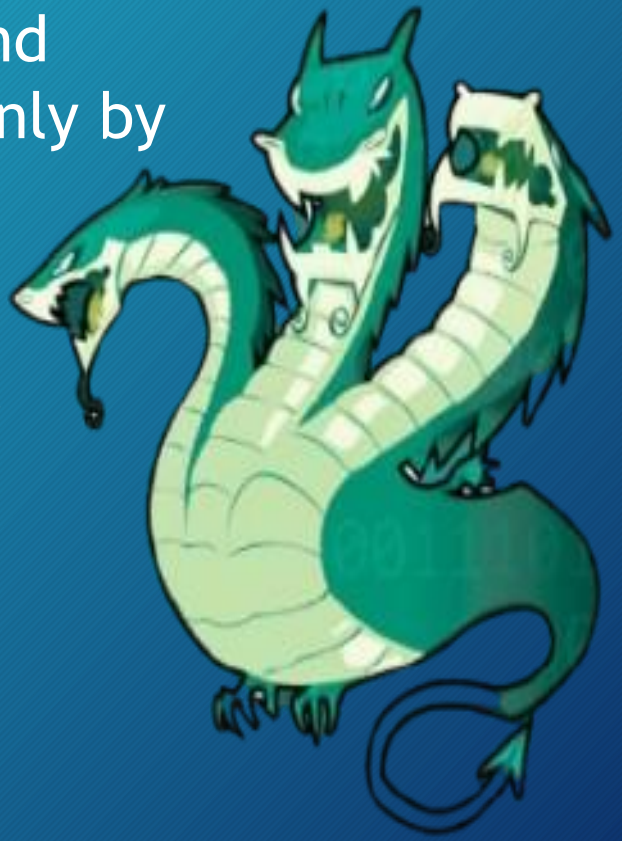
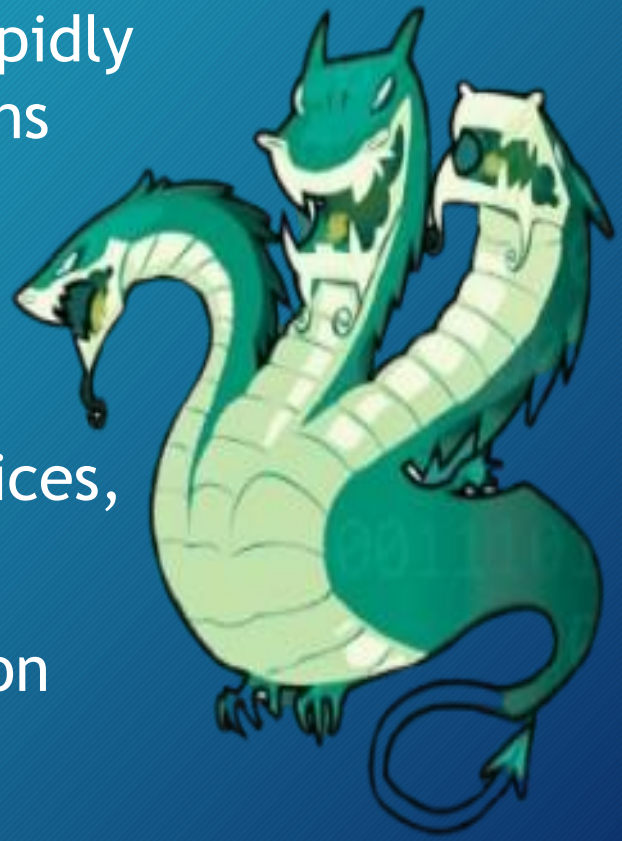
WHAT IS HYDRA

- **Hydra** is a powerful and popular tool for brute-forcing and dictionary attacks on various network services, used mainly by penetration testers, ethical hackers, and cybersecurity experts.
- It helps in testing the security of a target by attempting to log in with different username and password combinations on different protocols like HTTP, FTP, SSH, SMTP, and more.



WHAT HYDRA DOES

- **Hydra** automates the process of password guessing by rapidly attempting multiple username and password combinations against a login service
- Test for weak or default passwords.
- Perform brute-force attacks on login forms, remote services, or APIs.
- Identify potential vulnerabilities related to authentication mechanisms.



HOW TO INSTALLING HYDRA

- Hydra can be installed on most Linux distributions using the package manager

- sudo apt-get install hydra (For Debian/Ubuntu)
- sudo yum install hydra (For CentOS/RedHat)
- brew install hydra (For macOS)

BASIC SYNTAX FOR HYDRA

- hydra [options] service://target

Here :

- **Options:** Specify flags and arguments for usernames, passwords, threads, etc.
- **Service:** The protocol or service being attacked (e.g., ssh, ftp, http).
- **Target:** The IP address or domain name of the target.

Common Hydra Command Options

- -l [username]: Specifies a single username.
- -L [username_list]: Specifies a file containing a list of usernames.
- -p [password]: Specifies a single password.
- -P [password_list]: Specifies a file containing a list of passwords.
- -t [number]: Sets the number of parallel threads (default is 16).
- -s [port]: Specifies the target port (default varies by service).

Common Hydra Command Options

- -f: Stops the attack once a valid credential pair is found.
- -V: Verbose mode; displays each attempt in the console.
- -e nsr: Performs additional checks (e.g., no password, same password as username).

Common Hydra Protocols

Protocol	Command Example
SSH	`hydra -L usernames.txt -P passwords.txt ssh://target-ip`
FTP	`hydra -L usernames.txt -P passwords.txt ftp://target-ip`
HTTP Form	`hydra -L usernames.txt -P passwords.txt http-post-form "/login:username=^USER^&password=^PASS^:F=failed"`
RDP	`hydra -L usernames.txt -P passwords.txt rdp://target-ip`
SMTP	`hydra -L usernames.txt -P passwords.txt smtp://target-ip -s 587`
SNMP	`hydra -P community_strings.txt snmp://target-ip`

THANK YOU

Thank You For Giving Your Valuable Time To Us

Follow and Subscribe For More

Youtube :-
@InfoTechFly

Instagram :-
infotechfly

You will find all source code and notes on GitHub

GitHub :- infotechfly