Cracking Network Passwords (Hydra)

Often you may wish to obtain access to a service or password protected area on a network. Examples of this may be trying to log into a ssh service, RDP, http-get (i.e. what your router pops up with), etc. There a multitude of tools that will allow you to perform these password attacks, hydra, medusa and ncrack are popular examples. Some tools may cope with certain protocols better than others, but hydra has become a staple tool in my arsenal. You have the choice of nominating a single host name, then cycling through a password list; nominating a username list and testing a password, or a combination of both username lists and password lists.

Tool

hydra

Basic Syntax

```
hydra -l/-L <user name / user list> -p/-P <password / password list> <protocol://hostname>
```

Break Down

-l/-L : Only one of these is needed. Little l is for nominating a single username, capital is for a username list

-p/-P : Only one of these is needed again. Little p for a single password, capital p for a password list.

<protocol://hostname> : This specifies the target and protocol. For example cracking ssh on 192.168.1.1 would be ssh://192.168.1.1, while ftp on 10.1.2.3 would be ftp://10.1.2.3

Example

```
hydra -l bob -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.15  # Cycle through a wordlist trying to log in as bob over ssh on 192.168.1.1
hydra -L usernames.txt -p password  192.168.1.1 http-get / -s 80   # Cycle through a list of usernames and try and log into the router at http://192.168.1.1:80/ with the password 'password'
```

Advanced Reading

Hydra can do a lot more than mentioned here. Ton’s more protocols are also supported (although some like RDP aren’t that great to try and brute

force). Options like the ‘C’ flag allow you to use username:password combinations. https-post protocols allows you to target forms embedded in websites, etc.