**Dictionary Attacks**

**Hydra**

* Performs many different tasks, some of which include brute forcing

Hydra -l admin -P /usr/share/wordlists/fasttrack.txt -t 4 192.168.1.22 ssh

* -l # for username
* -P # to provide a passwords wordlist
* -t # to specify number of threads (keep at 4 and no higher)
* Ssh # specify which protocol to use

This will perform a brute force

**Password Spraying**

\*Would try this on a local account, not admin

Taking a known usr and pwd and attempt to authenticate across an entire network range/service

* May have compromised the credentials
* Plaintext in a config file etc.
* Pulled plaintext from different machine etc.

Trying to hit each accounts with many password attempts can raise red flags and lock you out

* This technique involves hitting each account once with this usr/pwd set

Spray.py is a script that can be used for this, it wont automate it but can be used

* Python3 spray.py 192.168.0.0/24 admin admin
  + admin admin # use these as usr/pwd

Text

Description automatically generated

This shows that .1.9 failed but .1.22 succeeded

You would then access the account via ssh

* ssh [admin@192.168.1.22](mailto:admin@192.168.1.22)
  + enter password
* logged in

A good way to check a username and password across multiple systems whilst staying under the radar of password lockouts (from multiple uses)

HW – rebuild the script with a different library and make it work for SSH and FTP

* also make it multi-threaded