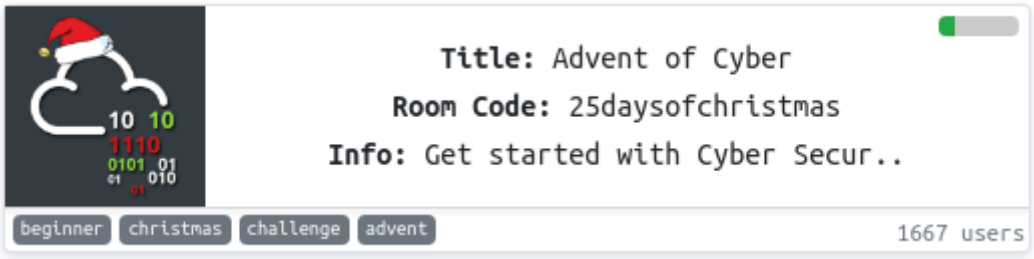
TryHackMe Blog

Share this

17 DECEMBER 2019 / HYDRA

Hydra

This blog post will explain what Hydra is and how we this tool to crack a remote authentication service.



Do the Hydra Christmas Challenge: https://tryhackme.com/room/25daysofchristmas

What is Hydra?

Hydra is a brute force online password cracking program; a quick

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.

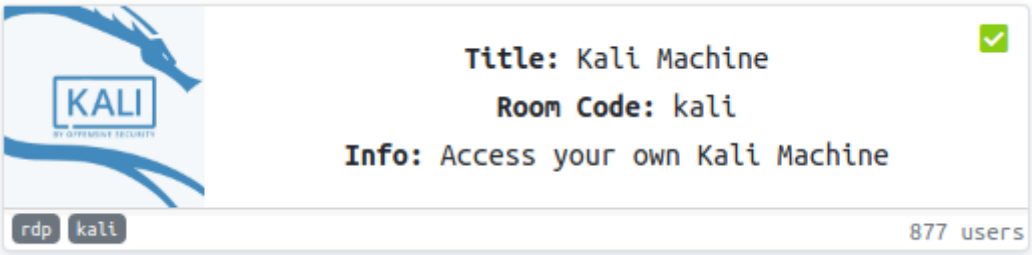
Hydra has the ability to bruteforce the following protocols: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, IRC, 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 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.

can download it here: https://github.com/vanhauser-thc/thc-hydra

If you don't have Linux or the right desktop environment, you can deploy your own Kali Linux machine with all the needed security tools. You can even control the machine in your browser! Do this with our Kali room - https://tryhackme.com/room/kali



Using Hydra

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://192.168.0.1
```

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

SSH

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

-l is for the username
-P Hydra to use a list of passwords, we can also pass in a list of

-t specifies the number of threads used

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, of simply view the source code.

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

```
hydra -l <username> -P <password list> <ip> http-post-form "/<logi
n url>: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

and complete the Hydra Christmas challenge!

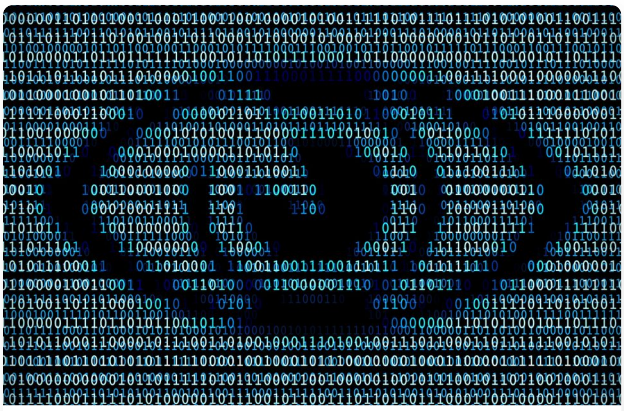
Ben Spring
Read more posts by this author.

Read More

— TryHackMe Blog —
hydra

Zeus Writeup

1 post →



Dumping Router Firmware - WriteUp

Dumping Router Firmware is a room at TryHackMe and can be accessed by using the below link! https://tryhackme.com/room/rfirmwareW will move step by step i.e. from downloading the sample

6 MIN READ