabilidades conocidas.
- Limitar el acceso público: Ajustar HFS para que solo sea accedido desde IPs o segmentos específicos, limitando la exposición de HFS, y disminuyendo la superficie de ataque.
- Limitar Permisos: Restringir los permisos de acceso a archivos y carpetas compartidos a solo lectura, en la medida de lo posible, para reducir el impacto en caso de un ataque exitoso.
- Desactivar funciones innecesarias: Desactivar funcionalidades no utilizada en HFS, como la edición de archivos o scripts, para reducir las vulnerabilidades explotables.

5.3 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS TRABAJO DE LOS EQUIPOS DE REDTEAM Y BLUETEAM.

A continuación, algunas estrategias y herramientas que contribuyen al trabajo que adelantan los equipos Blue Team y Red Team:

CIS

Proporciona herramientas, guías y estándares que fortalecen la postura de seguridad de una organización, mediante la implementación de controles y prácticas de seguridad. Su uso dentro del Blue Team se enfoca en:

- Estandarización de Controles de Seguridad: El CIS publica los CIS Controls, que son un conjunto de prácticas diseñadas para prevenir y mitigar ciberataques. Dentro del equipo Blue Team, ayudan a implementar un marco de seguridad reconocido para priorizar las acciones más efectivas contra amenazas comunes y garantizar consistencia y estándares uniformes en las defensas.
- Uso de CIS Benchmarks: Son orientaciones de configuración de seguridad que disponen de pasos detallados para la protección de los sistemas, las redes y aplicaciones. En los equipos el Blue Team, les permite configurar dispositivos, sistemas operativos y software siguiendo estándares seguros y así reducir la superficie de ataque y eliminar configuraciones predeterminadas vulnerables.
- Evaluación de Vulnerabilidades: El CIS proporciona herramientas como CIS-CAT para evaluar la configuración de sistemas según los Benchmarks. A los equipos Blue Team les permite identificar configuraciones débiles o no alineadas a los estándares de seguridad y así facilitar la remediación proactiva de vulnerabilidades.

- Alineación con Cumplimientos Regulatorios: Los controles y benchmarks de CIS están diseñados para alinearse con estándares globales, como lo son la NIST, ISO 27001 y GDPR. Facilitar auditorías de cumplimiento y comprobar prácticas de seguridad.

SIEM

Es una solución que permite monitorear los entornos tecnológicos de una organización, que persigue proporcionar una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos, permitiendo a su vez a los equipos de seguridad gestionar posibles vulnerabilidades de forma proactiva.

Estos equipos deben tener un control total sobre los eventos que transcurren en la empresa para poder detectar cualquier tendencia o patrón fuera de lo habitual y así actuar de forma inmediata.

Funcionamiento

Dentro de las funciones más importantes que realiza un SIEM, son la de almacenar e interpretar los registros. Esto se ejecuta en tiempo real aportando un alto grado de reacción para impedir o solucionar cualquier incidente informático. Recopila toda la información de forma centralizada para realizar un análisis profundo y así detectar tendencias y patrones de comportamiento que permitan diferenciar aquellos que no sean habituales.

Las principales características que dispone un buen sistema SIEM son:

- Identificar entre amenazas reales y falsos positivos.
- Monitoreo centralizado de todas las potenciales amenazas.
- Redirigir la actuación a personal cualificado para resolverlas.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.
- Cumplir con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad.

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

Para nuestro caso de estudio, y de acuerdo al hallazgo de las vulnerabilidades, como medidas generales se realizan las siguientes recomendaciones:

- Monitorización del Tráfico: Uso de herramientas como IDS/IPS para detectar patrones sospechosos en el puerto 445 y 8080, ya que este tipo de ataque deja rastros característicos que pueden ser detectados.

- Firewall y Reglas de Red: Restringir el puerto 445 en los firewalls tanto de red y como local del sistema, y limitar los accesos por el puerto 8080 ya que el exploit utiliza este puerto para comunicarse con los dispositivos vulnerables.

- Segmentación de Red: Implementar segmentación de red para limitar el acceso a dispositivos críticos, lo que reduce la opción de propagación.

6 CONCLUSIONES

- Se identificó los principales problemas de ciberseguridad afrontados por la organización causados por el estado actual de seguridad, con posible causa de incidentes de seguridad, e impactos emergentes. También hemos visto lo que puede llegar ser hoy en día el uso de tecnología sin los controles adecuados. A través de los equipos Red Team y Blue Team se logra definir el grupo de herramientas de seguridad adecuadas para emplear en procesos de prevención y contención frente a amenazas informáticas, manteniendo así confianza de la organización.

- De acuerdo a la evaluación de técnicas, tácticas y metodologías realizadas por el equipo Blue Team y Red Team, se logró establecer estrategias que permitieron mejorar los niveles de seguridad y defensa de la organización. Por medio de una simulación de un ataque dirigido sobre un ambiente controlado, se identificó vulnerabilidades en aquellos activos, y se logró demostrar cual sería el nivel de riesgo e impacto que tendría un ataque dirigido, de esta forma se reforzó la seguridad y defensa con herramientas de contención y detención, tomando en cuenta las cuatro fases de ejecución del diseño metodológico.

- Se demostró a través de la implementación y ejecución del modelo de amenazas en sus cuatro fases y los pasos para la recolección de la información, las vulnerabilidades del sistema informático con el que se compone la organización de estudio, apoyados y haciendo uso de las técnicas desplegadas por las herramientas de Kali Linux, como el análisis de red, informática forense, pentesting, análisis de sistemas, entre otros, que fueron

el suministro de los equipos Red Team y Blue Team, para la elaboración del informe que logrará mantener la seguridad y defensa y disminuir los niveles de riesgo.

7 RECOMENDACIONES

A partir de las investigaciones realizadas, se realizan las siguientes recomendaciones de seguridad:

- De acuerdo con el estándar ISO 27001 hacia los expertos en seguridad informática y encargados de la administración de las herramientas que se involucran en el flujo de recepción, transmisión y almacenamiento de la información, es de vital importancia realizar de forma constante la actualización de todos los sistemas, tanto a nivel de sistema operativo, firmware, parches o de propiamente las aplicaciones instaladas, con el objetivo de cerrar muchas puertas a los ciberdelincuentes.

- Mantener copias de seguridad en instalaciones con controles de accesos físicos, que se ejecuten de manera automática y periódica, y que se cifren para que en caso de robo esta no pueda ser accedida.

- Preparar un plan de respuesta ante incidentes de seguridad, en donde de acuerdo con la investigación realizada, el grupo SOC es el encargado del diseño de dicho plan, y que ayudará a minimizar el impacto ante la materialización de un evento de seguridad.

8 BIBLIOGRAFÍA

ADRIANA C, L, LORENA M, G., & CARLOS A, Q. (29 de octubre de 2019). Tendencia Cibercrimen en Colombia 2019 2020, Pg4: [En línea] Obtenido de EQUIPO DE INVESTIGACIÓN, EQU POLICIA NACIONAL: https://www.ccit content/uploads/informe-tendencias-cibercrimen compressed-3.pdf.

Ccn-cert. (s.f.). Enfoques y aspectos clave en ejercicios Red Team, Pg3 [En línea] 2021. Obtenido de Innotec Security: https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii.

Cuadernosdeseguridad. (6 de junio de 2016). Red Team: Pensando como el enemigo [En línea] 2016. Obtenido de El Arte de la Guerra. Disponible en: https://cuademosdeseguridad.com/2016/06/red-team-pensando-enemigo/

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). Recuperado de: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Gb-advisor, (2018). ¿Qué debemos hacer para librar nuestras redes de vectores de ataque en ciberseguridad? [En línea]. Disponible en: https://www.gb-advisors.com/es/vectores-de-ataque-en-cibersegundad/

Hackbysecurity. (2019). Ejercicio de Red Team [En línea] Disponible en: https://www.hackbysecurity.com/servidos-empresas/auditoria-informatica/ejercicio-de-red.

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

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas .

ISO 27001. (2013). NORMA ISO 2700. Disponible en: https://normaiso27001.es/

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

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles5482_G15_Auditoria.pdf

Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) Recuperado de: 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) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

PEÑALOZA POSADA, Omar Antonio. (2020). INFORME TÉCNICO ACCIONES DESARROLLADAS POR LOS EQUIPOS BLUE TEAM Y RED TEAM.

Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/37157/97612620.pdf?sequence=1&isAllowed=y