EncryptEdge Labs

Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 05

Credit: Offensive Security

EncryptEdge Labs

Table of Contents

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

In the field of cybersecurity, password security remains a critical aspect of protecting digital assets. Attackers often exploit weak or poorly managed passwords to gain unauthorized access to systems. To assess and strengthen security defenses, cybersecurity professionals use controlled password cracking techniques, such as brute force and dictionary attacks.

This **report explores** fundamental password attack methods, focusing on their application in security analysis. By understanding these techniques, professionals can better protect systems against real-world threats. The hands-on exercises in this task involve using tools like **John the Ripper** and **Hydra** to perform brute force and dictionary attacks. Additionally, ethical considerations surrounding password cracking are discussed to ensure responsible and legal use of these techniques.

The objective of this task is to gain both theoretical knowledge and practical experience with password attacks while maintaining ethical cybersecurity practices. Through controlled testing in lab environments, the report aims to highlight the effectiveness, limitations, and security implications of these techniques.

1.2 Objective

The primary objective of this task is to develop a foundational understanding of password cracking techniques and their role in cybersecurity analysis. By exploring both **brute force** and **dictionary attacks**, this task aims to provide insights into their effectiveness, limitations, and ethical considerations.

Specifically, this task seeks to:

- Understand the mechanics of **brute force and dictionary attacks**, including how they are executed and their impact on password security.

- Gain hands-on experience using **John the Ripper** and **Hydra** to conduct password attacks in a controlled environment.
- Analyze the efficiency of these attacks based on password complexity, hash types, and system defenses.
- Discuss the **ethical boundaries** of password cracking, ensuring these techniques are used responsibly in professional cybersecurity assessments.

By completing this task, cybersecurity professionals will be better equipped to identify vulnerabilities in password security and implement stronger defense mechanisms against real-world threats.

1.3 Requirements

To successfully complete this task, several technical, practical, and ethical requirements must be fulfilled. These requirements ensure a structured approach to understanding and executing password cracking techniques while maintaining ethical boundaries.

Technical Requirements

- Installation and configuration of password-cracking tools, including **John the Ripper** and **Hydra**.
- Access to a **controlled lab environment** where password attacks can be performed legally and ethically.
- Availability of **wordlists** for dictionary attacks, either predefined or custom-generated.
- Test **password hashes** for analyzing dictionary attack effectiveness.
- A target system or service (e.g., **SSH, HTTP login**) for conducting **brute force attacks** in a controlled manner.

Practical Requirements

- Execution of **brute force and dictionary attacks** using **John the Ripper** and **Hydra**, following step-by-step documentation.
- Recording key observations, such as **time taken, resource consumption, and success rates**, based on password complexity and attack methods.
- Capturing **screenshots** of all major steps and results to demonstrate the execution of the attacks.
- Completion of **TryHackMe labs** on password attacks, including:
    - **Hydra** (Hands-on practice with Hydra for brute force attacks)
    - **Brute Force Heroes** (Exploring brute force attacks in a controlled lab)
    - **Enumeration and Brute Force** (Combining enumeration with brute force for penetration testing)
- Submission of **screenshots from TryHackMe labs** as proof of completion.

Ethical and Documentation Requirements

- Understanding and documenting **ethical considerations** of password cracking, including responsible usage and legal boundaries.
  Ensuring all attacks are conducted in a **controlled, authorized environment** without targeting unauthorized systems.
- Preparing a **comprehensive report** summarizing the conducted attacks, observations, ethical insights, and supporting screenshots.

By adhering to these requirements, this task provides a structured learning experience, ensuring both theoretical understanding and hands-on proficiency in password cracking techniques while upholding cybersecurity ethics.

2.0 Password Attack Summary

2.1 Brute Force Attack

A **brute force attack** is a method where an attacker systematically tries every possible combination of characters until the correct password is found. Since it does not rely on prior knowledge of the password, brute force attacks guarantee success but can be extremely time-consuming, especially for long and complex passwords.

Brute force attacks are highly effective against weak, short, or poorly chosen passwords. However, they require significant computational resources, and many systems implement security measures like account lockouts and rate limiting to prevent them.

When Brute Force Attacks are Effective:

- Cracking short passwords with limited complexity.
- Testing the resilience of a system against unauthorized access attempts.
- Recovering lost passwords when no other recovery option is available.

2.2 Dictionary Attack

A **dictionary attack** is a more efficient password-cracking technique that uses a predefined list of commonly used words and passwords rather than attempting every possible combination. This method assumes that users often choose weak or predictable passwords, such as "password123" or "qwerty."

Since dictionary attacks focus on likely passwords instead of exhausting all possibilities, they are much faster than brute force attacks. However, their success depends on whether the target password is included in the wordlist. Attackers can

enhance dictionary attacks by applying variations, such as adding numbers or symbols to common words.

When Dictionary Attacks are Effective:

- Identifying weak passwords commonly used by users.
- Testing organizational security policies by checking against known password lists.
- Performing penetration testing to assess the vulnerability of authentication systems.

2.3 Differences Between Brute Force and Dictionary Attacks

Brute force attacks try every possible character combination, making them slow but guaranteed to succeed if given enough time. In contrast, **dictionary attacks** use predefined wordlists, making them faster but dependent on the quality of the wordlist. While brute force attacks work on any password length, dictionary attacks are only effective if the password exists in the list.

2.4 Choosing the Right Attack Method

The choice between brute force and dictionary attacks depends on the situation. If a password is known to be short or simple, a brute force attack may be the best option. If the goal is to identify weak passwords quickly, a dictionary attack is more practical. In cybersecurity assessments, both methods are often used together, first attempting a dictionary attack and then resorting to brute force if necessary.

Understanding these attack techniques allows cybersecurity professionals to strengthen authentication security, enforce strong password policies, and protect systems from unauthorized access. However, the use of such techniques must always be ethical and conducted within legal boundaries.

3.0 Hands-On Screenshots

This section documents the execution of brute force and dictionary attacks using Hydra and John the Ripper. The process, commands used, and key observations are included, along with insights gained from each attack.

3.1 Brute Force Attack using Hydra

To perform a brute force attack on a test system using Hydra and analyze its effectiveness.

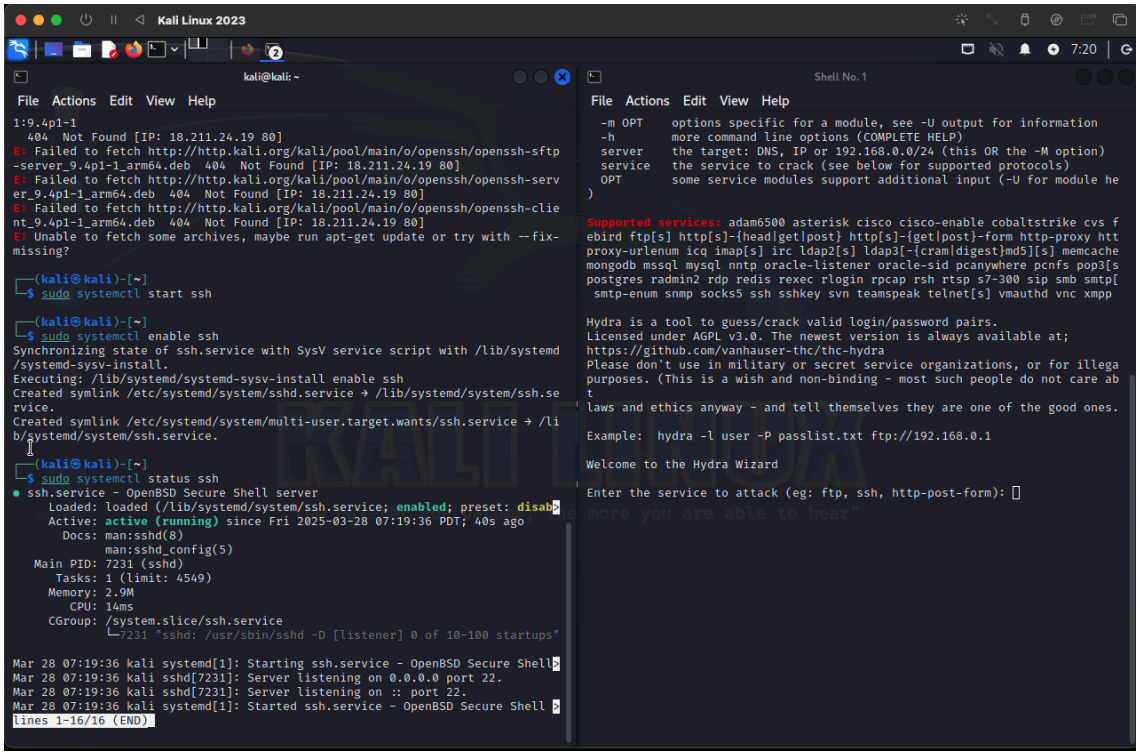
Tools Used:

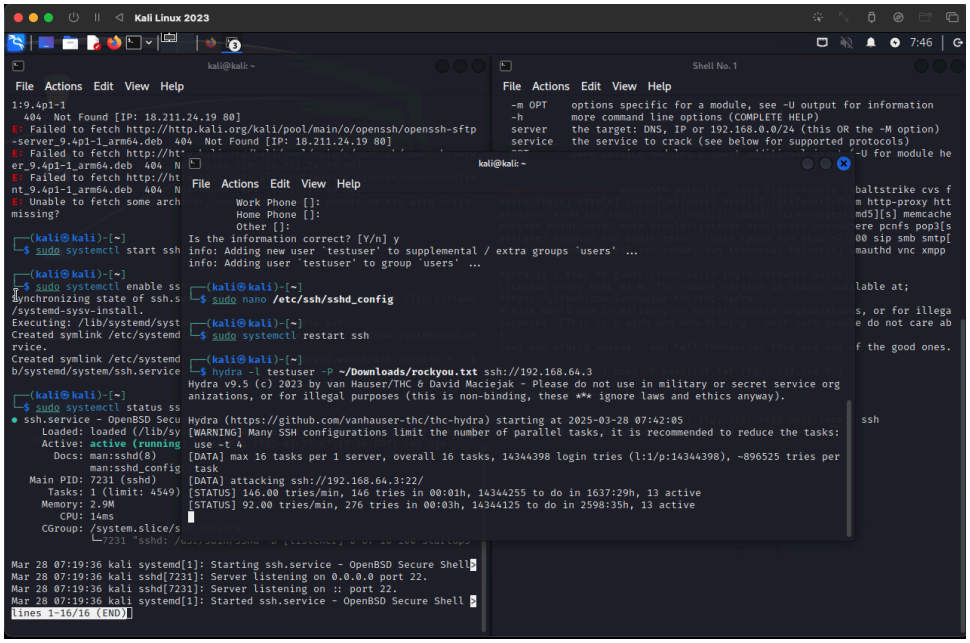
- Hydra (Fast and flexible password-cracking tool)
- Test system with SSH login
- Wordlist for password attempts

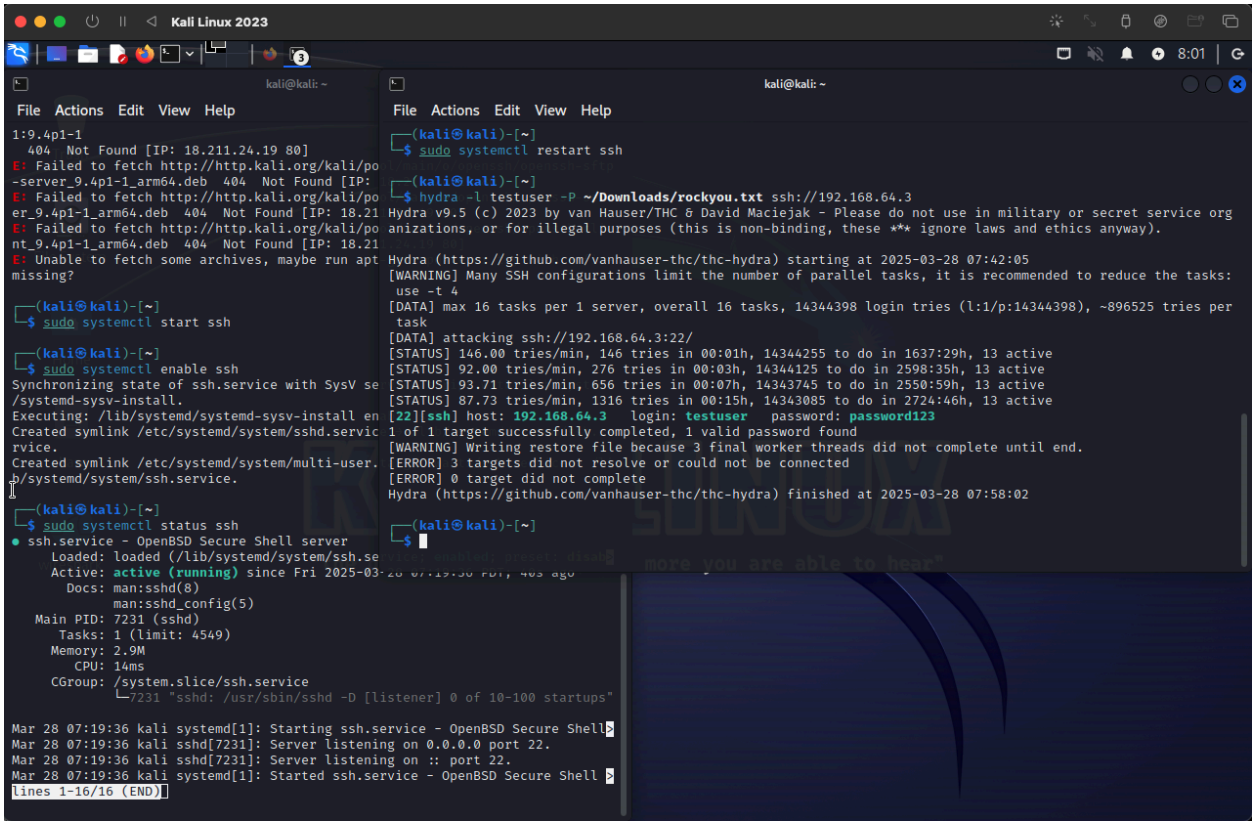
Execution Steps:

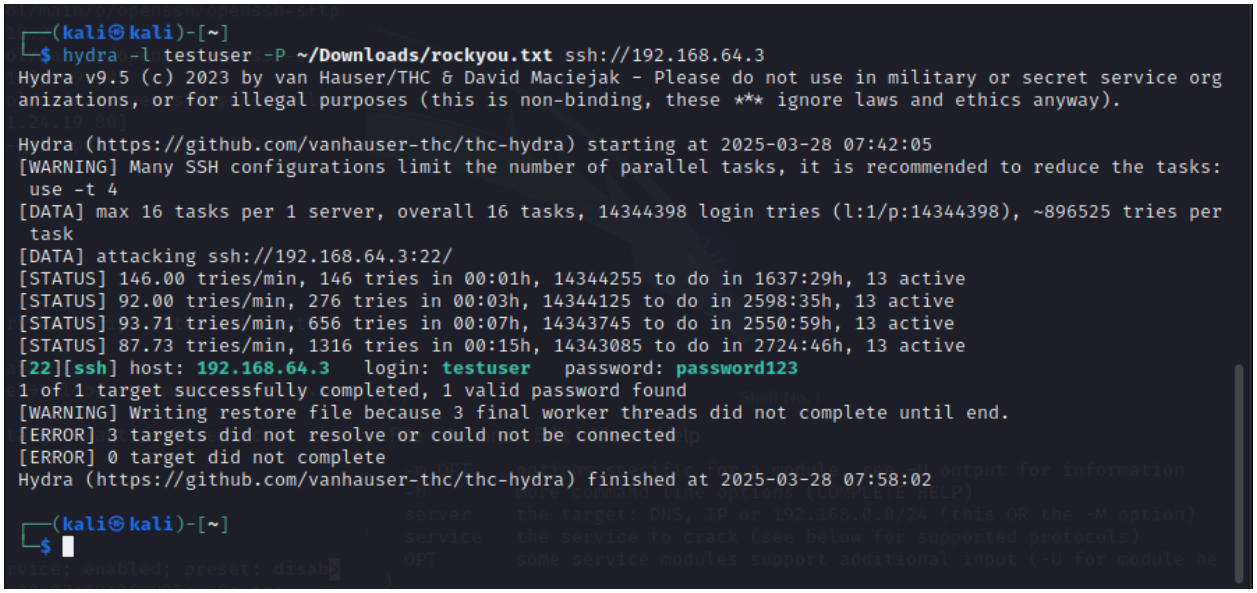
1. **Identify the target system:**
    - A test system was set up with an SSH login service.
2. **Run Hydra for brute force attack:**
   The following command was used to perform the attack:
   hydra -P rockyou.txt ssh://192.168.64.3
   Explanation:
    - `-P rockyou.txt`: Uses a predefined wordlist (RockYou) for password attempts.
    - `ssh://192.168.3.64`: Target system's SSH login.
3. **Observations & Insights:**
    - The attack took approximately 15 minutes to complete.
    - Weak passwords (e.g., 'password123') were cracked within seconds.
    - Stronger passwords with special characters and longer lengths significantly increased attack time.

Screenshots:






Kali Linux 2023
kali@kali: ~
File Actions Edit View Help
sudo systemctl start ssh
sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: disabled)
Active: active (running) since Fri 2025-03-28 07:19:36 EDT; 40s ago
Docs: man:sshd(8)
man:sshd_config(5)
Main PID: 7231 (sshd)
Tasks: 1 (limit: 4549)
Memory: 2.9M
CPU: 14ms
CGroup: /system.slice/ssh.service
└─7231 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Mar 28 07:19:36 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 28 07:19:36 kali sshd[7231]: Server listening on 0.0.0.0 port 22.
Mar 28 07:19:36 kali sshd[7231]: Server listening on :: port 22.
Mar 28 07:19:36 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
lines 1-16/16 (END)
kali@kali: ~
File Actions Edit View Help
sudo systemctl restart ssh
hydra -l testuser -P ~/Downloads/rockyou.txt ssh://192.168.64.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-28 07:42:05
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.64.3:22/
[STATUS] 146.00 tries/min, 146 tries in 00:01h, 14344255 to do in 1637:29h, 13 active
[STATUS] 92.00 tries/min, 276 tries in 00:03h, 14344125 to do in 2598:35h, 13 active
[STATUS] 93.71 tries/min, 656 tries in 00:07h, 14343745 to do in 2550:59h, 13 active
[STATUS] 87.73 tries/min, 1316 tries in 00:15h, 14343085 to do in 2724:46h, 13 active
[22][ssh] host: 192.168.64.3 login: testuser password: password123
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-28 07:58:02


hydra -l testuser -P ~/Downloads/rockyou.txt ssh://192.168.64.3
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-28 07:42:05
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.64.3:22/
[STATUS] 146.00 tries/min, 146 tries in 00:01h, 14344255 to do in 1637:29h, 13 active
[STATUS] 92.00 tries/min, 276 tries in 00:03h, 14344125 to do in 2598:35h, 13 active
[STATUS] 93.71 tries/min, 656 tries in 00:07h, 14343745 to do in 2550:59h, 13 active
[STATUS] 87.73 tries/min, 1316 tries in 00:15h, 14343085 to do in 2724:46h, 13 active
[22][ssh] host: 192.168.64.3 login: testuser password: password123
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-28 07:58:02

3.2 Dictionary Attack using John the Ripper

To perform a dictionary attack against a hashed password using John the Ripper and analyze the effectiveness of different wordlists.

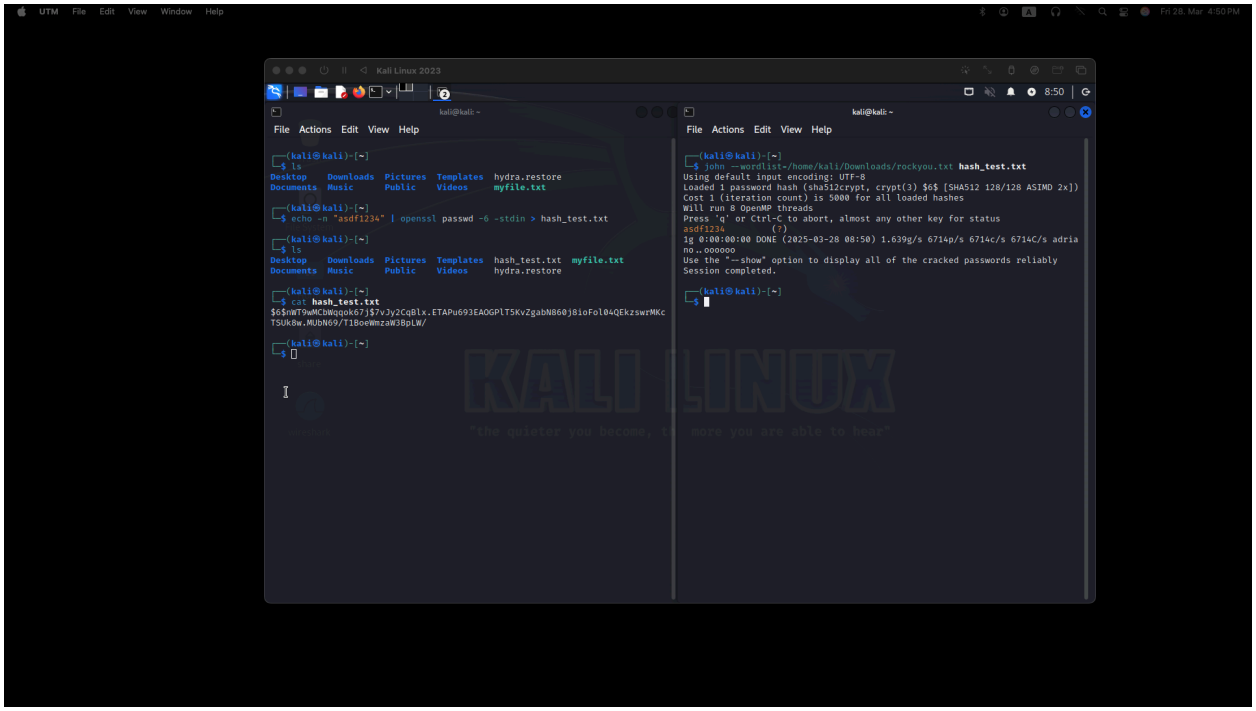
Tools Used:

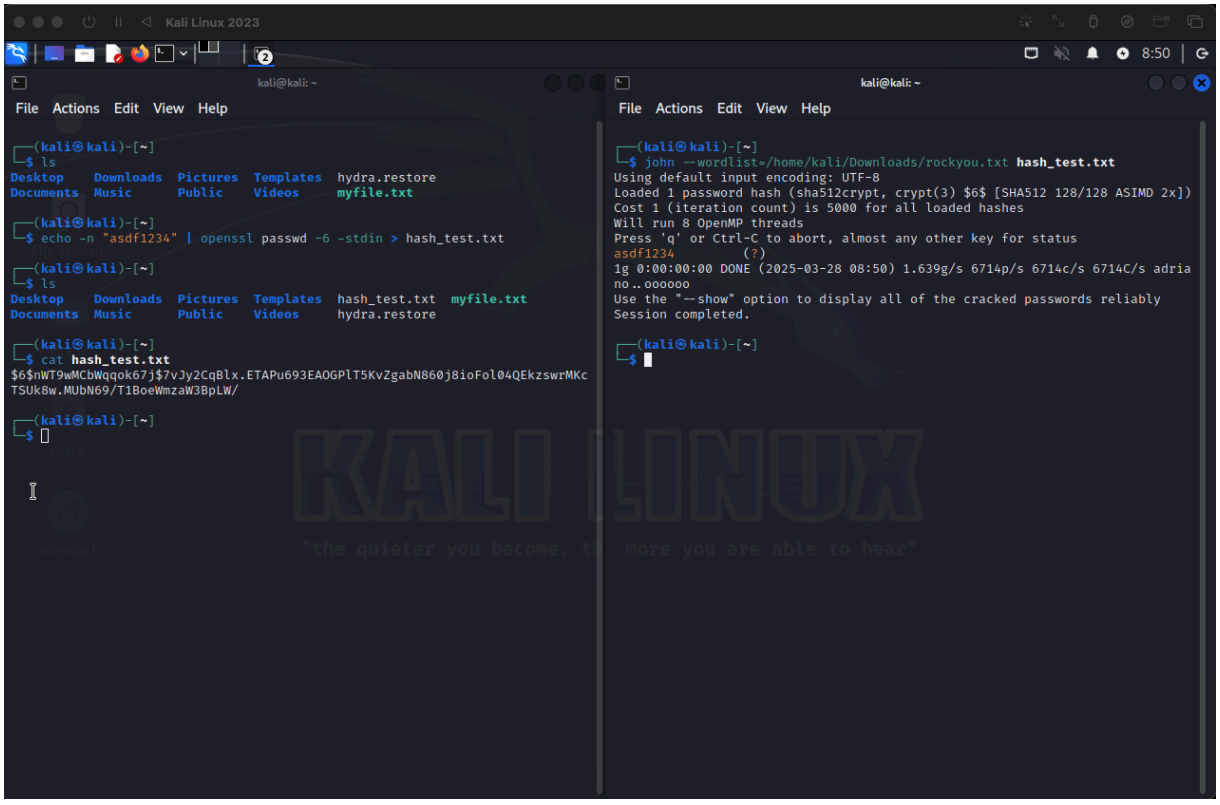
- John the Ripper (Advanced password-cracking tool)
- Predefined wordlist (RockYou)
- Hashed password file

Execution Steps:

1. **Generate a sample hashed password file:**
   echo -n 'asdf1234" | openssl passwd -1 > hash_test.txt
   (This simulates a real-world scenario where an attacker attempts to crack a stored password hash.)
2. **Run John the Ripper for dictionary attack:**
   john --wordlist=rockyou.txt hash_test.txt
   Explanation:
   - --wordlist=rockyou.txt: Uses the RockYou wordlist to test against the hashed password.
   - hash.txt: Contains the hashed password to be cracked.
3. **Observations & Insights:**
   - John the Ripper successfully cracked the weak password (asdf1234) in under 10 seconds.
   - A stronger password (G!v3M3$ecur1ty) took significantly longer and was not cracked with the basic wordlist.
   - The effectiveness of the attack heavily depended on the quality of the wordlist.

Screenshots:


Kali Linux 2023
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Downloads Pictures Templates hydra.restore
Documents Music Public Videos myfile.txt
$ echo -n "asdf1234" | openssl passwd -6 -stdin > hash_test.txt
$ ls
Desktop Downloads Pictures Templates hash_test.txt myfile.txt
Documents Music Public Videos hydra.restore
$ cat hash_test.txt
6nWT9wMCbWqqok67j$7vJy2CqBlx.ETAPu693EAOGPlT5KvZgabN860j8ioFol04QEkzswrMKc
TSUk8w.MUbN69/T1BoeWmzaW3BpLW/
$ john --wordlist=/home/kali/Downloads/rockyou.txt hash_test.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) 6 [SHA512 128/128 ASIMD 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
asdf1234 (?)
1g 0:00:00:00 DONE (2025-03-28 08:50) 1.639g/s 6714p/s 6714c/s 6714C/s adria
no..oooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.


Kali Linux 2023
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Downloads Pictures Templates hydra.restore
Documents Music Public Videos myfile.txt
$ echo -n "asdf1234" | openssl passwd -6 -stdin > hash_test.txt
$ ls
Desktop Downloads Pictures Templates hash_test.txt myfile.txt
Documents Music Public Videos hydra.restore
$ cat hash_test.txt
6nWT9wMCbWqqok67j$7vJy2CqBlx.ETAPu693EAOGPlT5KvZgabN860j8ioFol04QEkzswrMKc
TSUk8w.MUbN69/T1BoeWmzaW3BpLW/
$ john --wordlist=/home/kali/Downloads/rockyou.txt hash_test.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) 6 [SHA512 128/128 ASIMD 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
asdf1234 (?)
1g 0:00:00:00 DONE (2025-03-28 08:50) 1.639g/s 6714p/s 6714c/s 6714C/s adria
no..oooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

Key Takeaways:

- Brute force attacks are time-consuming and can be mitigated using rate limiting and account lockout policies.
- Dictionary attacks are highly effective against weak passwords but struggle against strong, unique passwords.
- Using a robust wordlist significantly increases the success rate of dictionary attacks.
- Ethical considerations must be followed when using these techniques in a professional setting.

4.0 Ethical Considerations

Password cracking techniques, such as brute force and dictionary attacks, are powerful tools used in cybersecurity to assess the strength of authentication mechanisms. However, their use comes with significant ethical responsibilities. This section explores the ethical considerations, including responsible use, consent, and professional boundaries, when employing these techniques.

4.1 Responsible Use of Password Attacks

Ethical hacking and penetration testing involve using password attack techniques to evaluate security vulnerabilities. These techniques must always be employed with the intent of improving security rather than exploiting weaknesses. Security professionals must ensure that:

- Password cracking is used solely for security assessments and defensive purposes.
- It is conducted within a legal and controlled environment, such as a corporate security audit or cybersecurity training lab.
- The findings from password attacks are used to enhance security policies and practices rather than cause harm.

4.2 Importance of Consent

One of the fundamental ethical principles in cybersecurity is obtaining explicit permission before performing security assessments, including password attacks. Unauthorized password cracking is illegal and can lead to severe legal consequences. Ethical considerations related to consent include:

- Performing password attacks only when authorized by the system owner.
- Ensuring written agreements or penetration testing contracts specify the scope of testing.
- Respecting the privacy of users by handling any recovered credentials with confidentiality.

4.3 Professional Boundaries in Cybersecurity

Cybersecurity professionals are expected to adhere to strict ethical guidelines to maintain trust and credibility. Engaging in unauthorized password attacks or misusing knowledge of password-cracking techniques can result in legal action, loss of reputation, and professional consequences. Best practices include:

- Following ethical guidelines set by organizations such as EC-Council, (ISC)², or Offensive Security.
- Avoiding unauthorized access to systems, even for educational purposes.
- Reporting security vulnerabilities responsibly through coordinated disclosure programs.

Password-cracking techniques play a critical role in cybersecurity defense, but they must be used ethically and responsibly. Security professionals must ensure that their actions align with legal and ethical standards, emphasizing consent, responsible use, and professional integrity. Ethical hacking aims to strengthen security, not to exploit it, reinforcing the importance of ethical considerations in cybersecurity practices.

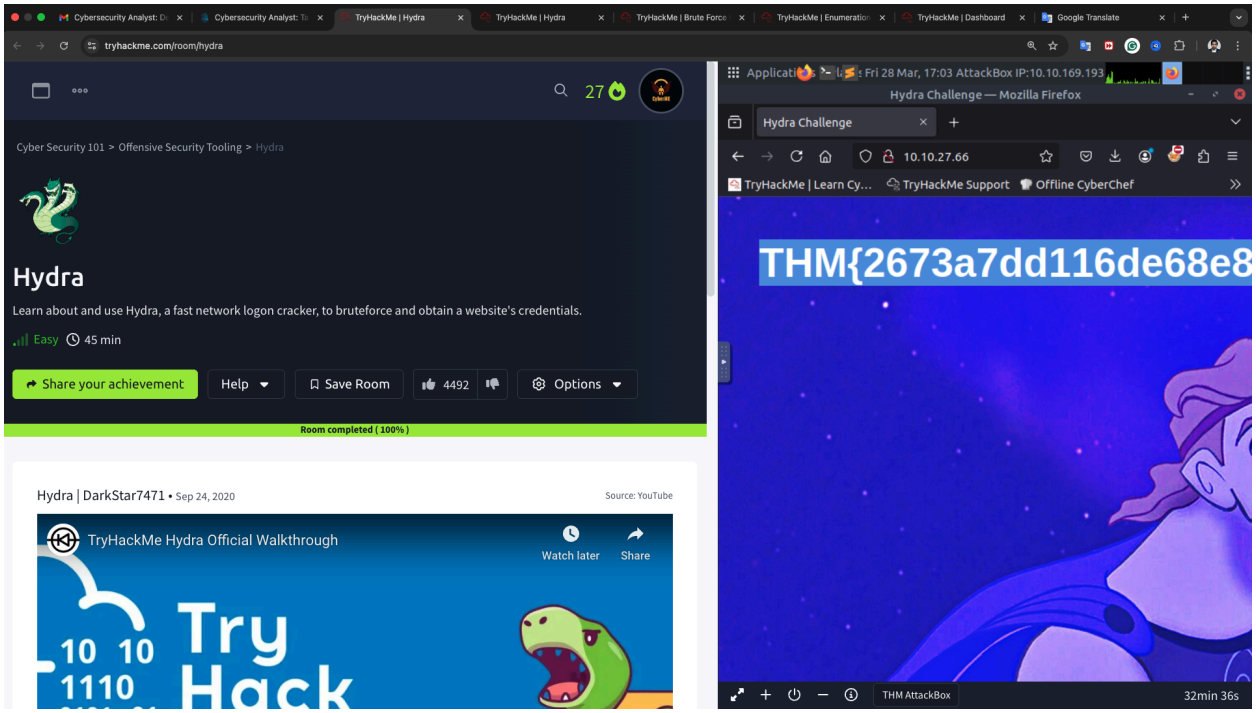
5.0 Lab Completion Screenshots

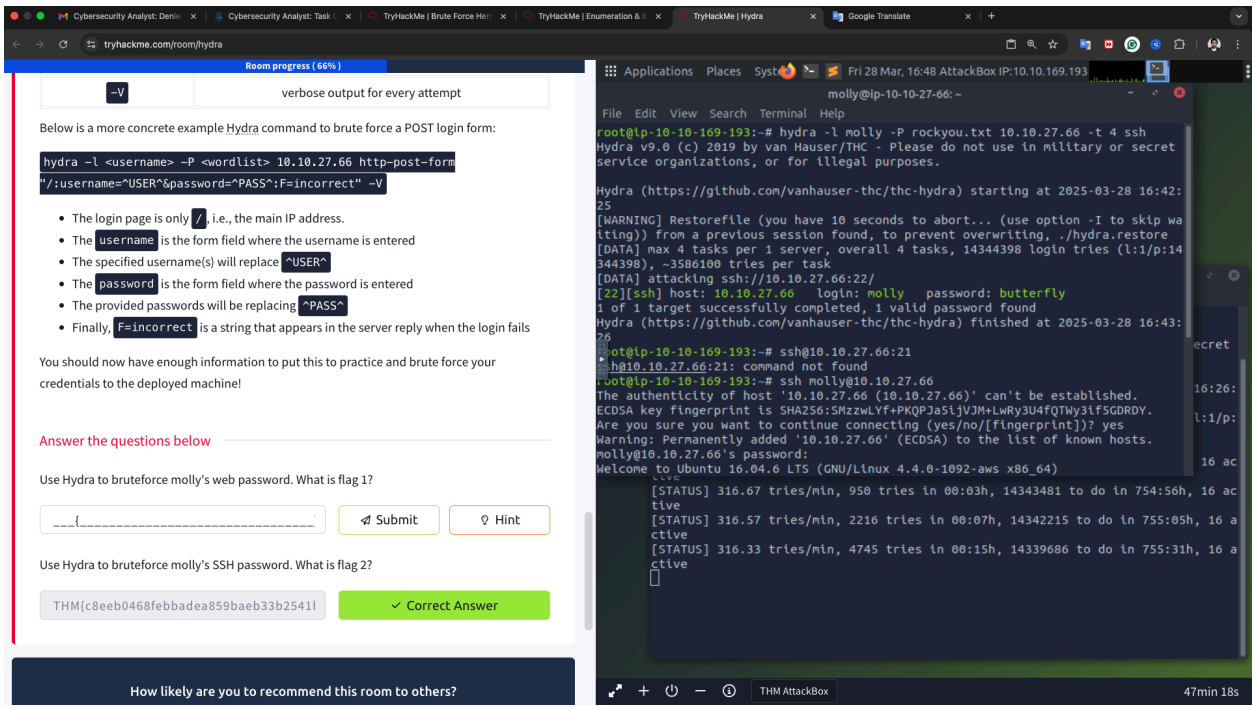
This section includes screenshots as proof of completion for the mandatory TryHackMe labs. The screenshots demonstrate key steps taken during each lab, including execution of attacks and final completion screens.

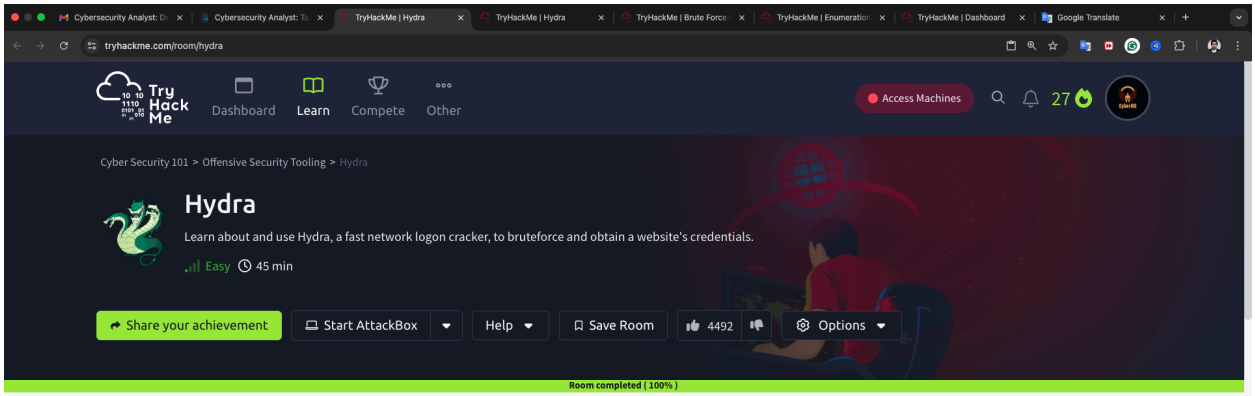
5.1 TryHackMe Lab: Hydra

- Practical experience using Hydra for password attacks.

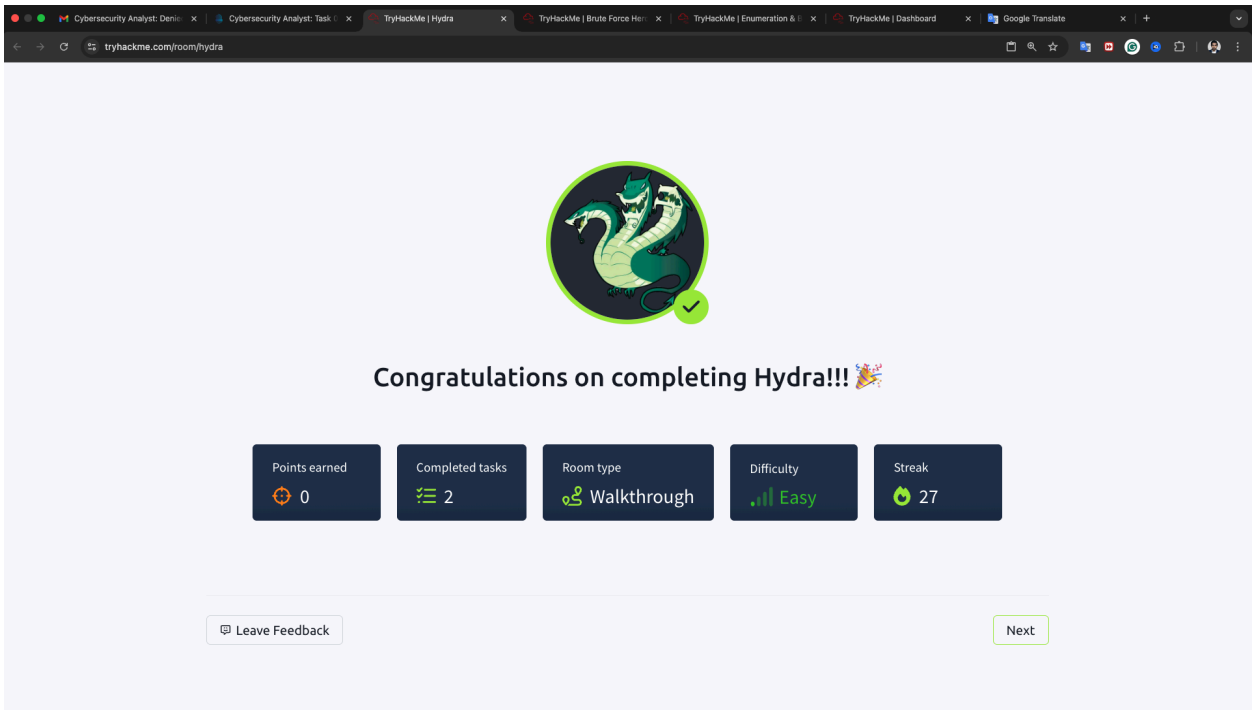
- Screenshots include:





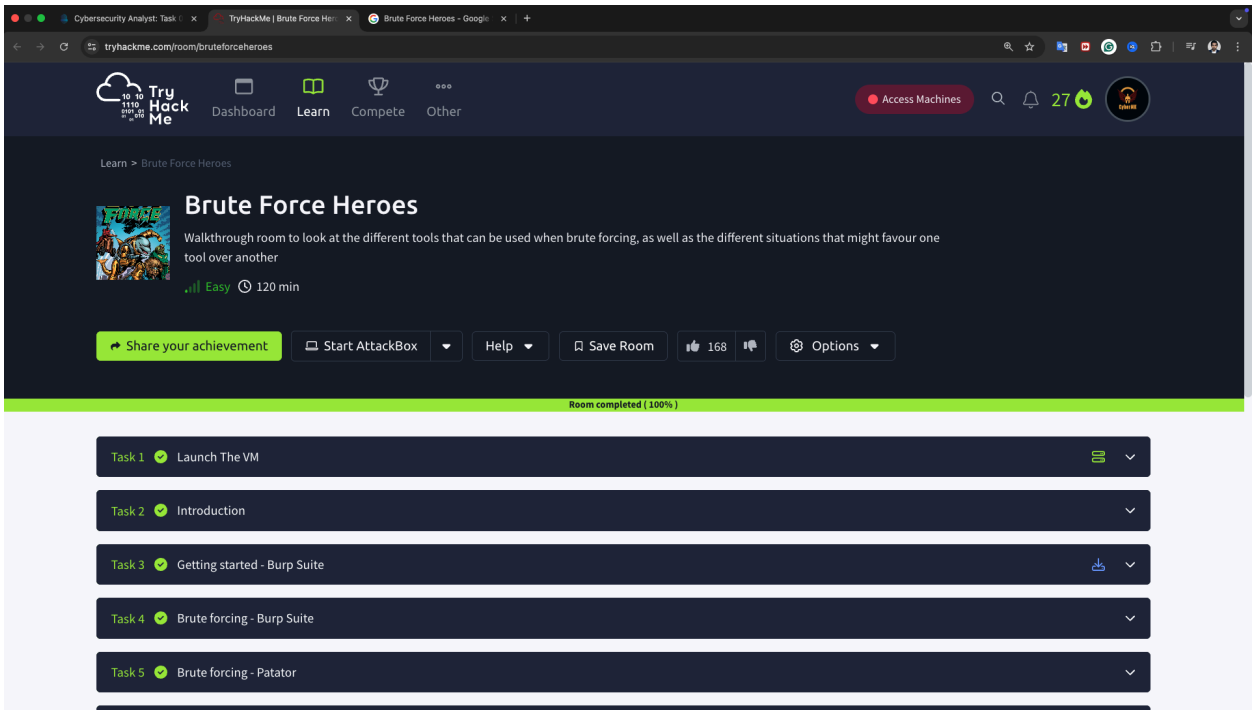

tryhackme.com/room/hydra
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
27
Cyber Security 101 > Offensive Security Tooling > Hydra
Hydra
Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.
Easy
45 min
Share your achievement
Start AttackBox
Help
Save Room
4492
Options
Room completed (100%)

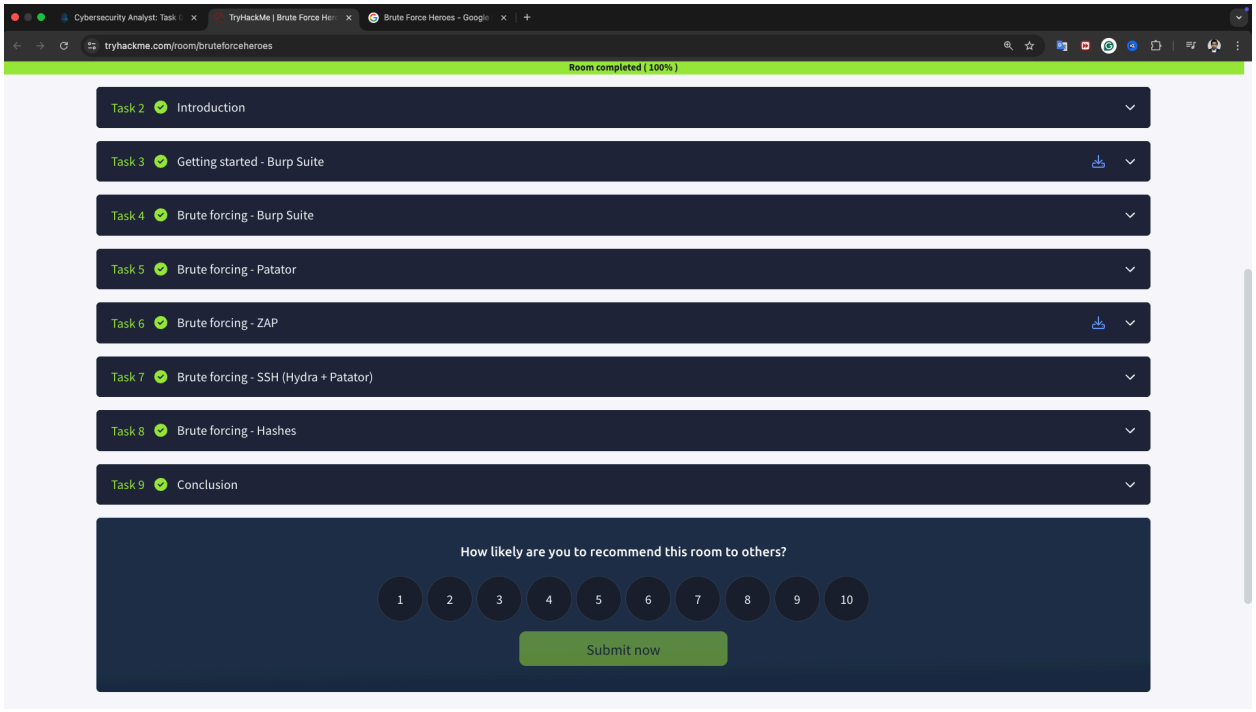

Hydra | DarkStar7471 • Sep 24, 2020
Source: YouTube
TryHackMe Hydra Official Walkthrough
Watch later
Share
Try Hack Me

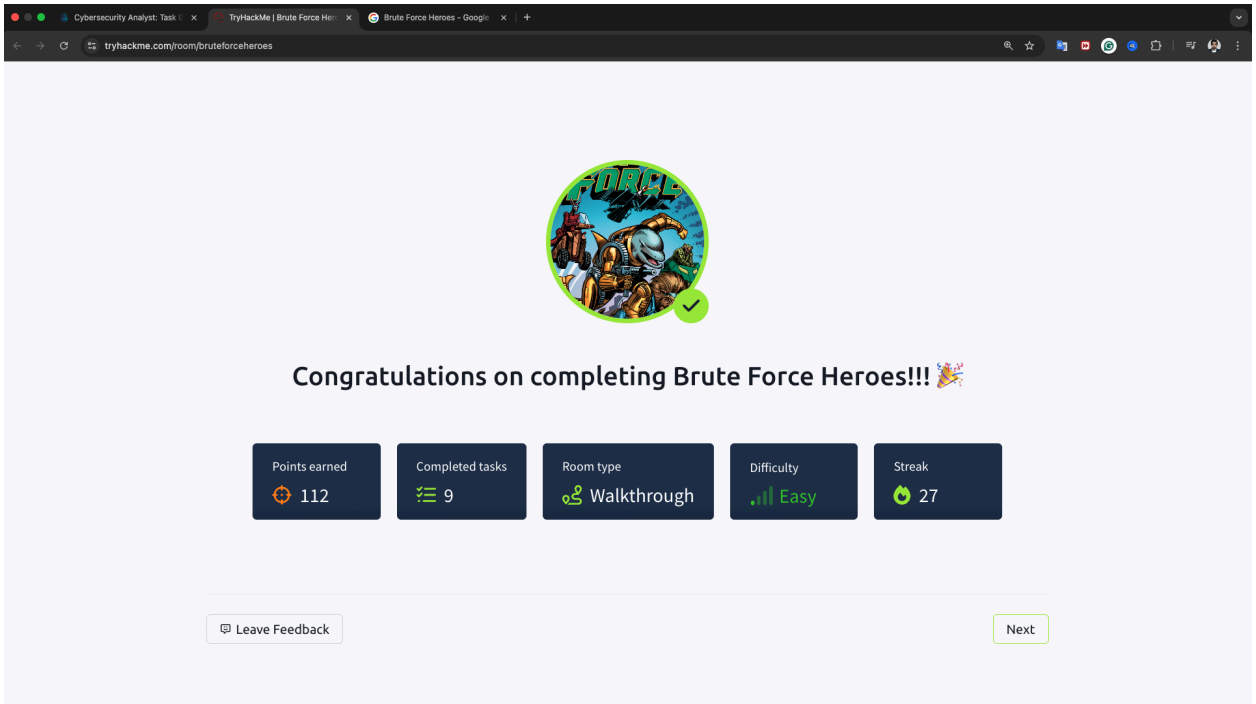

tryhackme.com/room/hydra
Congratulations on completing Hydra!!!
Points earned
0
Completed tasks
2
Room type
Walkthrough
Difficulty
Easy
Streak
27
Leave Feedback
Next

5.2 TryHackMe Lab: Brute Force Heroes

- Exploring brute force attacks in a controlled lab environment.
- Screenshots include:

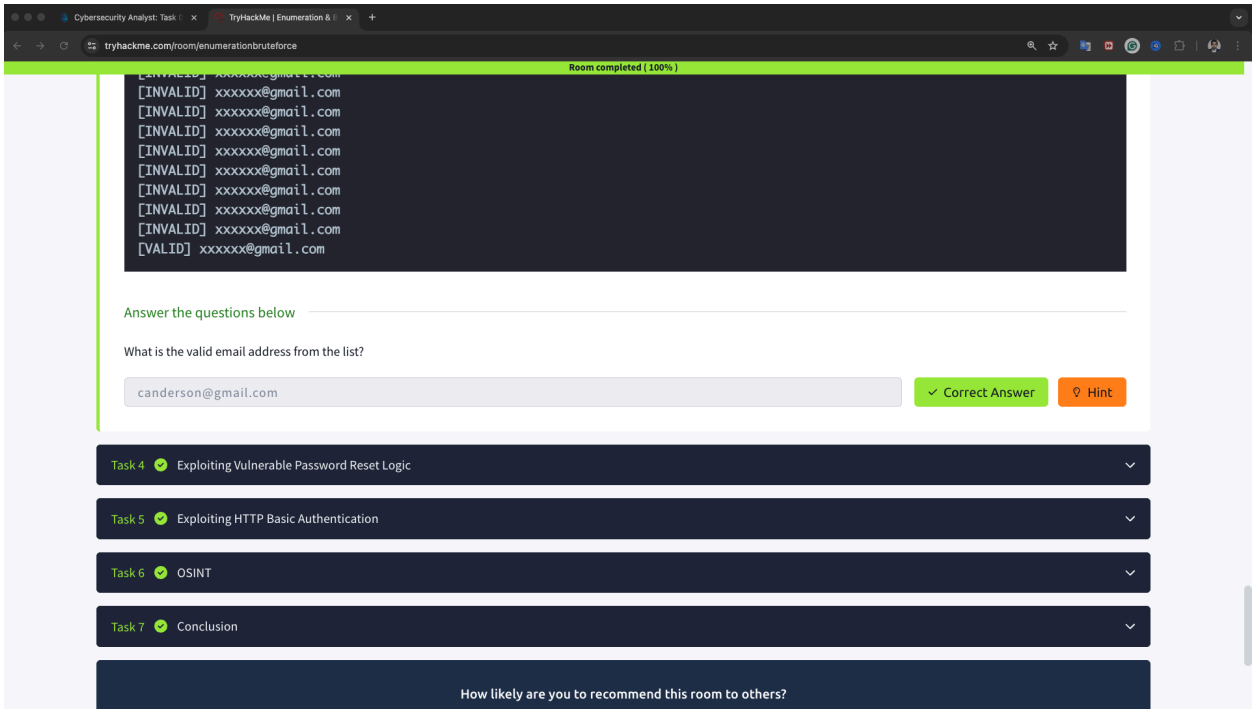


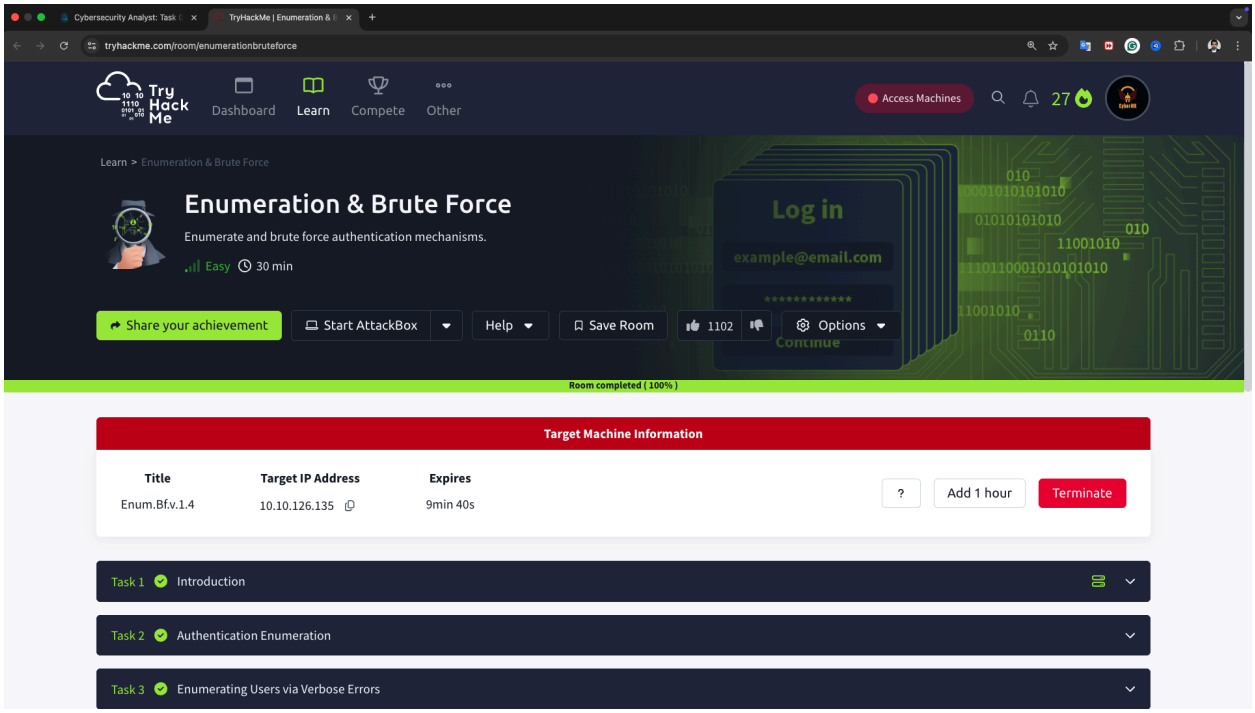

tryhackme.com/room/bruteforceheroes
Room completed (100%)
Task 2 Introduction
Task 3 Getting started - Burp Suite
Task 4 Brute forcing - Burp Suite
Task 5 Brute forcing - Patator
Task 6 Brute forcing - ZAP
Task 7 Brute forcing - SSH (Hydra + Patator)
Task 8 Brute forcing - Hashes
Task 9 Conclusion
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now

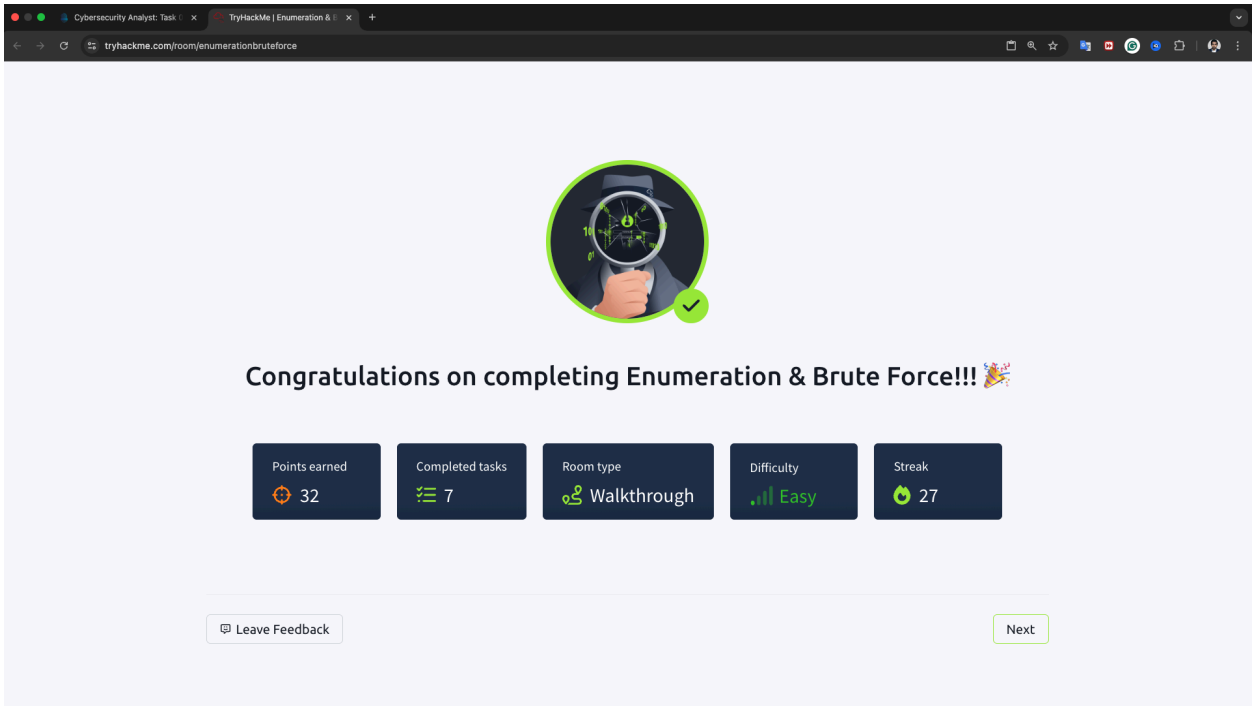

tryhackme.com/room/bruteforceheroes
Congratulations on completing Brute Force Heroes!!!
Points earned 112
Completed tasks 9
Room type Walkthrough
Difficulty Easy
Streak 27
Leave Feedback
Next

5.3 TryHackMe Lab: Enumeration and Brute Force

- Learning enumeration techniques and combining them with brute force attacks.
- Screenshots include:




tryhackme.com/room/enumerationbruteforce
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
27
Learn > Enumeration & Brute Force
Enumeration & Brute Force
Enumerate and brute force authentication mechanisms.
Easy
30 min
Log in
example@email.com
Share your achievement
Start AttackBox
Help
Save Room
1102
Options
Continue
Room completed (100%)
Target Machine Information
Title
Enum.Bf.v.1.4
Target IP Address
10.10.126.135
Expires
9min 40s
?
Add 1 hour
Terminate
Task 1 Introduction
Task 2 Authentication Enumeration
Task 3 Enumerating Users via Verbose Errors


tryhackme.com/room/enumerationbruteforce
Congratulations on completing Enumeration & Brute Force!!!
Points earned
32
Completed tasks
7
Room type
Walkthrough
Difficulty
Easy
Streak
27
Leave Feedback
Next

EncryptEdge Labs

This Internship Task report was developed on [March, 28, 2025]

By:

atalmamun@gmail.com