(/) 1 of 1 post ⬍

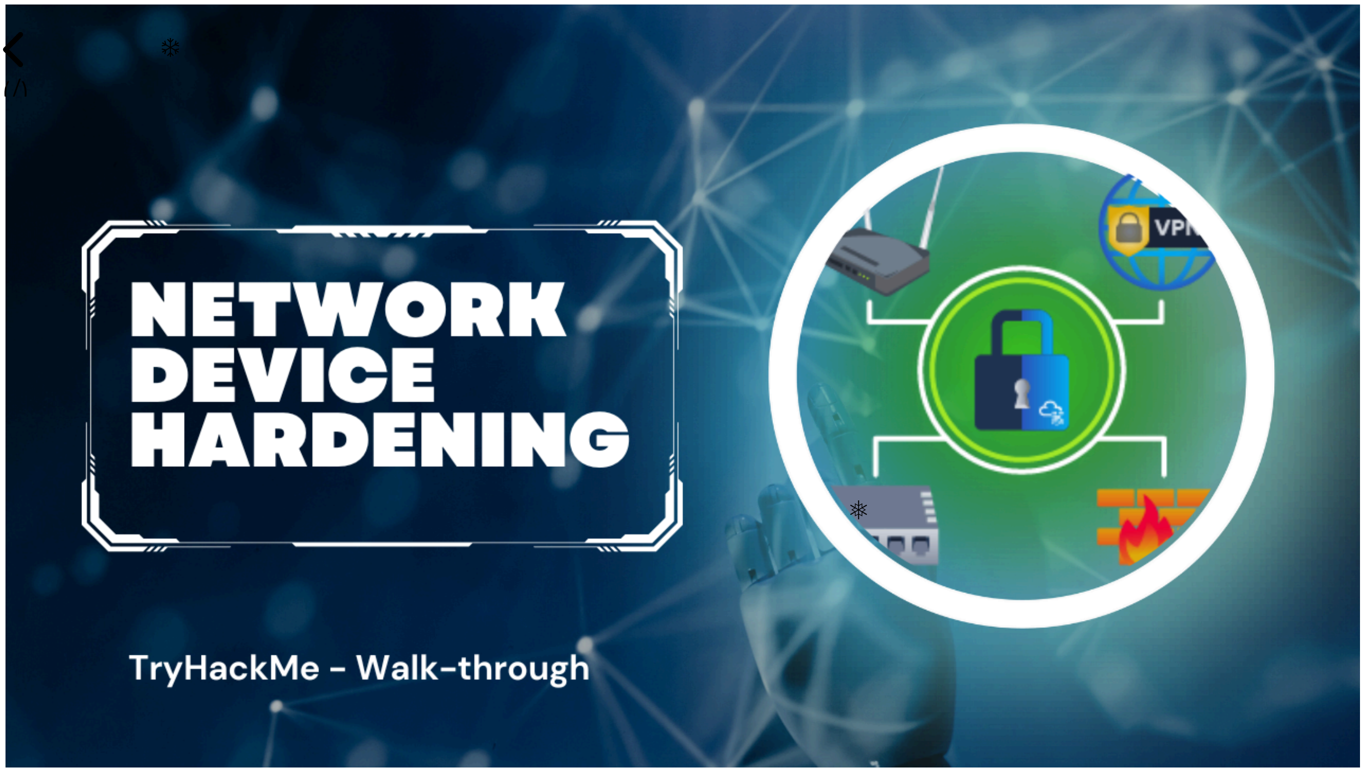
Network Security (/t/network-security) CTFs (/t/ctfs)

# Network Device Hardening | TryHackMe walk-through

**VOTERS** (/u/admiralarjun) (/u/mccleod1290) A (/u/Arulkumaran) S (/u/SamK) M (/u/Mohan183) H (/u/HariKumarKaranam) V (/u/Vibhu2004)

Share

**mccleod1290 (/u/mccleod1290)** Jun 25, 2023 Edited



🚪 ROOM-LINK- **https://tryhackme.com/room/networkdevicehardening (https://tryhackme.com/room/networkdevicehardening)**

This time we will be looking at **subscriber only** room from tryhackme. This room is labeled as **medium in difficulty** but it's more beginner friendly and holds our hand through each task. Though there may be a lot of theoretical concepts, note that they are important building blocks if one is really serious about doing something in cyber-security. **Don't worry if you don't have an active tryhackme subscription, you still can learn a lot about what are network devices and how to harden them.** This is a recently released room and hope you guys have fun solving this one.

**Suggestion on how to read and approach this road through this walk-through.**
This walk-through is fairly a long one with over 2000 words. So it's recommended to skim or to give a vague glance over the theory of the task and then directly jump into the questions. If you feel stuck come back and then re-read the theory part written in this blog, doing so will save your time even if you jumping back and forth from theory to questions.

# Task-1 Introduction

This task does not require any answers to be answered. Just some learning objectives and learning pre-requisites. This room assumes that the solver is familiar with networking concepts, some networking services, OSI model, and firewall. Although I still have not solved firewall room from tryhackme, remaining rooms have been solved. So feel free to check these pre-requisites rooms.

- **Networking (https://tryhackme.com/room/introtonetworking)**
- **Network Services (https://tryhackme.com/room/networkservices)**
- **Open Systems Interconnection (OSI) Model (https://tryhackme.com/room/osimodelzi)**
- **Firewalls (https://tryhackme.com/room/redteamfirewalls)**

---

# Task-2 Common Threat and Attack Vectors

So tryhackme does an excellent job on explaining some core-essential terminologies before we go into the actual real concept, but since it's a subscriber only room, I can't directly share their paragraphs or images that are informative. So I will be paraphrasing and trying to cover equivalent content with help of some chatgpt generated tables for deeper understanding of concepts.

**1. Differences between network device and endpoint devices.**

This should be obvious, we know that network devices are the ones that manage and control flow of network and it's resources in an network. These often require complex configuration and specialized knowledge as they are not as simple to use as a endpoint device is.

Examples of network devices are;

1. Routers
2. Firewalls
3. Load balancers
4. Gateways

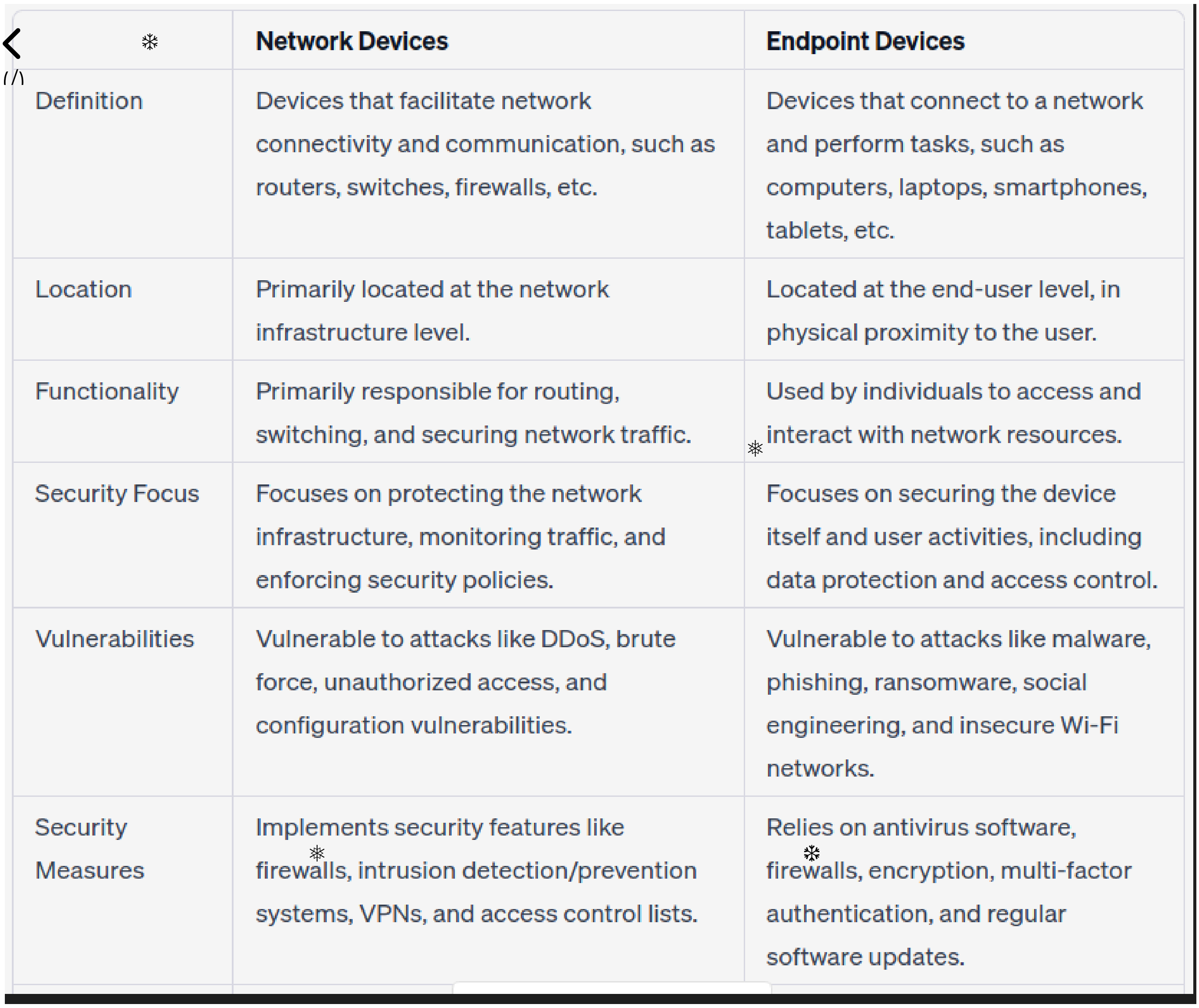
(/)

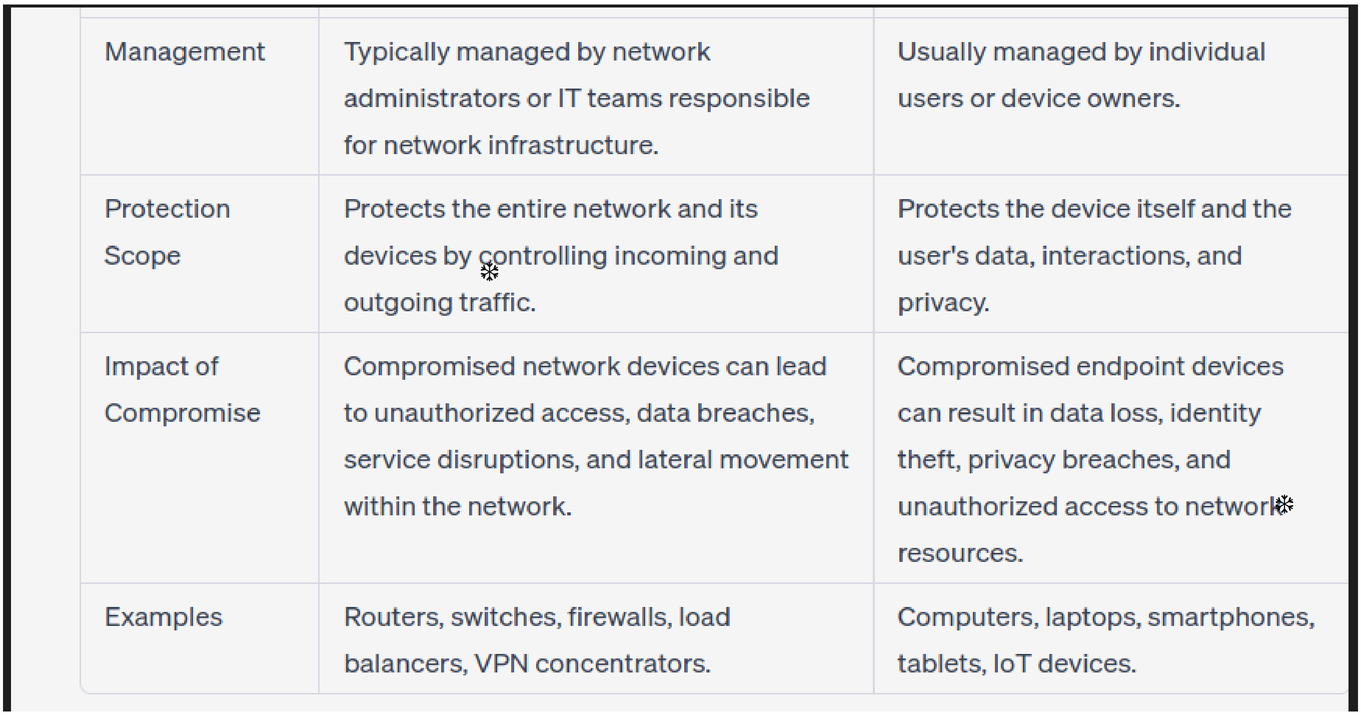
Endpoint devices on the other hand are the devices that use, access and consume network and it’s resources in an network. These devices are often located at the edge of the network i.e at the end and hence the name endpoint devices.

Examples of end-point devices are;

1. Laptops, tablets and smart-phones.
2. Printers and scanners.
3. VoIP phones and IoT devices.

To get deeper understanding of both, let’s ask chat-gpt to draw a difference table between end-point devices and network devices.





| | Network Devices | Endpoint Devices |
|---|---|---|
| Definition | Devices that facilitate network connectivity and communication, such as routers, switches, firewalls, etc. | Devices that connect to a network and perform tasks, such as computers, laptops, smartphones, tablets, etc. |
| Location | Primarily located at the network infrastructure level. | Located at the end-user level, in physical proximity to the user. |
| Functionality | Primarily responsible for routing, switching, and securing network traffic. | Used by individuals to access and interact with network resources. |
| Security Focus | Focuses on protecting the network infrastructure, monitoring traffic, and enforcing security policies. | Focuses on securing the device itself and user activities, including data protection and access control. |
| Vulnerabilities | Vulnerable to attacks like DDoS, brute force, unauthorized access, and configuration vulnerabilities. | Vulnerable to attacks like malware, phishing, ransomware, social engineering, and insecure Wi-Fi networks. |
| Security Measures | Implements security features like firewalls, intrusion detection/prevention systems, VPNs, and access control lists. | Relies on antivirus software, firewalls, encryption, multi-factor authentication, and regular software updates. |
| Management | Typically managed by network administrators or IT teams responsible for network infrastructure. | Usually managed by individual users or device owners. |
| Protection Scope | Protects the entire network and its devices by controlling incoming and outgoing traffic. | Protects the device itself and the user's data, interactions, and privacy. |
| Impact of Compromise | Compromised network devices can lead to unauthorized access, data breaches, service disruptions, and lateral movement within the network. | Compromised endpoint devices can result in data loss, identity theft, privacy breaches, and unauthorized access to network resources. |
| Examples | Routers, switches, firewalls, load balancers, VPN concentrators. | Computers, laptops, smartphones, tablets, IoT devices. |

### 2. Common Threats and Attack Vectors of Network Devices

In this context, we refer common threats to cyber-security attacks that compromise CIA triad of network devices. And attack vector according to wikipedia refers to

```
In computer security, an attack vector is a specific path, method, or scenario that can
```

In this task we will be looking at five attack vectors and threats to network devices.

1. **Unauthorized access.** This topic should be self-explanatory as everyone knows this refers to an external entity gaining access to whole or part of a network, which can be caused due to RCE, or social engineering or password attacks like password spraying and brute forcing.
2. **DoS or denial of service attack** refers to computers sending illegitimate requests that a device or service can't handle in hopes of making that service of device go offline or inaccessible for users.
3. **Man-in-the-middle attacks.** The age old Alice and Bob story when someone let's say Zack tries to listen to their conversations. This is caused due to Spoofing of all kinds or due to wire-less attacks that **@calc1f4r (https://hacklido.com/u/calc1f4r)** has documented well in his recent blogs.
4. **Privilege escalation**. After an attacker got initial access to the devices in order to gain more control or to cause more havoc the hacker needs more system or network privileges. In order to do that, hacker will try out if the network is using weak passwords or exploit any vulnerabilities or check out any security mis-configurations.
5. **Bandwidth theft/ hotlinking** . In simplest terms it refers to unauthorized linking of someone else's resource such as images, videos or any digital media from an original website [A] to malicious website **in hopes that this un-authorized linking of slows down or reduces performances of server [A].**

## Questions…

1. **The device that is used to control and manage network resource is called? This one was easy, don’t spend too much time thinking on this one and hint for this question lies in the room name it-self.**

   ```
   network device
   ```

2. A threat vector that includes disruption of critical devices and services to make them unavailable to genuine users is called?

   ```
   denial of service
   ```

# Task-3 General Hardening Techniques

Note that these techniques are self-explanatory and easy to understand.

1. Updating and patching.
2. Disabling unnecessary services and ports to avoid increasing attack vectors.
3. Principle of leas privilege to minimize risk after initial access.
4. Logs monitoring to co-relate hacker’s/malicious activity in a network.
5. Backup regularly to avoid accidental data loss.
6. Enforcing strong passwords
7. Using multi-factor-authentication

Some **secure protocols** in network devices if they are implemented corrected are

1. HTTPS
2. SSH
3. SSL/TLS

   You can learn more about secure network protocols in **this (http://tryhackme.com/jr/networksecurityprotocols)** room.

Some **insecure protocols** in network devices are…

1. FTP
2. HTTP
3. TELNET
4. SMTP

**Grey area protocols** that are safe but must be configured properly..

1. LDAP
2. RDP
3. SIPS

Implementation of monitoring and logging controls is important as it helps to investigate security incidents properly and helps organization to stay secure. One could use these techniques for this.

1. **Syslog** is a standardized protocol for storing, sharing and analyzing log messages in a centralized server.
2. **SMNP** alerts user via notification when predefined event happens.
3. **Netflow** is a protocol used to analyze network traffic via monitoring and security analysis.
4. **Packet captures** using wireshark

## Questions

1. Suppose you are configuring a router; which of the following could be considered an insecure protocol:

   A: HTTPS

   B: FTP

   C: SSH

   D: IPsec

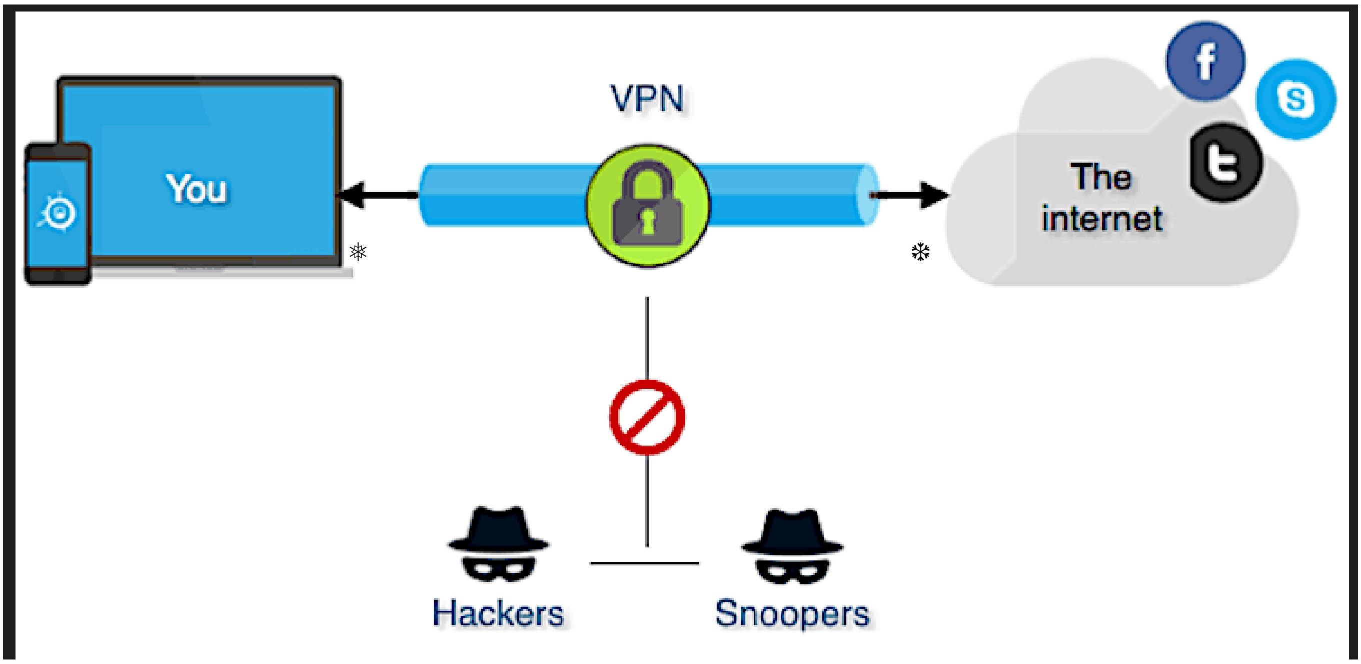
B

2. The protocol for sending log messages to a centralised server for storage and analysis is called?

syslog

# Task -4 Hardening Virtual Private Networks

Now we all have used VPN's at one point of time and we all know why it's important. [I mean nordvpn and other VPN companies do an excellent work on why everyone needs a vpn.]. Here is a simple diagram how vpn works by providing a secure network tunnel between you and the internet.



If you are interested on protocols of an VPN check out this link. **https://nordvpn.com/blog/protocols/ (https://nordvpn.com/blog/protocols/)**

Now for this task there are six ways to harden an VPN.

1. **Use strong encryption algorithm**. I mean this should be obvious most openvpn or vpn configurations use and rely on weaker encryption standard such as AES-128-CBC, although AES or advance encryption standard is secure by it-self, but use of just 128 bit key in cipher block chaining mode or CBC mode is not enough. It's advised to use 256 bit key. You can edit the cipher mode by following commands.

```
sudo nano /etc/openvpn/server/server.conf
```

Edit the cipher line from the configuration line and then hit Ctrl+O and hit enter and then hit Ctrl+X. Now restart the service.

```
sudo systemctl restart openvpn-server@server.service
```

Alternatively go to the directory where your vpn is stored and then use this command this should update your depreciated ciphers.

```
sed -i 's/cipher AES-256-CBC/data-ciphers AES-256-CBC/' *.ovpn
```

2. **Keep VPN gateway software up-to-date**:

   You can update your vpn gateway software with this simple command.

   ```
   sudo apt-get upgrade openvpn
   ```

3. **Implement strong authentication:**

   Again go to the openvpn configuration file, and edit the auth line.

   ```
   sudo nano /etc/openvpn/server/server.conf
   ```

Once you have edited the auth line to either SHA256, OR SHA516 which ever one you want to use hit hit Ctrl+s and then hit Ctrl+X

4. **Change default settings**. Refer documentation of your vpn to do this and aa bit of googling always helps.
5. **Enable Perfect Forward Secrecy (PFS)**:

   This open generates unique session keys so that even if one session key gets hacked by hacker, remaining session remain in tact without getting compromised. **You should be able to do this as mentioned here (https://serverfault.com/questions/959944/openvpn-does-perfect-forward-secrecy-key-need-to-be-kept-private)** .

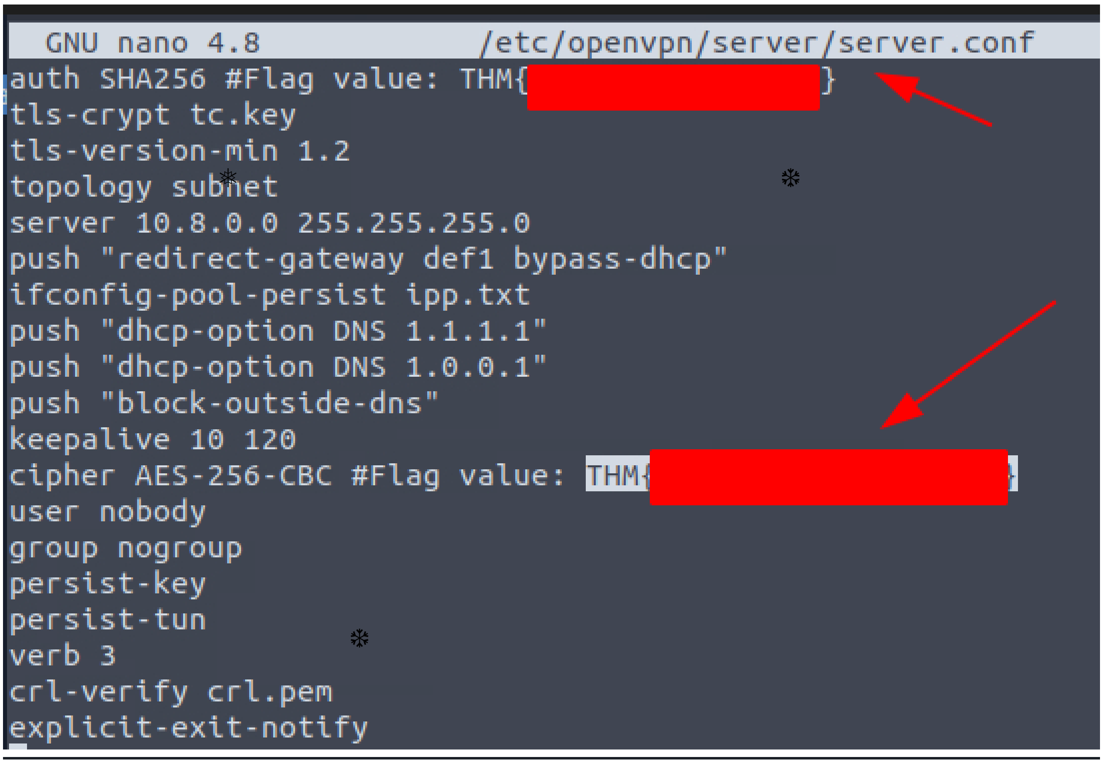
6. Have separate dedicate user for VPN server and this limits the potential of harm.

## QUESTIONS

1. Update the config file to use **cipher AES-128-CBC**. What is the flag value linked with the cipher directive?
2. Update the config file to use **auth SHA512**. What is the flag value linked with the auth directive?

```
sudo nano /etc/openvpn/server/server.conf
```

Both the answer flags are here in this configuration file you just need to open and go through it.



```
  GNU nano 4.8              /etc/openvpn/server/server.conf
auth SHA256 #Flag value: THM{[redacted]}
tls-crypt tc.key
tls-version-min 1.2
topology subnet
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 1.1.1.1"
push "dhcp-option DNS 1.0.0.1"
push "block-outside-dns"
keepalive 10 120
cipher AES-256-CBC #Flag value: THM{[redacted]}
user nobody
group nogroup
persist-key
persist-tun
verb 3
crl-verify crl.pem
explicit-exit-notify
```

3. As per the config file, what is the port number for the OpenVPN server?

```
1194
```

# Task -5 Hardening Routers, Switches & Firewalls

Now for this task we are provided a router with openwrt installed and in the task itself we are given how to access. In your case it might tryhackmemachineip;8080 . And login with the credentials given there.

Some of the hardening techniques are..

1. Set up the device which you can go to `System > System` and then select your desired option.
2. Change default credentials under `System > Administration` and then hit the `save` button
3. Enable secure network protocols under `System > Administration > SSH Access` .
4. Disable unnecessary scripts using `System > Startup`
5. Use secure wifi standard like WPA2/WPA3.

Note that for the sake of simplicity no screenshots are attached, as this is a subscriber room so I don't want to take any risk. You can setup openwrt locally in your virtual machine and play out.

## Questions

1. Update the password of the router to TryHackMe123.

```
no answer needed
```

2. What is the default SSH port configured for OpenWrt in the attached VM?

```
22
```

3. Go through the **General Settings** option under the **System** tab in the attached VM. The administrator has left a special message in the Notes section. What is the flag value?

```
THM{xxxxxxxxxx}
```

4. What is the default system log buffer size value for the OpenWrt router in the attached VM?

```
64
```

5. What is the start priority for the script **uhttpd**?

```
50
```

Navigating around the openwrt interface would give answer to question 4 and 5 if not use google….

## Task -6 Hardening Routers, Switches & Firewalls - More Techniques

**Recommended Hardening Techniques…**

1. Manage traffic rules by going to the following settings at openwrt console `Network > Firewall > Traffic Rules`, and click `Add` to create a new rule.
2. Monitor traffic, under `Status > Realtime Graph > Traffic` one can monitor the network traffic, this is super useful as it gives us visual representation of traffic.
3. You can also configure port forwarding option using this option from network tab `Network > Firewall > Port Forwards`, and click the `Add` button.
4. You can monitor scheduled tasks using `System > Scheduled Tasks`, add the new cron job, and click `Save`
5. Updating of firmware can be done easily through `System > Software`.

**WHEN DEALING IN AN ENTERPRISE ENVIRONMENT MAKE SURE THAT**

1. **Port security** is configured properly depending on the product you are using
2. **Preventing 'ARP SPOOFING'** **using this link as reference (https://tryhackme.com/room/layer2)**.

3. **Preventing rogue DHCP servers** which you can learn more **here (https://tryhackme.com/room/introtolan)**.
4. **Enabling IPv6** This will help us stay safe from MITM, eavesdropping, and tampering of packets in transit.

## QUESTIONS

1. What is the name of the rule that accepts ICMP traffic from source zone **WAN** and destination zone as **this device**?

```
Allow-Ping
```

HINT- check `network > firewall > traffic rules`

2. What is the name of the rule that forwards data coming from **WAN** port 9001 to **LAN** port 9002?

```
THM_PORT
```

HINT- check `network > firewall > port forwards`

3. What is the version number for the available **apk** package?

```
2.12.2-1
```

HINT- check `system > software` and search until you find apk.

# Task -7 Important Tools for Network Monitoring

Some well known tools used for network monitoring are...

1. **Nagios (https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/quickstart.html)** [Open-source]

2. **SolarWinds Network Performance Monitor (https://documentation.solarwinds.com/en/success_center/npm/content/npm_installation_guide.htm)**
3. **PRTG (https://www.paessler.com/manuals/prtg/installation)**
4. **Zabbix (https://www.zabbix.com/download)**

## Question

1. Are network monitoring tools capable of detecting bandwidth bottlenecks? (yea/nay)

```
The answer is obviously yea.
```

# Task- 8 Conclusion

We have seen that hardening involves implementing various security measures like

1. Firmware updates
2. Change of default passwords
3. Strong authentication mechanisms
4. Encryption
5. Logging
6. Use of security protocols
7. And network monitoring tools

Go ahead and complete this task as this task does not require you to answer anything. With this we come to an end and hopefully you guys have learned something new from this walk-through.

7 30% Reply

(/)

**Home for infosec writers and readers.**

Create your account today and explore more content on this platform. You can also start blogging and be inspiration for others 😎

Signup

Write a Reply...

## Blogpost that you may like!

(/u/mccleod1290)

125

0

### Directory Fuzzing and Hidden Resources: Using Ffuf Effectively

General Web Security **mccleod1290** Posted 2 days ago
(/blog/969-directory-fuzzing-and-hidden-resources-using-ffuf-effectively)

(/u/mccleod1290)

311

0

### Web Recon : A Pentester's Guide to Information Gathering

General Web Security **mccleod1290** Posted 5 days ago
(/blog/968-web-recon-a-pentesters-guide-to-information-gathering)

(/u/mccleod1290)

410

0

### Introduction to Web Proxies: Mastering Burp Suite and OWASP ZAP

General Web Security **mccleod1290** Posted 8 days ago
(/blog/967-introduction-to-web-proxies-mastering-burp-suite-and-owasp-zap)

(/u/mccleod1290)

669

0

### Web Application Basics: The foundation of Modern Internet

General **mccleod1290** Posted 17 days ago
(/blog/966-web-application-basics-the-foundation-of-modern-internet)

(/)

(/u/mccleod1290)

796

0

## Understanding HTTP: The Language of the Web

General Web Security **mccleod1290** Posted 22 days ago

(/blog/965-understanding-http-the-language-of-the-web)