TryHackMe - Tutorial Machine Documentation

This document provides a comprehensive guide for setting up and completing the **Tutorial** machine on TryHackMe. The process includes configuring the VPN, securing the connection, and performing the required steps to complete the challenge.

Table of Contents

---

1. Prerequisites

Software and Hardware Requirements:
- **Operating System:** Kali Linux or Parrot Security OS.
- **Network Access:** Internet connection to access TryHackMe.
- **TryHackMe Account:** A registered account on [TryHackMe](https://tryhackme.com/).

Required Tools:
- SSH access to the machine.
- Basic packages: `nano`, `curl`, `git`, `openvpn`.

Cloning the Repository
To access the scripts and documentation, clone this GitHub repository:

```
git clone https://github.com/fartaviao/tryhackme-tutorial/.git
cd tryhackme-tutorial
```

---

2. Repository Structure

```
tryhackme-tutorial/
├── README.md              # Introduction and overview
├── tutorial.md            # Main Documentation
├── tutorial-writeup.pdf   # Writeup
├── Scripts/
│   ├── safevpn-thm.sh     # Security script for VPN
└── Screenshots/           # Visual references
    ├── Screenshot-01.png
    ├── Screenshot-02.png
    ├── Screenshot-03.png
    ├── Screenshot-04.png
    ├── Screenshot-05.png
    ├── Screenshot-06.png
    ├── Screenshot-07.png
    ├── Screenshot-08.png
    ├── Screenshot-09.png
    └── Screenshots.md
```

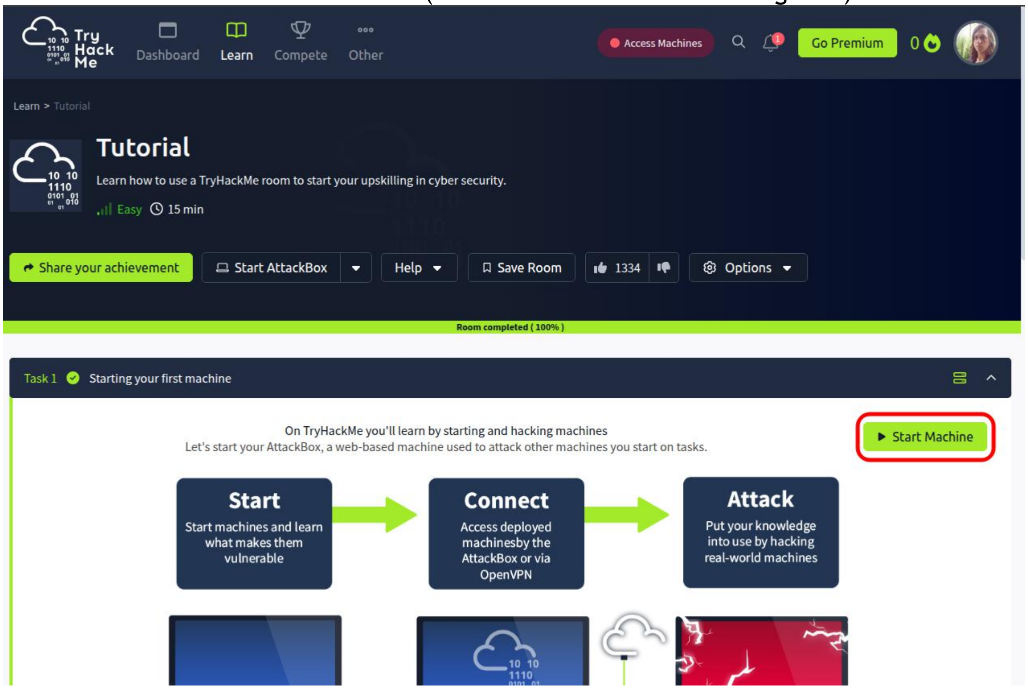
---

3. Step 1: Setting Up TryHackMe VPN

The first step is to establish a secure connection with the TryHackMe platform using OpenVPN.

**Steps:

Access TryHackMe and Join the Tutorial Machine
1. **Log in to TryHackMe:**
   - Visit [TryHackMe](https://tryhackme.com/) and log in.
2. **Join the Tutorial Machine:**
   - Search for the *room* named **Tutorial**.
   - Click on **Join Room** to participate.
   - Then click on **Start Machine** (wait around 1 min to the target IP)



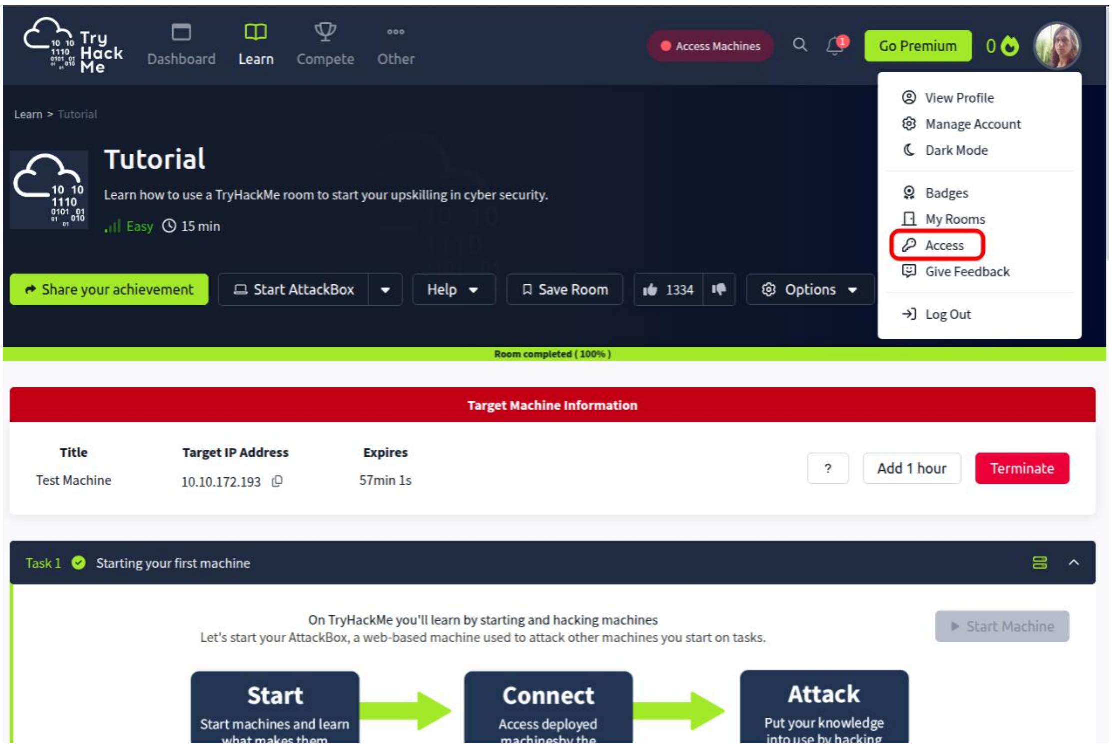
Tutorial

Learn how to use a TryHackMe room to start your upskilling in cyber security.

Starting your first machine

On TryHackMe you'll learn by starting and hacking machines
Let's start your AttackBox, a web-based machine used to attack other machines you start on tasks.

Download the VPN Configuration File
To connect to TryHackMe machines, we need a **VPN**. Follow these steps:
1. **Access the VPN settings:**
   - Click on your **profile** at the top-right corner of TryHackMe.
   - Select **Access**.



Tutorial

Learn how to use a TryHackMe room to start your upskilling in cyber security.

Easy 15 min

Target Machine Information

Title	Target IP Address	Expires
Test Machine	10.10.172.193	57min 1s

Task 1 Starting your first machine

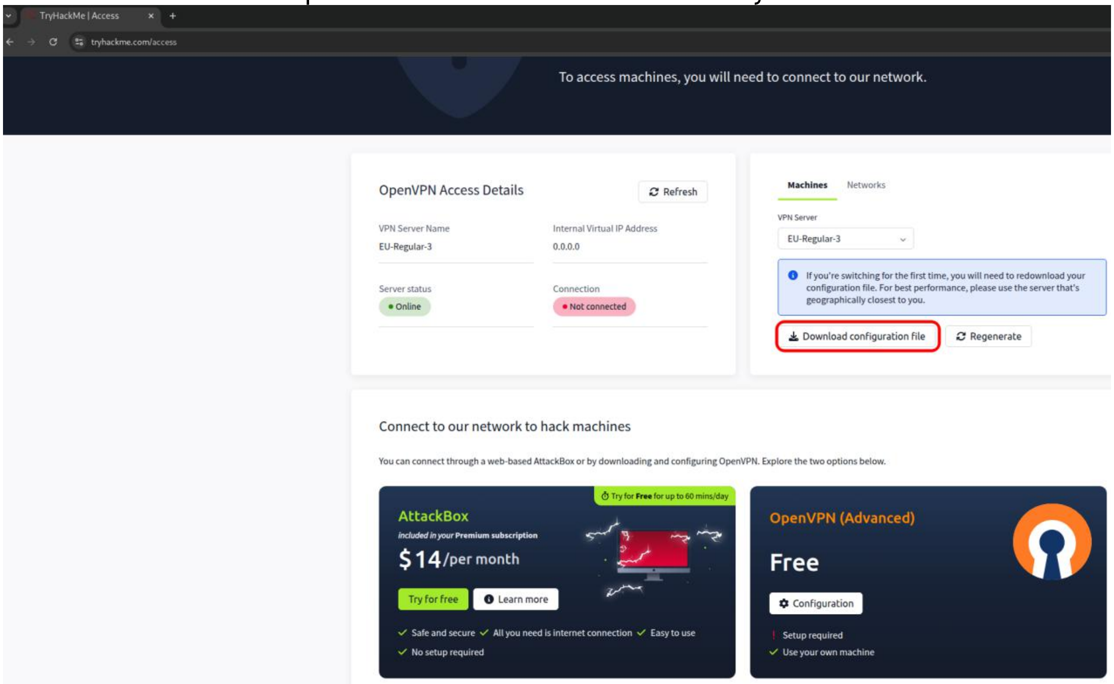
On TryHackMe you'll learn by starting and hacking machines
Let's start your AttackBox, a web-based machine used to attack other machines you start on tasks.

Start machines and learn what makes them

Access deployed machinesby the

Put your knowledge into use by hacking

2. **Download the configuration file:**
   - In the VPN section, choose **Download My Configuration File**.
   - The file with the `.ovpn` extension will be downloaded to your `Downloads` folder.



To access machines, you will need to connect to our network.

OpenVPN Access Details

VPN Server Name	Internal Virtual IP Address
EU-Regular-3	0.0.0.0

Server status	Connection
● Online	● Not connected

VPN Server: EU-Regular-3

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

Connect to our network to hack machines

You can connect through a web-based AttackBox or by downloading and configuring OpenVPN. Explore the two options below.

AttackBox
Try for Free for up to 60 mins/day
Included in your Premium subscription
$14/per month
✓ Safe and secure ✓ All you need is internet connection ✓ Easy to use
✓ No setup required

OpenVPN (Advanced)
Free
! Setup required
✓ Use your own machine

Connect Kali Linux or Parrot Security to TryHackMe via VPN

1. **Open a terminal.**
2. **Navigate to the folder where the file was downloaded:**

```
cd ~/Downloads
ls
```

   - You should see a file with the `.ovpn` extension (e.g., `<youruser.ovpn>` with the name of your user).
3. **For be more organized we can crete the following structure ~/Downloads/TryHackMe/Tutorial/OpenVPN**

```
mkdir -p TryHackMe/Tutorial/OpenVPN
ls -R TryHackMe
```

   - Move the .ovpn file to the OpenVPN location

```
mv youruser.ovpn TryHackMe/Tutorial/OpenVPN
cd TryHackMe/Tutorial/OpenVPN
ls
```

4. **Run the following command to connect to the VPN:**

```
sudo openvpn <youruser.ovpn>
```

   - Enter your password when prompted.
   - If the connection is successful, you will see a message indicating that a new network interface `tun0` has been created.

Verify Connectivity with the TryHackMe Machine

1. **Open a new terminal and run:**

```
ip a
```

   - Look for the `tun0` interface, which should have an assigned IP address.
2. **Check the connection to the machine:**
   - Find the machine's IP address on TryHackMe.
   - Run a ping test:

```
ping -c4 <MACHINE_IP>
```

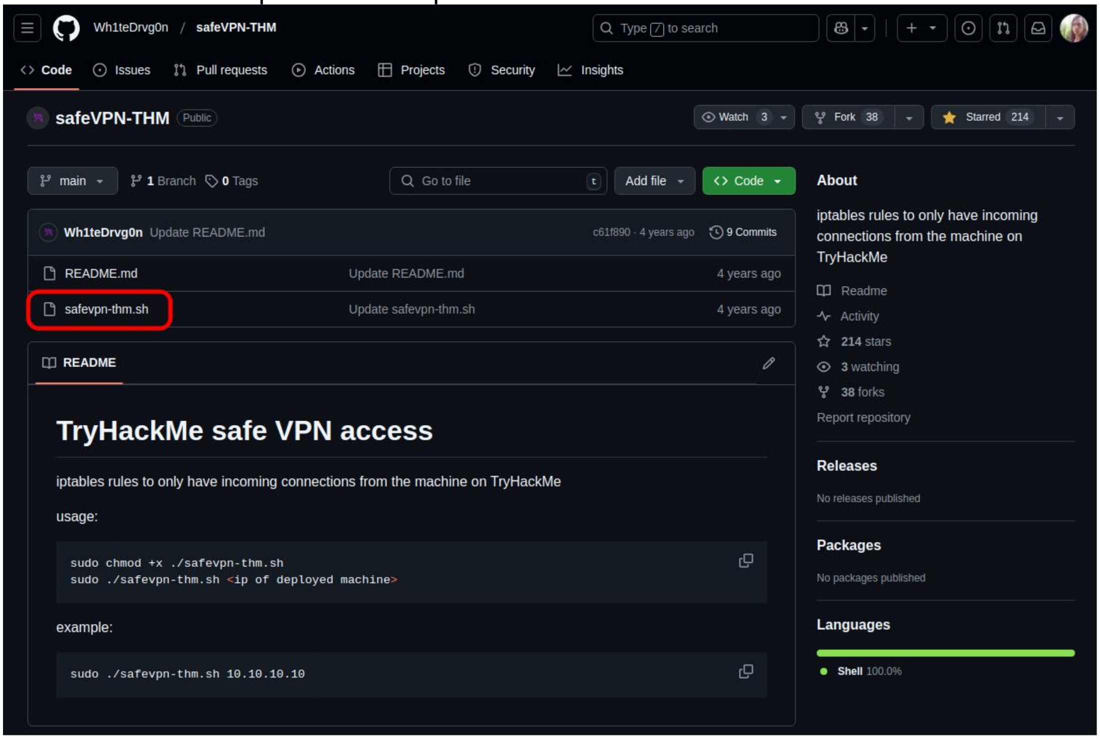
   - If you receive responses, it means the VPN is working correctly.

---

4. Step 2: Securing Your Connection

For security reasons, we can restrict our machine's access to only the machine of TryHackMe VPN using `iptables`.

1. **Download the security script:**
   - Get the "Wh1teDrvg0n" Script on GitHub to ensure security in your network:
   - Open a browser and search for *White Dragon VPN Safe* on Google.
   - Download the script from `safevpn-thm.sh` on GitHub.



README.md	Update README.md	4 years ago
safevpn-thm.sh	Update safevpn-thm.sh	4 years ago

About

iptables rules to only have incoming connections from the machine on TryHackMe

TryHackMe safe VPN access

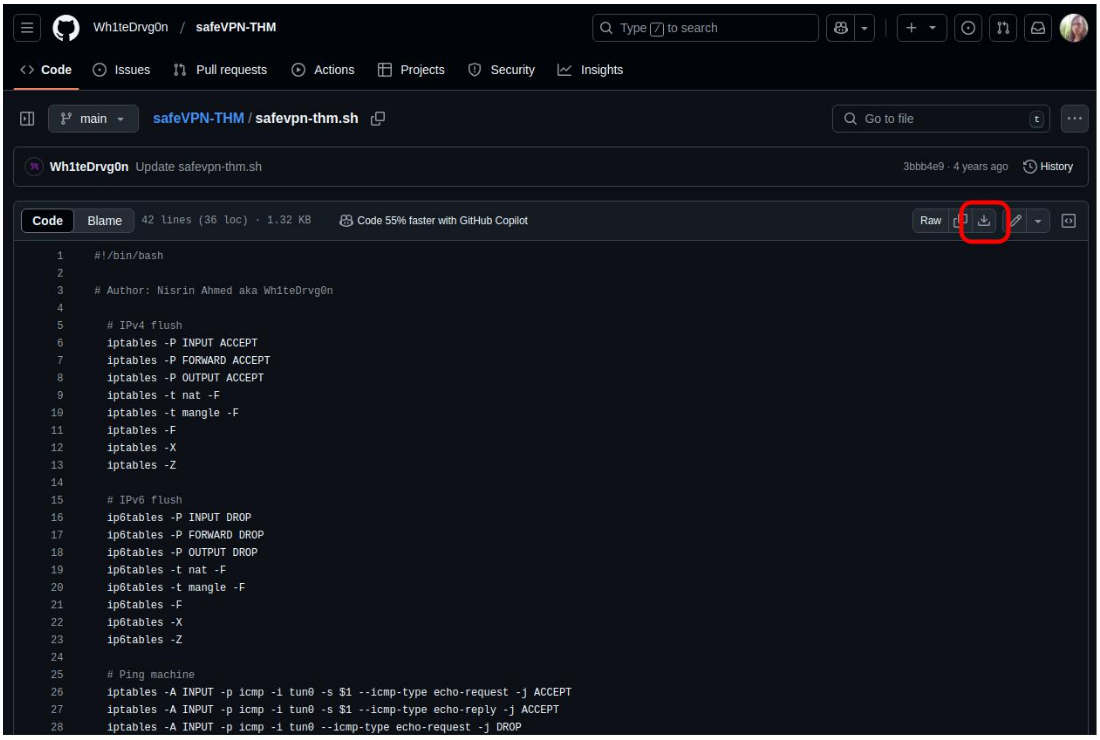
iptables rules to only have incoming connections from the machine on TryHackMe

usage:

```
sudo chmod +x ./safevpn-thm.sh
sudo ./safevpn-thm.sh <ip of deployed machine>
```

example:

```
sudo ./safevpn-thm.sh 10.10.10.10
```


Wh1teDrvg0n / safeVPN-THM
Type / to search
Code
Issues
Pull requests
Actions
Projects
Security
Insights
main
safeVPN-THM / safevpn-thm.sh
Go to file
Wh1teDrvg0n Update safevpn-thm.sh
3bbb4e9 · 4 years ago
History
Code
Blame
42 lines (36 loc) · 1.32 KB
Code 55% faster with GitHub Copilot
Raw

```
#!/bin/bash

# Author: Nisrin Ahmed aka Wh1teDrvg0n

  # IPv4 flush
  iptables -P INPUT ACCEPT
  iptables -P FORWARD ACCEPT
  iptables -P OUTPUT ACCEPT
  iptables -t nat -F
  iptables -t mangle -F
  iptables -F
  iptables -X
  iptables -Z

  # IPv6 flush
  ip6tables -P INPUT DROP
  ip6tables -P FORWARD DROP
  ip6tables -P OUTPUT DROP
  ip6tables -t nat -F
  ip6tables -t mangle -F
  ip6tables -F
  ip6tables -X
  ip6tables -Z

  # Ping machine
  iptables -A INPUT -p icmp -i tun0 -s $1 --icmp-type echo-request -j ACCEPT
  iptables -A INPUT -p icmp -i tun0 -s $1 --icmp-type echo-reply -j ACCEPT
  iptables -A INPUT -p icmp -i tun0 --icmp-type echo-request -j DROP
```

2. **Move the script to the working folder**

```
cd ~/Downloads
mv safevpn-thm.sh TryHackMe/Tutorial/OpenVPN
cd TryHackMe/Tutorial/OpenVPN
ls
```

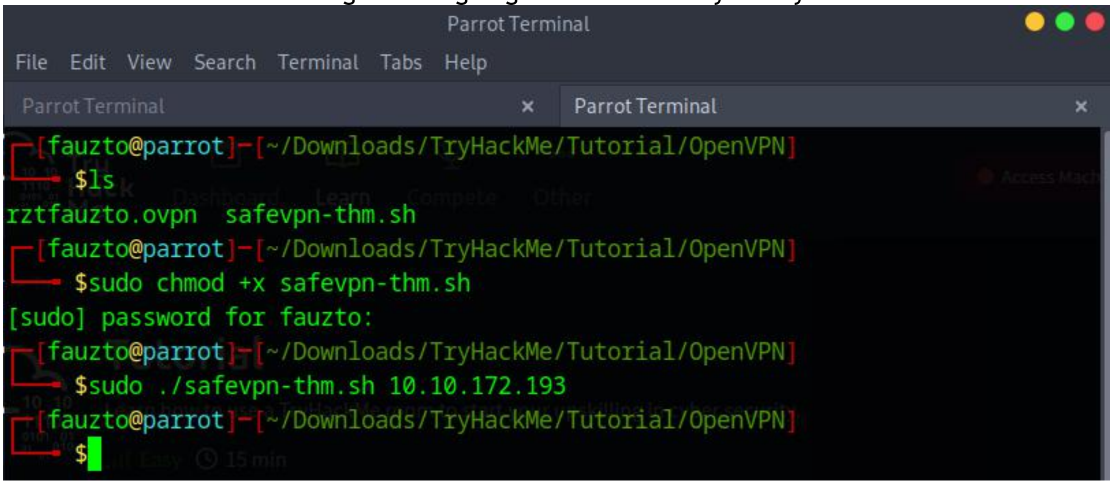
2. **Grant execution permissions to the script:**

```
sudo chmod +x safevpn-thm.sh
```

3. **Run the script to configure firewall rules:**

```
sudo ./safevpn-thm.sh <MACHINE_IP>
```

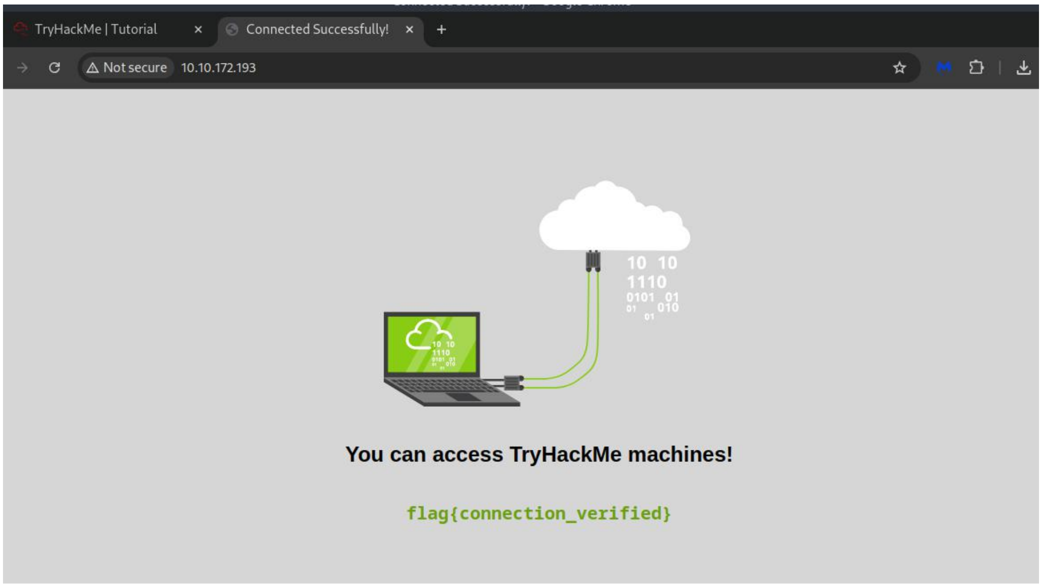
- This will restrict incoming and outgoing connections only to TryHackMe's VPN.



```
┌─[fauzto@parrot]─[~/Downloads/TryHackMe/Tutorial/OpenVPN]
└──╼ $ls
rztfauzto.ovpn  safevpn-thm.sh
┌─[fauzto@parrot]─[~/Downloads/TryHackMe/Tutorial/OpenVPN]
└──╼ $sudo chmod +x safevpn-thm.sh
[sudo] password for fauzto:
┌─[fauzto@parrot]─[~/Downloads/TryHackMe/Tutorial/OpenVPN]
└──╼ $sudo ./safevpn-thm.sh 10.10.172.193
┌─[fauzto@parrot]─[~/Downloads/TryHackMe/Tutorial/OpenVPN]
└──╼ $
```

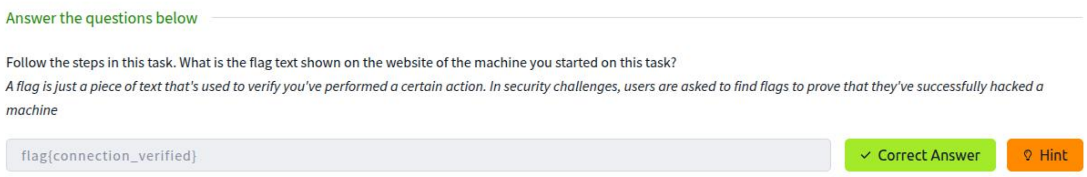
---

5. Step 3: Access the Machine and Complete the Challenge
1. **Open a browser in Kali Linux or Parrot Security.**
2. **Enter the machine's IP address in the address bar.**
3. **Find the *flag* on the web page.**
4. **Copy the *flag* and paste it into TryHackMe.**
5. **Click *Submit* to complete the machine.**



You can access TryHackMe machines!

flag{connection_verified}

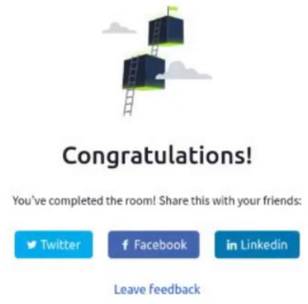


Answer the questions below

Follow the steps in this task. What is the flag text shown on the website of the machine you started on this task?

A flag is just a piece of text that's used to verify you've performed a certain action. In security challenges, users are asked to find flags to prove that they've successfully hacked a machine

flag{connection_verified}



Congratulations!

You've completed the room! Share this with your friends:

---

6. Validation and Testing

1. **Verify VPN Connection:**

```
ip a | grep tun0
```

2. **Test Connectivity to the Target Machine:**

```
ping -c 4 <MACHINE_IP>
```

3. **Check Firewall Rules:**

```
sudo iptables -L
```

---

7. Conclusion and Additional Resources

Summary
With this guide, you have successfully connected to TryHackMe via VPN, secured your connection, and completed the Tutorial machine.

Recommended Resources:
- TryHackMe Official Documentation → https://tryhackme.com/
- OpenVPN Documentation → https://openvpn.net/
- TryHackMe safe VPN access → https://github.com/Wh1teDrvg0n/safeVPN-THM

Security Considerations
- Always **disconnect the VPN** after finishing a session.
- Use **firewall rules** to prevent unauthorized access.

Contributions
Contributions are welcome! Feel free to fork the repository, make improvements, and submit a pull request.

Happy hacking!