

UNIVERSIDAD DE MURCIA

GRADO EN INGENIERÍA INFORMÁTICA

4º CURSO

GRUPO 6

CURSO 2016/2017 - JUNIO

Seguridad

Práctica final

Alumnos:

Cristian Roche Borja

DNI: 76581531H

Alicia Ruiz Tovar

DNI: 48693813F

Docentes:

Gabriel López Millán

Gregorio Martínez Pérez



Índice

1. NMAP y Metasploit	4
1.1. Víctima	4
1.2. Atacante	4
1.2.1. NMAP	4
1.2.2. NMAP con Metasploit	6

1. NMAP y Metasploit

1.1. Víctima

Utilizaremos una máquina virtual de prueba. Esta máquina ha sido creada con vulnerabilidades para la práctica de ataques. La URL de descarga es la siguiente: wiki.inf.um.es/metasploitable2/metasploitable-linux-2.0.0.zip.

La IP de esta máquina es la 192.168.62.189.

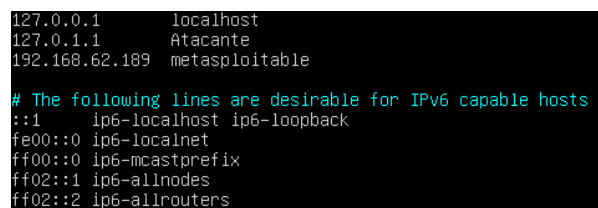
1.2. Atacante

1.2.1. NMAP

El equipo que actuará como atacante hace uso de la herramienta NMAP. Para instalarla ejecutamos el siguiente comando:

```
$ sudo apt-get install nmap
```

Establecemos en el archivo `/etc/hosts`, equivalente al DNS local, la IP de la víctima (192.168.62.189) y la denominamos `metasploitable`, como muestra la figura 1.



```
127.0.0.1    localhost
127.0.1.1    Atacante
192.168.62.189 metasploitable

# The following lines are desirable for IPv6 capable hosts
::1         ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

Figura 1: Atacante_dns_victima.

De esta forma, tenemos dos opciones para hacer referencia a la víctima. En la figura 2 se observa el resultado de este escaneo simple fruto de cualquiera de estas dos opciones.

```
$ nmap 192.168.62.189
$ nmap metasploitable
```

De forma un poco más elaborada, se puede ejecutar el escaneo de puertos haciendo uso de otras técnicas:

- Mediante listado de equipos: `$ nmap 192.168.62.1 192.168.62.10 192.168.62.189`
- Mediante subred: `$ nmap 192.168.62.0/24`
- Mediante un fichero que almacene las IPs (o las expresiones de las mismas) a analizar: `$ nmap -iL hosts.txt`, como muestra la figura 3.

```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-04-23 13:06 CEST
Nmap scan report for 192.168.62.189
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
alumno@Atacante:~$
```

Figura 2: Atacante_nmap_simplescan.

```
alumno@Atacante:~$ cat hosts.txt
192.168.62.189
192.168.62.1
alumno@Atacante:~$ cat hosts2.txt
192.168.61.0/24
metasploitable
192.168.62.1
192.168.62.200-220
alumno@Atacante:~$
```

Figura 3: Atacante_nmapscan_filecomplex.

1.2.2. NMAP con Metasploit

También hemos de instalar Metasploit para hacer uso de él: <https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers>. Una vez instalado, con `$ msfconsole` inicializamos Metasploit y la base de datos asociada.

A continuación, realizamos un scanner básico de la red, almacenando el contenido en la base de datos interna y exportándolo completo de la misma a un fichero, para así analizarlo:

```
$ db_nmap -v -sV 192.168.62.0/24
$ db_export out_ejercicio1.txt
```

Como muestra la figura 4, se observa que en dicho fichero encontramos el contenido del escaneo. Por un lado, podemos ver información del usuario que ha invocado el Metasploit. Seguidamente, tenemos el apartado que refiere a los hosts y servicios que se han encontrado en la dirección de subred que se le ha pasado al escaneo. Por último, podemos observar que el grueso del fichero son los módulos del Metasploit.

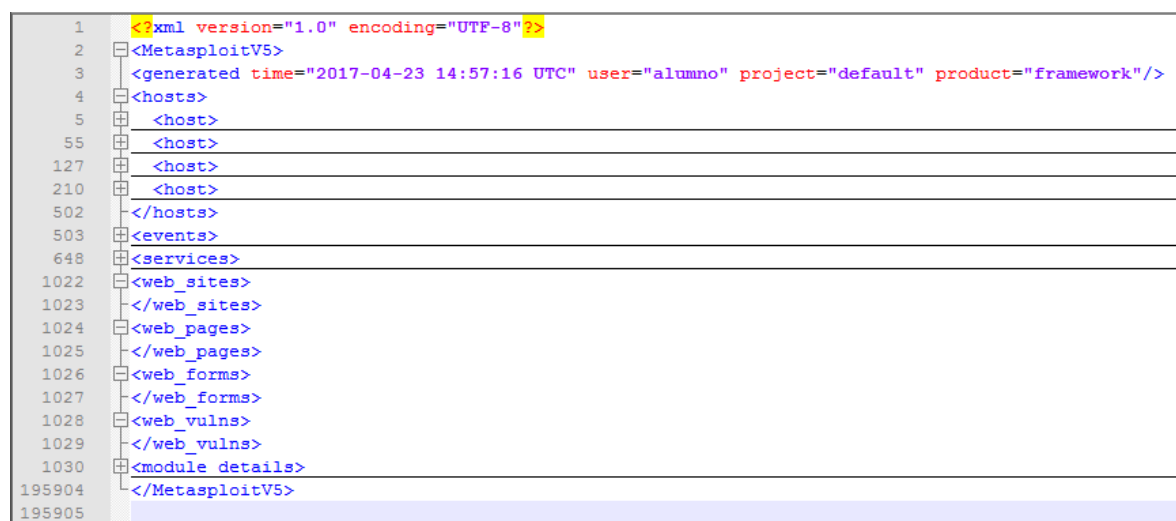


Figura 4: Atacante_scanner_y_BBDD.

1.2.3. Wireshak: trazas

A continuación mostramos algunas trazas obtenidas tras ejecutar ciertos comandos con NMAP.

- `$ nmap -sS -p 20-30 192.168.62.0/24`. En el host `metasploitable` se lanza un escaneo de puertos cada segundo a un puerto diferente entre los puertos 20 al 30, como muestra la figura ???. El fin principal de realizar un escaneo de puertos de esta forma es evitar ser detectado por la seguridad que pueda tener la subred.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <MetasploitV5>
3    <generated time="2017-04-23 14:57:16 UTC" user="alumno" project="default" product="framework"/>
4    <hosts>
5      <host>
55     <host>
127    <host>
210    <host>
502    </hosts>
503    <events>
648    <services>
1022   <web_sites>
1023     </web_sites>
1024   <web_pages>
1025     </web_pages>
1026   <web_forms>
1027     </web_forms>
1028   <web_vulns>
1029     </web_vulns>
1030   <module_details>
195904 </MetasploitV5>
195905

```

Figura 5: Atacante_wireshar_scaneo_delay.

- \$sudo nmap -sS |mtu 24 -p 80 metasploitable 192.168.62.102.
En el hots metasploitable y en la IP 192.168.62.102 se lanza un escaneo al puerto 80 con el bit SYN activado, como se muestra en la figura ?? Lo que se hace es enviar un paquete SYN, como si se fuera a abrir una conexión real y después se espera una respuesta. Si se recibe un paquete SYN/ACK esto indica que el puerto está abierto, mientras que si se recibe un RST (reset) indica que no hay nada escuchando en el puerto. Si no se recibe ninguna respuesta después de realizar algunas retransmisiones o se recibe un ICMP entonces el puerto se marca como filtrado.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <MetasploitV5>
3    <generated time="2017-04-23 14:57:16 UTC" user="alumno" project="default" product="framework"/>
4    <hosts>
5      <host>
55     <host>
127    <host>
210    <host>
502    </hosts>
503    <events>
648    <services>
1022   <web_sites>
1023     </web_sites>
1024   <web_pages>
1025     </web_pages>
1026   <web_forms>
1027     </web_forms>
1028   <web_vulns>
1029     </web_vulns>
1030   <module_details>
195904 </MetasploitV5>
195905

```

Figura 6: Atacante_wireshar_scaneo_delay.