Hydra

Password Cracking

Disclaimer/Warning

The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conduced with aid from these Kali Guides.

Only use this tool on domains, addresses, files and resources that you have permission to.

Brief Summary

A powerful and flexible tool for username and password cracking using a **brute-force** approach.

Helpful Vocabulary

Brute-Force Attack:

- A method of guessing login info by running through every single combination within a set of parameters (e.g. a “dictionary attack” would be checking for every word within an established list of common words and phrases)

Network Protocol

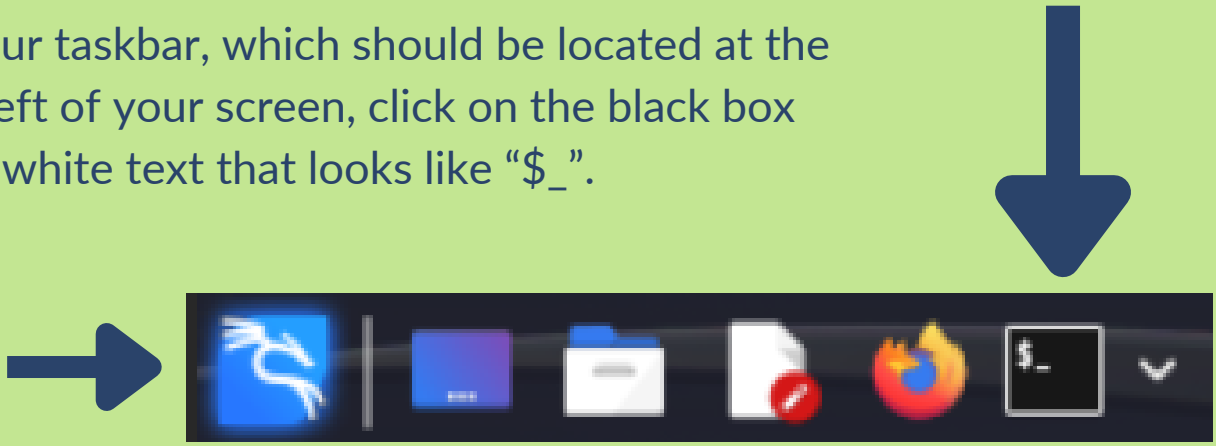
- A universal language for communication between different devices. Each protocol has a set of rules that regulates communications and/or data processing across networks.

SSH:

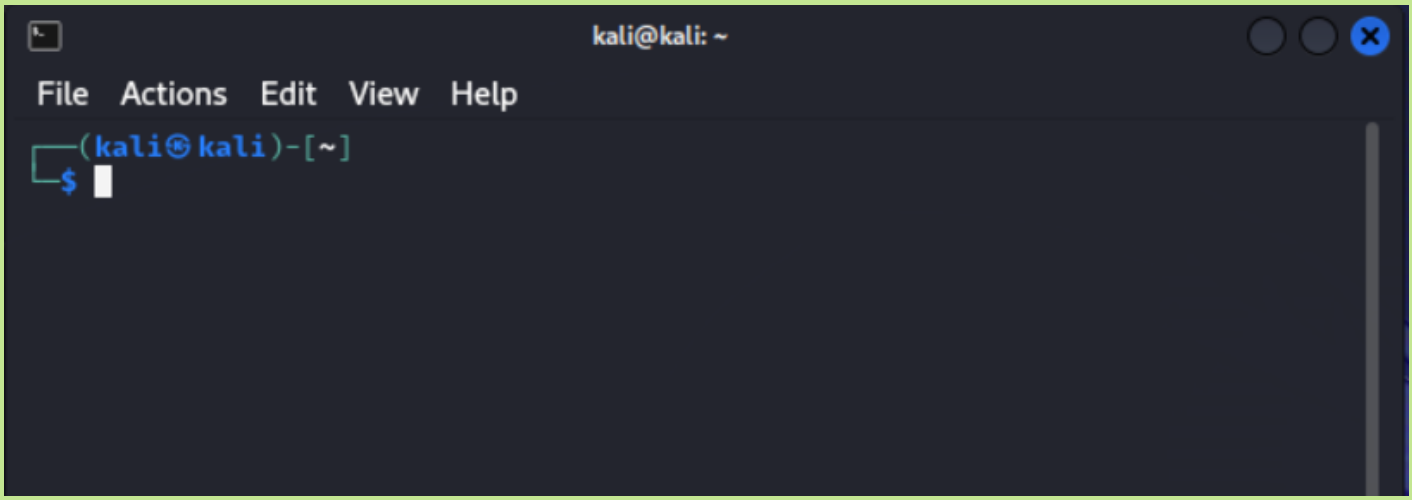
- Secure Shell Protocol or SSH, is a network protocol that allows hackers to safely access services on an unsecure network. It does this by remotely encrypting connections between devices.

How to Access Hydra Through the Terminal

In your taskbar, which should be located at the top left of your screen, click on the black box with white text that looks like “$_”.

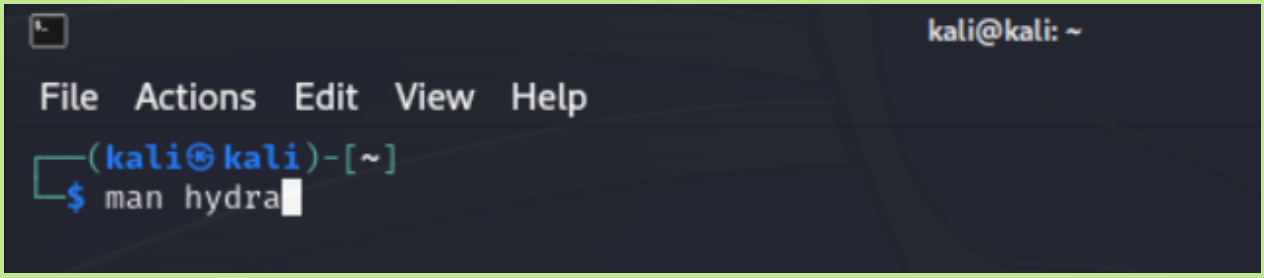


*If the black box isn't there, click on the blue dragon symbol and type “**Terminal Emulator**” into the search bar.*

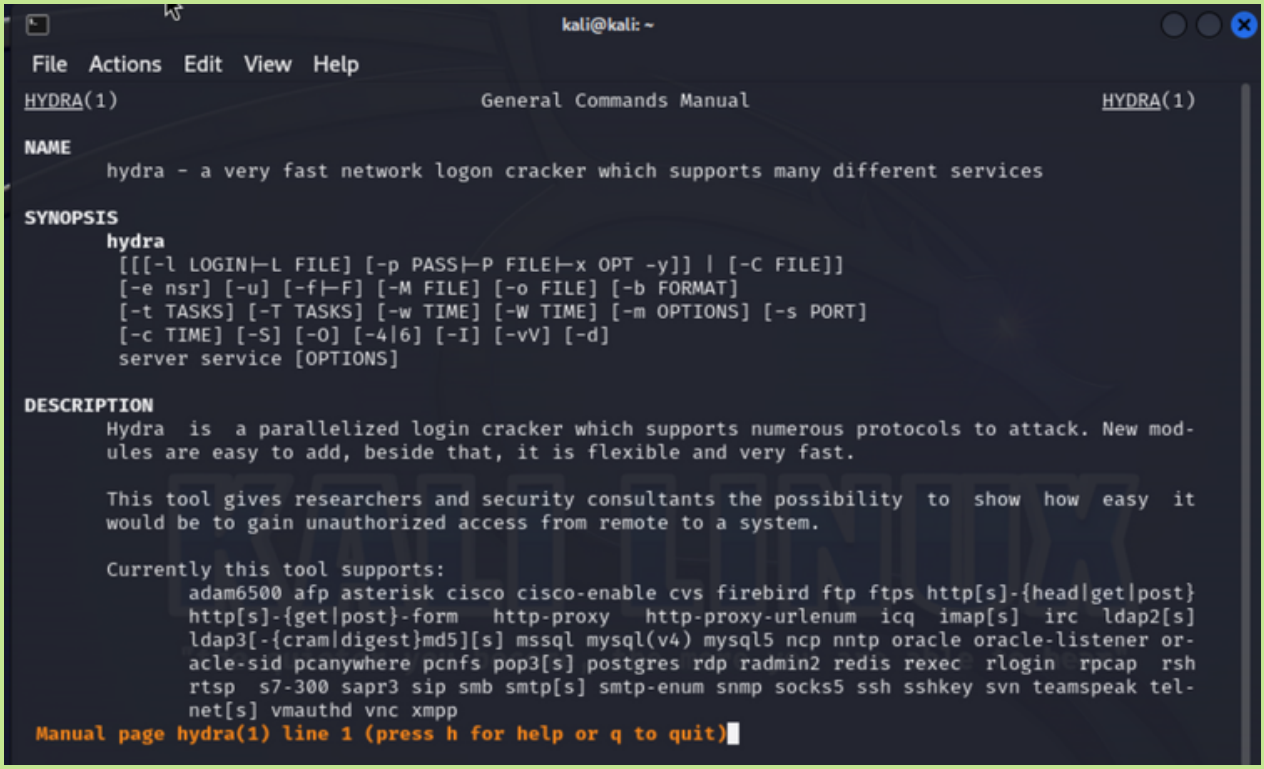


This is what the terminal looks like once it’s opened. The default user is “kali@kali”.

How to Find the Manual for Commands and Tools



The “man” command displays the manual for the command that can be run in the terminal.



Above is the user manual for the “hydra” command

Hydra: Single Attack

ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN

```
hydra -l thebestusername -p groundhog http://44.228.249.3
```

hydra -l thebestusername -p groundhog http://44.228.249.3

What is this command doing?

This command is testing if a certain login (username and password) exists at within certain server.

Hydra

- Tells the system that it's going to be using an **hydra** command

-l

- The flag to search for a username, followed by the username that is being searched for (thebestusername)

-p

- The flag to search for a password, followed by the password that is being searched for (groundhog)

http

- The service that needs to be cracked to brute force the logins

44.228.249.3

- The target IP address for the attack (tip: the IP address of a url can be found by running "ping [url]" within command prompt/terminal)

Hydra: Spray Attack

*****ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN*****

```
hydra -l users.txt -P passwords.txt -M ipaddr.txt -T 4
```

hydra -l users.txt -p passwords.txt -M ipaddr.txt -T 4

What is this command doing?

This command is testing if any combinations of a list of usernames and passwords exist within multiple target IP addresses.

Hydra

- Tells the system that it's going to be using an **hydra** command

-l

- The flag to load a list of several usernames from a file (in this case, users.txt)

-p

- The flag to load a list of several passwords from a file (in this case, passwords.txt). This list is often a predetermined list of common words and phrases used in passwords.

-M

- The flag to load a list of several target IP addresses from a file (in this case, ipaddr.txt)

-T

- The flag used to define how many of these combinations can be run simultaneously, which defines the speed of the command

Additional Resources:

Kali Linux Hydra Official Webpage:
https://www.kali.org/tools/hydra/

How to use the Hydra password-cracking tool:
https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-Hydra-password-cracking-tool?Offer=abMeterCharCount_var3

How to Use Hydra to Hack Passwords – Penetration Testing Tutorial:
https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/

How to use Kali Linux Hydra:
https://medium.com/@ibo1916a/how-to-use-kali-linux-hydra-d49cc6b50b60