CSE 3157: Penetration Testing Workshop

Using Hydra and xHydra for Password Attacks

By
Manjog Padhy
Asst Professor, Dept of CSE,ITER

Introduction to 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 for us, determining the correct password.
- Helps in penetration testing to identify weak passwords.
- Hydra Types- 1.CLI Based 2. GUI Based
- Hydra is preinstalled with kali Linux for both CLI (Command line Interface) and GUI (Graphical user Interface).

How Kali Linux interact with Hydra & xHydra

- CLI version installed by default in Kali Linux.
- Can be run using: hydra –h
- Provides powerful brute-force attack capabilities on various protocols like SSH, FTP, HTTP, MySQL, etc.
- Can be run using xhydra. If it does not open, install it using

```
sudo apt install hydra-gtk
```

- To launch xHydra Type: **xhydra** (This will launch the GUI interface).
- Main tabs in xHydra:

  1. Target- Select the target IP and service. (Single, A Network, List of Hosts)

  2. Password- Set the username and password list.

  3. Tuning- Adjust the number of parallel tasks.

  4. Start- Begin the attack.

- Single Target (192.168.0.102) A Network or Subnet (192.168.2.0/24)

Syntax Breakdown For Hydra

- **hydra ftp://192.168.0.2:2221 –l admin –P list.txt**

  Where ftp-> Protocol.

  192.168.0.2-> IP Address.

  2221-> Port Number in which service is running.

  -l admin-> User

  -P list.txt-> Password List.

- Options (Ethical Hacker will use very frequently in Hydra)

  -l Single User Name

  -L List of User Names

  -p Single User password

  -P List of Passwords

  -V Show Output on the Screen

  -t Parallel Tasks

  -o Output File

  -m Module Options

Relation Between IMAP and Hydra

- IMAP (Internet Message Access Protocol) is an email protocol used to authenticate users and access mailboxes. Hydra, a powerful password-cracking tool, can target IMAP to perform **brute-force attacks** on email logins. By supplying lists of usernames and passwords, Hydra systematically tries combinations to find valid credentials on an IMAP-enabled mail server.

  Example Scenario:

  You want to test the security of an email server that uses IMAP for user logins. Hydra can be used to:

- Try a **list of usernames and passwords** against the IMAP server.
- See if it can **guess valid login credentials** by brute force.
- **hydra -L users.txt -P passwords.txt 127.0.0.1 imap**

  hydra->Starts hydra Tool, -L users.txt -> Uses a File (users.txt) containing a list of user names, –P passwords.txt-> Uses a File (passwords.txt) containing a list of passwords, 127.0.0.1-> Target IP Address, imap-> Specifies the Protocol being Targeted.

Brute Force SSH Protocol Using Hydra

- **hydra ssh://192.168.0.104:2222 –L /home/ITER/temp/users.txt –P /home/ITER/temp/passwords.txt -V**
- It can find the Username and Password in highlighted section. But still it will not stop making Brute Force.
- To stop hydra to Brute Force, once it can identify the required username and password, we can use –f option. For that command is mentioned as below:

hydra ssh://192.168.0.104:2222 –L /home/ITER/temp/users.txt –P /home/ITER/temp/passwords.txt -V –f

- It might happen , when you Brute Force any service, u may have Firewall. By default hydra sends 16 username and passwords. As a result of which, if Firewall detects your IP Address , it can block you to perform Brute Force Attack.
- To overcome this , we have a mechanism to send 2 requests at a time. It is being highly recommended max(4) u can send ,so that it can bypass the Firewall.
- To achieve this ,we can issue the following command in the Terminal.

Hydra ssh://192.168.0.104:2222 –L /home/ITER/temp/users.txt –P /home/ITER/temp/passwords.txt –V –t 2

Brute Force MySQL Using Hydra

- **hydra mysql://127.0.0.1 –l root –P /home/ITER/temp/users.txt –o PassCrack –V**
- U will get The username as root and ,also password will be retrieved.
- Type ls to find a file called PassCrack, where your output would be saved.
- Then type cat passCrack to see the Username and Password.

  [3306] [mysql] host:127.0.0.1 login: root password: root
- Type clear command from the Terminal.

Thank You