

Cyber Security

UTS

Nama :Moch.Zulfa Akbar Maulana

NIM :2231740016

HYDRA

What is Hydra?

Hydra is a brute force online password cracking program, a quick system login password “hacking” tool.

Hydra can run through a list and “brute force” some authentication services. Imagine trying to manually guess someone’s 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.

According to its [official repository](#), Hydra supports, i.e., has the ability to brute force 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](#), [MEMCACHED](#), [MONGODB](#), [MS-SQL](#), [MYSQL](#), [NCP](#), [NNTP](#), [Oracle Listener](#), [Oracle SID](#), [Oracle](#), [PC-Anywhere](#), [PCNFS](#), [POP3](#), [POSTGRES](#), [Radmin](#), [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, you can check the [Kali Hydra tool page](#).

This shows the importance of using a strong password; if your password is common, doesn’t contain special characters and is not above eight characters, it will be prone to be guessed. A one-hundred-million-password list contains common passwords, so when an out-of-the-box application uses an easy password to log in, change it from the default! CCTV cameras and web frameworks often use `admin:password` as the default login credentials, which is obviously not strong enough.

Installing Hydra

Hydra is already installed on the AttackBox. You can access it by clicking on the **Start AttackBox** button.

If you prefer to use the in-browser Kali machine, Hydra also comes pre-installed, as is the case with all Kali distributions. You can access it by selecting Use Kali Linux and clicking on **Start Kali Linux** button.

However, you can check its official repositories if you prefer to use another Linux distribution. For instance, you can install Hydra on an Ubuntu or Fedora system by executing `apt install hydra` or `dnf install hydra`. Furthermore, you can download it from its official [THC-Hydra repository](#).

Answer the questions below

Read the above and have Hydra at the ready.

No answer needed

✓ Correct Answer

Start the AttackBox by pressing the **Start AttackBox** button at the top of this page. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.


Press the green **Start Machine** button below to deploy the machine attached to this task, then navigate to [http://MACHINE_IP](#) on the AttackBox (this machine can take up to 3 minutes to boot)

▶ Start Machine

Target Machine Information

Title	Target IP Address	Expires			
Hydra Challenge	10.10.197.47	58min 44s	?	Add 1 hour	Terminate

Learn > Hydra



Hydra

Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.

👍 Easy ⌚ 45 min

Help

Save Room

👍 4548


🗨️

Options

Room progress (33%)

Hydra | DarkStar7471 • Sep 25, 2020

Source: YouTube



Connecting...

Access desktop in 44s

THM AttackBox

58min 35s

Room progress (33%)

Task 2 Using Hydra

Start the AttackBox by pressing the **Start AttackBox** button at the top of this page. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.

Press the green **Start Machine** button below to deploy the machine attached to this task, then navigate to <http://10.10.189.117> on the AttackBox (this machine can take up to 3 minutes to boot)

▶ Start Machine

Hydra Commands

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

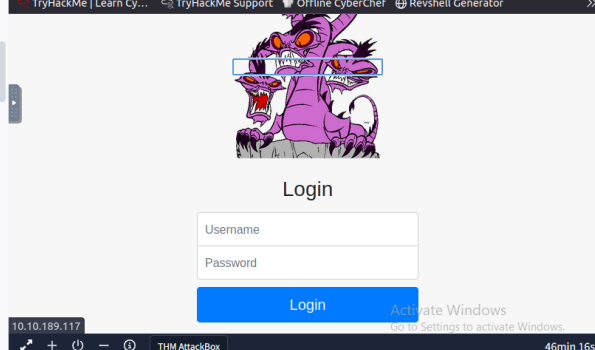
```
hydra -l user -P passlist.txt ftp://10.10.189.117
```

For this download machine, here are the commands to use Hydra on

Thu 24 Apr, 13:32 AttackBox IP: 10.10.179.162

Hydra Challenge — Mozilla Firefox

10.10.189.117/login



10.10.189.117

THM AttackBox

46min 16s

vnc.tryhackme.tech wants to

See text and images copied to the clipboard

Allow

Block

System Thu 24 Apr, 14:17 AttackBox IP: 10.10.35.109

Hydra Challenge — Mozilla Firefox

Hydra Challenge

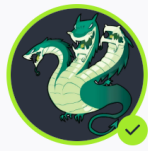
10.10.214.138

TryHackMe Support Offline CyberChef Revshell Generator

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox...

THM{2673a7dd116de68e85c48ec0}



Congratulations on completing Hydra!!! 🎉

Points earned

0

Completed tasks

2

Room type

Walkthrough

Difficulty

Easy

Streak

1

Leave Feedback

Next

Activate Windows
Go to Settings to activate Windows.