Prueba de Penetración

HTB Labs (Blue)

nico.sanchezsierra@hotmail.com, OSID: OS-001

2025-07-29

Contents

1 Reporte

1.1 Introducción

Este reporte forma parte de una serie de análisis técnicos documentados en mi repositorio de GitHub (https://github.com/NicolasSanchezSierra/Pruebas-de-Penetracion) con el fin de demostrar competencias prácticas en pruebas de penetración profesional.
El objetivo de estos informes es reflejar un proceso riguroso, estructurado y documentado acorde con metodologías como OSSTMM, PTES y OSCP.

Se trata de laboratorios desarrollados en plataformas como Hack The Box (HTB) o TryHackMe (THM), seleccionados para simular escenarios reales de red interna, explotación, escalamiento y persistencia.

1.2 Objetivo

El objetivo de esta evaluación es recrear una prueba de penetración interna hacia el entorno de HTB. Para hacer la prueba de penetración se requerirá hacer la metodología completa y la evaluación de la misma. En este caso usaremos la máquina Blue. Por compromiso con la plataforma de Hack The Box, no podremos atacar direcciones IP que no sean las asignadas, pues eso esta fuera de nuestro alcance.

2 Resumen High-Level

Fui mandado a hacer una prueba de penetración interna hacia una máquina de HTB. La prueba de penetración interna se basa en atacar los servicios internos conectados entre si. La finalidad de esta prueba es hacer una metodologia de ataque similar a las que se hacen en los entornos profesionales y algunas instituciones academicas como OSCP.

Mi objetivo principal fue evaluar la red interna, identificar sistemas y explotar las fallas mientras documentamos.

Cuando ejecutábamos la prueba de penetración interna, identificamos varias vulnerabilidades. Al explotar algunas de ellas, fui capaz de obtener acceso a la máquina, principalmente debido a la falta de parches de seguridad y versiones desactualizadas. Durante la prueba, logré obtener acceso de administrador y todos los sistemas fueron explotados con éxito.

A continuación anotamos las vulnerabilidades encontradas y el peligro que estas suponen. Más adelante se explican con más detalle.

Alto	Medio	Bajo	Total
1	3	0	4

ID	Riesgo	CVE	Nombre
1	Medio	N/A	Samba Public Shares
2	Medio	N/A	Rpcclient Enumeration
3	Medio	N/A	Enumeración Excesiva
4	Alto	CVE-2017-0144	Eternal Blue

2.1 Recomendaciones

Visto las vulnerabilidades encontradas, es necesario actualizar los sistemas y las aplicaciones para que estas vulnerabilidades no puedan ser ejecutadas. Además no todas ellas pueden ser arregladas con un parche, y necesitan más trabajo. Por ello, estas serán explicadas con más detalle en la sección de penetración.

3 Metodología

Utilicé un enfoque estándar de pruebas de penetración que incluye las fases de reconocimiento, enumeración, explotación, escalación de privilegios y post-explotación.
Este método es comúnmente empleado en entornos de certificación Offensive Security para evaluar la seguridad de sistemas y redes.

A continuación, se describen los pasos realizados para identificar y explotar las vulnerabilidades encontradas.

3.1 Recolección de Información

La recolección de información es una porción de la prueba de penetración que se centra en identificar los límites y las tecnologías de nuestro objetivo. Durante la prueba de penetración fui asignado la siguiente IP.

Redes disponibles

- 10.10.10.40

3.2 Penetración

La penetración del sistema es otra parte de la prueba, que se basa en ganar acceso al sistema de todas las formas posibles. Fue posible acceder al sistema que se encontraba detrás de la dirección IP. Ahora veremos como conseguimos entrar al sistema.

3.2.1 Dirección IP: 10.10.10.40

3.2.1.1 Enumeración de servicios

La enumeración de servicios se enfoca en retener toda la información posible que podamos encontrar de los servicios que se encuentran en los sistemas. Es una parte valiosa, pues nos da posibles ideas

para encontrar vectores de ataque con los cuales ganar acceso al sistema. Como hemos dicho, miraremos todos los puertos disponibles y sus versiones. En caso de encontrar aplicaciones web también tendremos que inspeccionarlas.

Dirección IP	Puertos Abiertos
10.10.10.40	135,139,445

Servicio	Versión
msrpc	Microsoft Windows RPC
netbios-ssn	Microsoft Windows netbios-nss
microsoft-ds	Windows 7 Profesional 7601

A continuación pondremos capturas de Nmap para verificar la enumeración.

Puertos encontrados:

```
nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertos.txt 10.10.10.40
Host is up, received user-set (0.16s latency).

PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

Figure 3.1: Nmap escaneo puertos

Versiones de los servicios encontrados anteriormente:

```
nmap -sCV -A -O -p135,139,445 -oN versiones.txt 10.10.10.40
Host is up (0.13s latency).

PORT    STATE SERVICE      VERSION
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)

Device type: general purpose|specialized
Network Distance: 2 hops
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-07-30T09:05:04
|_  start_date: 2025-07-30T08:56:32
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-07-30T10:05:01+01:00
```

Figure 3.2: Nmap escaneo de versiones

Escaneo profundo con nmap y scripts NSE sobre Samba:

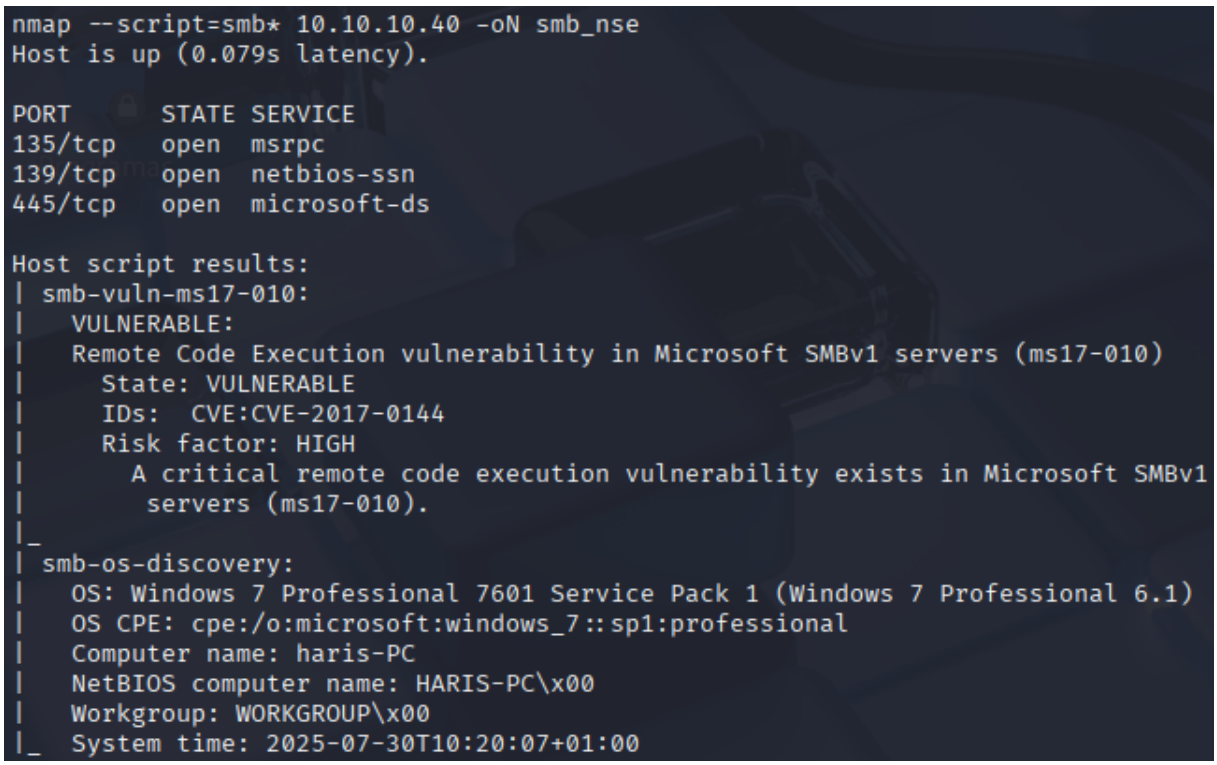

Figure 3.3: Nmap scripts nse para samba

3.2.1.2 Escalada de Privilegios

Una vez ya tenemos información sobre los servicios y aplicaciones con sus respectivas versiones, nos hacemos una idea por dónde podemos atacar. Puesto que si no es una versión vulnerable, es falta de capas de seguridad. A continuación reportaremos las vulnerabilidades que se nombraron al inicio del documento.

3.2.1.3 Vulnerabilidad (ID: 1, Samba Public Shares)

Riesgo: Medio

CVE: N/A

Explicación de la vulnerabilidad: Esta vulnerabilidad nos permite autenticarnos dentro del servicio de SMB sin contraseña ni usuario. Podemos listar carpetas, descargar archivos y subir archivos. Supone un riesgo tener esos privilegios sin usuario ni contraseña.

Servicios Afectados: SMB (microsoft-ds) - Windows 7 Profesional 7601

Remedio de la vulnerabilidad: Sugerimos bloquear el acceso anónimo sin contraseña, además de permitir acceso limitado y con contraseña. Además, sugerimos no tener carpetas Públicas ni de Usuarios en estos servicios.

Pruebas:

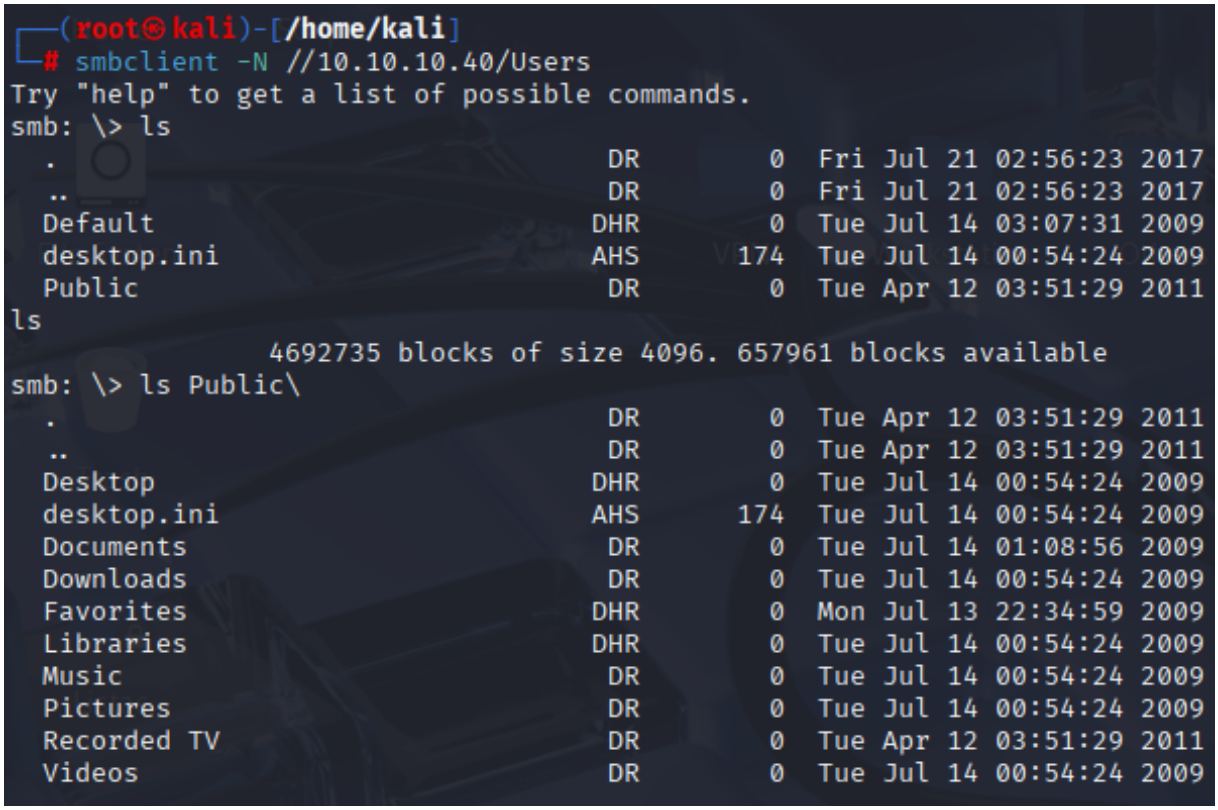

Figure 3.4: Smbclient

3.2.1.4 Vulnerabilidad (ID: 2, Rpcclient Enumeration)

Riesgo: Medio

CVE: N/A

Explicación de la vulnerabilidad: Esta vulnerabilidad se basa en poder enumerar y recolectar información a través del servicio RPC (msrpc). Visto que no tiene usuario y se puede entrar anónimamente sin contraseña, supone un riesgo.

Servicios Afectados: msrcp - Microsoft Windows RPC

Remedio de la vulnerabilidad: Sugerimos bloquear el acceso anónimo sin contraseña, además de permitir acceso limitado y con contraseña.

Pruebas:

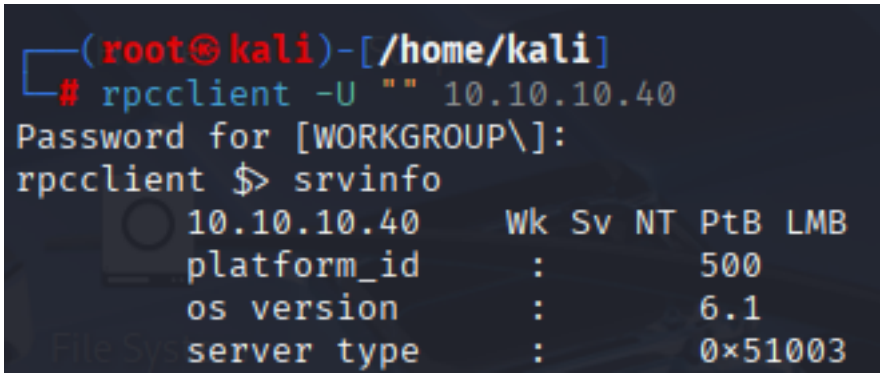

Figure 3.5: Rpcclient

3.2.1.5 Vulnerabilidad (ID: 3, Enumeración Excesiva)

Riesgo: Medio

CVE: N/A

Explicación de la vulnerabilidad: Esta vulnerabilidad se basa en poca medida de seguridad. Pues podemos enumerar y conseguir información tanto de los servicios como del sistema sin mucha complicación. Nos permite saber el host, enumerar puertos y versiones, además de identificar ciertas vulnerabilidades.

Servicios Afectados: Sistema Operativo Windows y sus servicios.

Remedio de la vulnerabilidad: Se recomienda filtrar puertos no utilizados, limitar acceso a ciertas IP, configurar correctamente los servicios, implementar soluciones de detección de escaneos (IDS/IPS) y desactivar servicios innecesarios.

Pruebas: Anteriormente ya pusimos capturas sobre comandos Nmap, por lo tanto no las implementaremos otra vez.

3.2.1.6 Vulnerabilidad (ID: 4, Eternal Blue)

Riesgo: Alto

CVE: CVE-2017-0144

Explicación de la vulnerabilidad: Esta vulnerabilidad de ejecución remota en el protocolo SMBv1 afecta a sistemas Windows XP, Vista, 7 además de Windows Server 2003 y 2008. El problema surge en la función de manejar paquetes Trans2, pues no valida los tamaños de memoria del cliente, permitiendo

un heap overflow y ejecute código arbitrario con privilegios elevados. Se puede ejecutar sin necesidad de autenticación.

Servicios Afectados: SMB (microsoft-ds) - Windows 7 Profesional 7601

Remedio de la vulnerabilidad: Para solucionar este problema se recomienda desactivar el protocolo SMBv1. Además se recomienda actualizar Windows con el parche (MS17-017). También será recomendable configurar el firewall para bloquear el puerto 445 hacia redes externas y usar IDS/IPS para detectar y analizar tráfico.

Pruebas: Hemos podido vulnerar el sistema a través de Eternal Blue con la ayuda de metasploit.

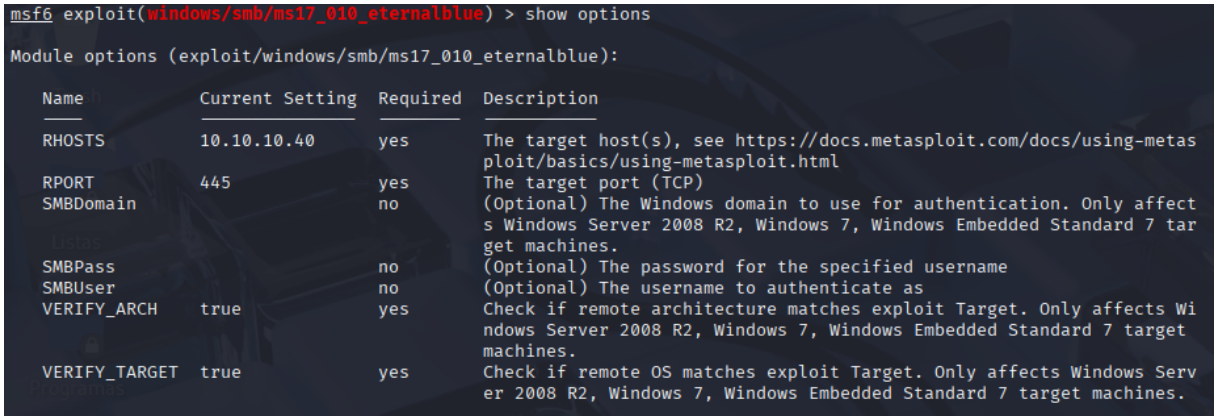

Figure 3.6: Metasploit

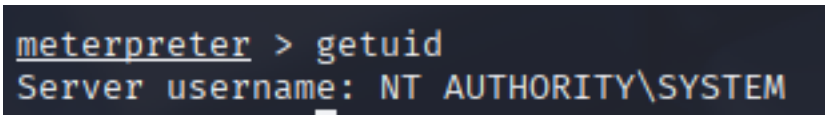

Figure 3.7: Metasploit

3.3 Mantener Acceso

Mantener acceso al sistema es una parte importante, pues nos permite volver al sistema después de haber sido comprometido. Esta fase se enfoca en mantener acceso y privilegios al sistema manteniendo una conexión para volver a entrar cuando queramos. En esta parte notaremos como hemos podido conseguir mantener acceso al sistema.

Pruebas: Una vez ya comprometido el sistema, crearemos un usuario en Windows con privilegios Administrador. De esa forma siempre podemos conectarnos con privilegios elevados.

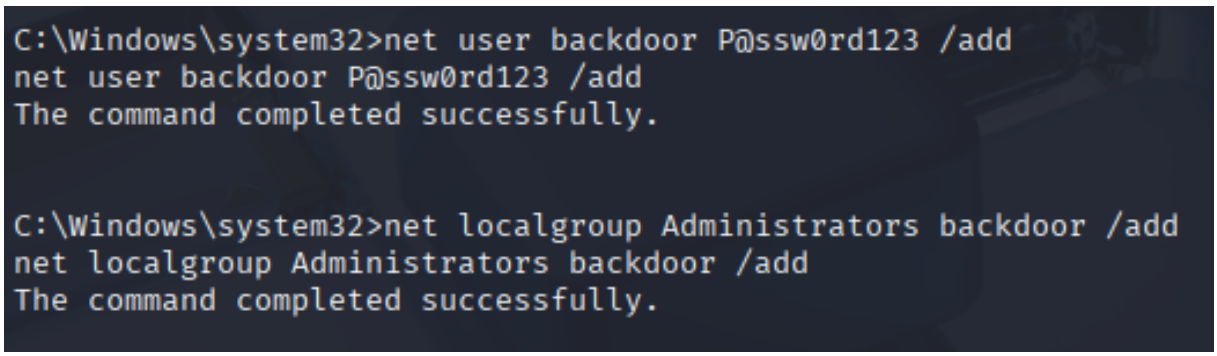

Figure 3.8: Metasploit (CMD)

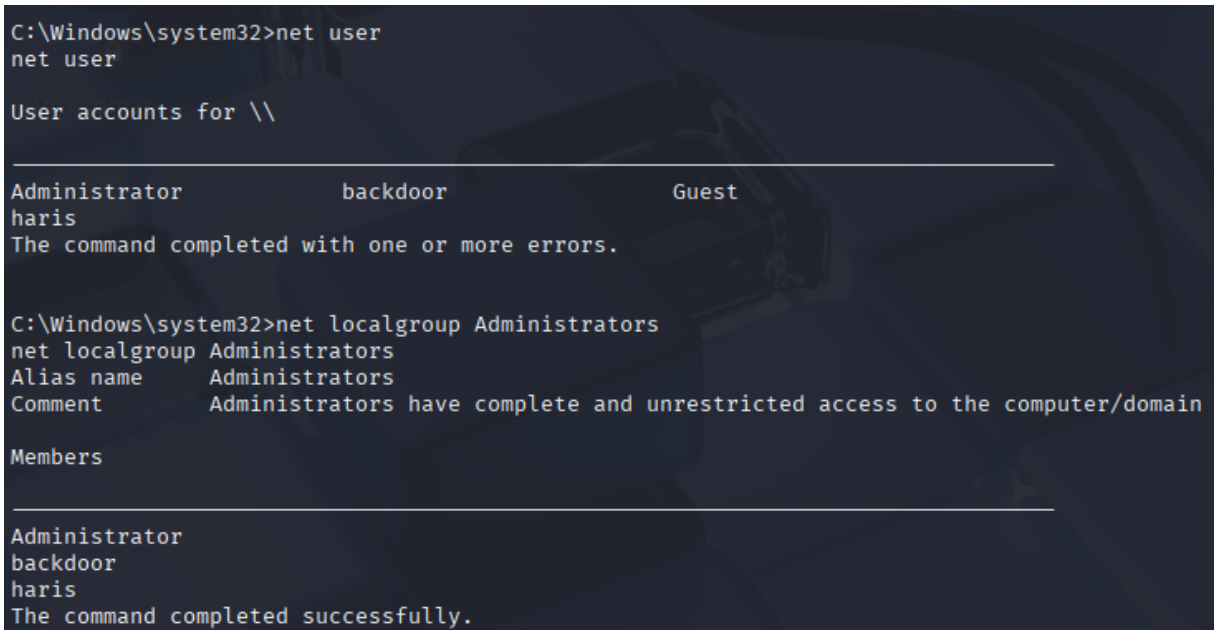

Figure 3.9: Metasploit (CMD)

3.4 Limpieza de Pruebas

Una vez hemos terminado de identificar, explotar y ganar privilegios, debemos eliminar todas aquellas piezas que fuimos añadiendo para hacer esto posible. No queremos manchar los sistemas, no queremos dejar paso a nuevas vulnerabilidades. Además también eliminaremos cualquier tipo de puerta trasera que hayamos creado.

Pruebas: Empezaremos eliminando el usuario Backdoor.

```
C:\Windows\system32>net localgroup "Administrators" backdoor /delete
net localgroup "Administrators" backdoor /delete
The command completed successfully.


C:\Windows\system32>net localgroup "Users" backdoor /delete
net localgroup "Users" backdoor /delete
The command completed successfully.


C:\Windows\system32>net user backdoor /delete
net user backdoor /delete
The command completed successfully.
```

Figure 3.10: Metasploit (CMD)

```
C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    haris
The command completed with one or more errors.


C:\Windows\system32>net localgroup Administrators
net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
haris
The command completed successfully.
```

Figure 3.11: Metasploit (CMD)

Eteneral Blue ejecutó una Shell en memoria RAM, lo que quiere deir que no tenemos nada que borrar. Quedarán pruebas en los logs, pero nosotros no borramos logs de empresas.