

hydra tool ppt

by Alish Mahat

Submission date: 27-Apr-2025 09:53PM (UTC+0545)

Submission ID: 2658284282

File name: Hydra_AlishMahat_23000965.pptx (4.94M)

Word count: 388

Character count: 2350

Research on THC-HYDRA

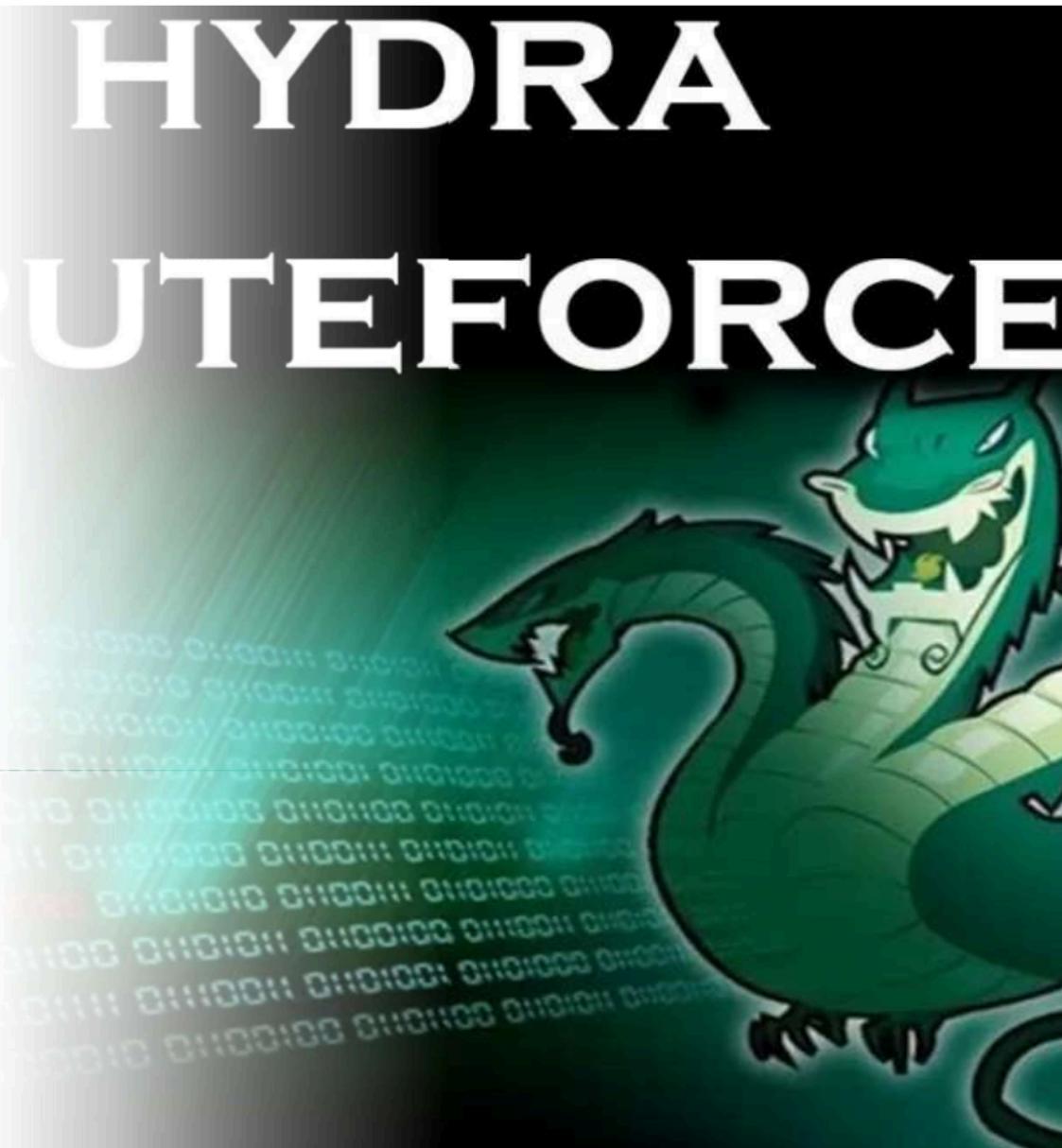
Presented by: Alish Mahat

Student ID: 23000965

Module: Security and Forensics Tools

Table of Contents

1. Introduction
2. Purpose and Applicability
3. Alternatives
4. Comparison with Medusa and Ncrack
5. Strengths
6. Weaknesses and Limitations
7. Future Enhancements
8. Demonstration and Case Study
9. Will I Use THC-Hydra?
10. Conclusion and Recommendation
11. References



```
(root㉿kali)-[~]
# hydra
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military
Syntax: hydra [[[[-l LOGIN[-L FILE] [-p PASS[-P FILE]] | [-C FILE]] [-e nsr] [-o FILE]
T][OPT]]]

Options:
-l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE  try password PASS, or load several passwords from FILE
-C FILE  colon separated "login:pass" format, instead of -L/-P options
-M FILE  list of servers to attack, one entry per line, ':' to specify port
-t TASKS  run TASKS number of connects in parallel per target (default: 16)
-U  service module usage details
-m OPT  options specific for a module
-h  more command line options (COMPLET
server  the target: DNS, IP or 192.168.1.100
service  the service to crack (see
OPT      some service modules

Supported services: adam6500 asterisk
odb mssql mysql nntp oracle-listener or
Hydra is a tool to guess/crack valid logins
Licensed under AGPL v3.0. The new version is available at
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or
purposes. (This is a wish and
laws and ethics anyway - and tell t
Example: hydra -l user -P passlist
```

Introduction

1. THC-Hydra is a powerful, fast, and flexible network login cracker.
2. It is open-source and supports numerous protocols like FTP, SSH, HTTP, RDP, etc.
3. Used to test login credentials via brute-force or dictionary attacks.

HYDRA BRUTEFORCE



Purpose and Applicability

1. Main purpose: Identify weak login credentials.
2. Used by ethical hackers, penetration testers, and security auditors.
3. Applicable for login security tests in multiple network environments.

CYBERSECURITY TOOLS USED FOR PASSWORD CRACKING

Alternatives



John The
Ripper



Hydra



Hashcat



Medusa



THC-Hydra



Cain & Abel

1. Medusa - Similar to Hydra but older and less active.
2. Ncrack - Built for SSH/RDP, limited protocol support.
3. Patator - Modular brute-force tool, slower but flexible.



Comparison with Medusa and Ncrack

1. Hydra: High-speed, protocol-rich, command-line based.
2. Medusa: Similar speed, less active development.
3. Ncrack: Specialized for SSH/RDP, fewer options, simpler interface.

A large, dark blue, multi-headed dragon with a textured, scaly appearance. It has several heads, each with a different expression. The dragon is positioned in front of a complex, glowing blue circuit board or network diagram. The circuit board features various icons, nodes, and connections, suggesting a sophisticated digital system or network. The overall aesthetic is futuristic and mysterious.

Strengths

1. Supports wide range of protocols.
2. Highly customizable and scriptable.
3. Parallel connections for fast cracking.
4. Regularly updated and widely used.

vanhauser-thc/thc-hydra

#921 RDP brute force failed with correct password

vanhauser-thc/thc-hydra

#619 Missing GET parameters and Hydra never ends

vanhauser-thc/thc-hydra

#339 Hydra marks password as valid,while it isn't

Weaknesses and Limitations

- No GUI (command-line only).
- May trigger IDS/IPS during scan.
- Requires quality wordlists to be effective.
- No built-in reporting or result visualization.

Future Enhancements

The terminal window shows the output of the THC-Hydra tool performing a password attack on a DVWA 'Brute' vulnerability. The command used was `-P rockyou 127.0.0.1 http-post-form "/DVWA/vulnerabilities/brute/index.php" -l admin -p admin`. The output lists 16 successful password combinations:

```
[+] [http-post-form] host: 127.0.0.1 login: admin password: 12345
[+] [http-post-form] host: 127.0.0.1 login: admin password: password
[+] [http-post-form] host: 127.0.0.1 login: admin password: princess
[+] [http-post-form] host: 127.0.0.1 login: admin password: 123456
[+] [http-post-form] host: 127.0.0.1 login: admin password: 123456789
[+] [http-post-form] host: 127.0.0.1 login: admin password: iloveyou
[+] [http-post-form] host: 127.0.0.1 login: admin password: 1234567
[+] [http-post-form] host: 127.0.0.1 login: admin password: rockyou
[+] [http-post-form] host: 127.0.0.1 login: admin password: 12345678
[+] [http-post-form] host: 127.0.0.1 login: admin password: abc123
[+] [http-post-form] host: 127.0.0.1 login: admin password: daniel
[+] [http-post-form] host: 127.0.0.1 login: admin password: monkey
[+] [http-post-form] host: 127.0.0.1 login: admin password: nicole
[+] [http-post-form] host: 127.0.0.1 login: admin password: babygirl
[+] [http-post-form] host: 127.0.0.1 login: admin password: lovely
[+] [http-post-form] host: 127.0.0.1 login: admin password: jessica
[*] successfully completed, 16 valid passwords found
[*] setting restore file because 1 final worker threads did not complete until end.
[*] netcat did not resolve or could not be connected
[*] netcat did not complete
[*] //github.com/vanhauser-thc/thc-hydra) finished at 2023-05-17 04:07:18
```

Demonstration and Case study

- Target: Local FTP server.
- Command: hydra -l admin -P rockyou.txt ftp://127.0.0.1
- Hydra uses a dictionary to try logins.
- Output shows success when password is found.
- This demonstrates Hydra's capability for credential testing.

```
—(kali㉿kali)-[~]
$ sudo systemctl start vsftpd

—(kali㉿kali)-[~]
$ sudo systemctl enable vsftpd
ynchronizing state of vsftpd.service with SysV service
 /usr/lib/systemd/systemd-sysv-install.
executing: /usr/lib/systemd/systemd-sysv-install enable

—(kali㉿kali)-[~]
$ sudo systemctl status vsftpd
vsftpd.service - vsftpd FTP server
 Loaded: loaded (/usr/lib/systemd/system/vsftpd.serv
 Active: active (running) since Sat 2025-04-12 20:30
 Invocation: 598cb5ef0b59472e815e8dae8abd8d3f
 Main PID: 763 (vsftpd)
```

```
—(kali㉿kali)-[~]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt ft
0.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak -
o not use in military or secret service organizations, or
egal purposes (this is non-binding, these ** ignore laws
ics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starti
25-04-12 20:52:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login
l:1/p:4), ~1 try per task
[DATA] attacking ftp://127.0.0.1:21/
[21][ftp] host: 127.0.0.1 login: admin password: adm
[21][ftp] host: 127.0.0.1 login: admin password: adm
1 of 1 target successfully completed, 2 valid passwords f
Hydra (https://github.com/vanhauser-thc/thc-hydra) finish
25-04-12 20:52:25
```



Will I Use THC-Hydra?

- YES – it's fast, reliable, and feature-rich.
- Ideal for red team and internal security testing.
- Powerful tool when used ethically and legally.



Conclusion and Recommendation

1. Hydra is a vital tool for network security testing.
2. Despite some CLI limitations, its power is unmatched.
3. Continued development ensures future-proof capability.
4. Highly recommended for professional use.

Useful Pentesting Tool

HYDRA

in Kali linux machine



References

1. <https://github.com/vanhauser-thc/thc-hydra>
2. <https://sectools.org/tool/hydra/>
3. <https://null-byte.wonderhowto.com/how-to/use-hydra-crack-remote-authentication-servers-0149619/>
4. https://linuxhint.com/hydra_tool_examples/



hydra tool ppt

ORIGINALITY REPORT

0%
SIMILARITY INDEX

0%
INTERNET SOURCES

0%
PUBLICATIONS

0%
STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes Off
Exclude bibliography On

Exclude matches Off