

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



Network Device Hardening (Try Hack Me)



Nitish Agrawal · [Follow](#)

8 min read · Jun 21, 2023



Listen



Share

... More

Task 1 — Introduction



Learning Objectives

The room aims to teach techniques for identifying and mitigating security vulnerabilities, hardening network device configurations, and implementing security best practices. By the end of this room, you should be able to assess and strengthen network device security, enhance network resilience, and effectively defend against common cyber threats.

I am ready to start the room.

Answer — No answer needed

Task2 — Common Threats and Attack Vectors

Difference between Network Devices and Endpoint Devices

Before proceeding with our actual topic, it is imperative to understand the difference between network devices and endpoint devices. Endpoint devices refer to any device that can generate or consume data on a network, such as Laptops, Desktops, Smartphones, Tablets, Printers, Servers, and IoT Devices. They are typically located at the edge of a network and interact directly with users. The figure below shows the difference between endpoint and network devices based on their functionality, traffic, and configuration.

Q.1 The device that is used to control and manage network resource is called?

Ans. — Network device

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

Ans. — Denial of Service

Task3 — Common Hardening Techniques

General Techniques

Hardening techniques are meant to reduce the attack surface of a system or network by removing unnecessary functionality, limiting access, and implementing various security controls. Some standard methods are mentioned below:

- **Updating & Patching:** Ensuring the latest version of the Operating System and underlying applications of all devices and systems and installing regular security patches is the core hardening measure. Outdated OS and applications contain vulnerabilities that attackers can exploit.
- **Disabling unnecessary services & ports:** Turn off all unnecessary services and block all ports (physical and virtual) that are not needed for system functionality. This will reduce the attack surface by minimising the number of entry points an attacker can exploit.
- **Principle of Least Privilege (POLP):** Restrict users and processes to only the minimum necessary permissions required to perform their functions.
- **Logs Monitoring:** Implement a log monitoring system to monitor for unusual activity or security events.

- **Backup regularly:** Take routine backups of systems and configurations as they can help recover from a security incident or system failure.
- **Enforcing Strong Passwords:** Change default login passwords and use strong passwords that are at least ten characters long with a combination of small letters, capital letters, special characters, and numbers. These types of passwords protect against dictionary and brute-force attacks.
- **Multi-Factor Authentication (MFA):** MFA is an additional security layer requiring two or more types of identification before accessing the account or system. The two factors are generally something we know (like passwords) and something we have (like biometrics).

Q.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

Ans. — B

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

Ans . — SysLog

Task4 — Hardening Virtual Private Network

Virtual private networks (VPNs) are now needed in the age of remote work and online communication to protect sensitive data and preserve privacy. Yet, hardening VPNs is crucial to ensure their efficiency as cyberattacks continue to develop. Hardening VPNs entails adopting additional security measures, such as multi-factor authentication and encryption techniques, to make it more challenging for hackers to access the network. By taking these extra precautions, businesses can better safeguard their data and defend against cyberattacks, raising their security level and bringing them more peace of mind.

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

Ans. — THM{CIPHER_UPDATED_1101}

Q.2 — Update the config file to use **auth SHA512**. What is the flag value linked with the auth directive?

Ans. — THM{AUTH_UPDATED_123}

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

Ans. — 1194

Task5 — Hardening Routers, Switches & Firewall

Routers and switches must be hardened for the network infrastructure to be secure and reliable. Every network needs routers and switches, often the first line of defence against potential security risks and attacks. By hardening these devices, we can lower the possibility of unauthorised access, avoid data breaches, and ensure network service availability. Improved network performance, increased resilience against cyberattacks, and regulatory compliance are a few of the main advantages of hardening routers and switches. Routers and switches without enough hardening are susceptible to various attacks, including denial of service and network profiling.

In the previous task, we studied how to harden a network device using a configuration file on a Command Line Interface (CLI). In this task, we will use the web interface to learn different methods for hardening a router. We will be using a router that has OpenWrt installed, which is a free and open-source Linux-based operating system for embedded devices. We know that a router configuration varies from product to product; however, a few standard techniques can be applied to protect from potential attacks. You can access the OpenWrt web interface at `MACHINE_IP:8080` with the following credentials:

Q .1— Update the password of the router to TryHackMe123.

Ans. — NO Answer Needed

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

Ans.2 — 22

Q.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?

Ans3. — THM{SYSTEM101}

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

Ans. — 64

Q.5— What is the start priority for the script uhttpd?

Ans. — 50

Task5 — Hardening Routers, Switches & Firewall — More Techniques

Recommended Hardening Techniques

- **Manage traffic rules:** Network devices allow you to create and implement traffic rules that accept/deny network traffic. For example, we notice that the data of users connected with our network device is being exfiltrated to a command and control server IP address. We can create a rule to block all traffic where the destination IP matches the attacker's command and control server. We can add/edit traffic rules through `Network > Firewall > Traffic Rules`, and click `Add` to create a new rule.
- **Monitor traffic:** As a network administrator, keeping track of network traffic, like uploads and downloads of data at different intervals, is essential. For example, you have excessive data uploaded from one of the email servers to an unknown IP address. Such alerts enable you to take remedial measures and stop data pilferage timely. Usually, network devices provide real-time graphs to monitor the traffic. We can view real-time traffic statistics through `Status > Realtime Graph > Traffic`.
- **Configuring port forwarding:** A firewall's port forwarding capability enables inbound traffic from the internet or other sources to be routed to a particular device or service on the internal network. The firewall can send incoming traffic to the appropriate device or service on the internal network by establishing port forwarding rules while blocking any other incoming traffic that does not comply with the rules. This feature helps host applications that need outside access, granting remote control of internal devices. Port forwarding should be used carefully because it can expose internal devices and

services to potential security issues if improperly secured and configured. Threat actors could add new rules here for creating connections to external command and control servers. We can configure port forwarding through `Network > Firewall > Port Forwards`, and click the `Add` button.

Additional Techniques in an Enterprise Environment

A network device deployed in an enterprise environment generally provides an increased attack surface for an attacker to launch attacks. As enterprise environments include a variety of devices with different models, makes, and types, there are no definite rules to harden network devices; however, a few important ones are mentioned below:

- **Configuring port security:** This includes limiting the number of MAC addresses registered on a switch port and taking particular action whenever unauthorised access is detected. Enabling port security enables an administrator that data is coming from a valid source and will be forwarded to a legitimate receiver.
- **Preventing ARP spoofing:** ARP spoofing is one of the most common vectors for launching man-in-the-middle attacks on the network. The threat can be mitigated by enabling static ARP tables and implementing MAC address filtering. You can learn more about mitigating ARP spoofing [here](#).
- **Preventing rogue DHCP servers:** The attacker creates a spoofed DHCP server that can be later on used for assigning IPs to clients and launching MITM attacks. Mitigation measures to prevent such attacks include configuring static DHCP binding and ensuring no unknown devices are added to a network through network mapping tools. You can learn more about DHCP [here](#).
- **Enabling IPv6:** Unlike IPv4, IPv6 has built-in support of IPsec that can be used to secure network communication and provide confidentiality, integrity, and authenticity. Moreover, this will help in protection against MITM, eavesdropping, and tampering of packets in transit.

A network device is configured with many options for protection against cyberattacks. We have discussed some of the most common and important ones in this task.

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

Ans.1 — Allow-Ping

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

Ans.2 — THM_PORT

Q.3 — What is the version number for the installed apk package?

Ans. — 2.12.2-1

Task7 —Important Tools for Network Monitoring

Network monitoring tools are enablers for maintaining the security and performance of networks. These tools use sophisticated algorithms and protocols to capture and analyse real-time network traffic. In addition, they enable network administrators to detect and troubleshoot problems such as bandwidth bottlenecks, network outages, and security threats. Some commonly used tools and their usage is mentioned below:

Tool

Usage Description

Nagios

A popular open-source software for monitoring systems, networks, and infrastructure. It provides real-time monitoring and alerting for various services and applications.

SolarWinds Network Performance Monitor

A comprehensive network monitoring tool that provides real-time visibility into network performance and availability. It includes network mapping, automated network discovery, and customisable dashboards.

PRTG An all-in-one network monitoring tool that provides comprehensive performance and availability monitoring. It includes real-time traffic analysis, custom dashboards, and customisable alerts.

Zabbix A powerful open-source network monitoring tool that provides real-time network performance and availability monitoring. It includes features such as customisable dashboards, network mapping, and alerting.

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

Ans.1 — Yea

Task8 — Conclusion

Q.1- I have completed the room.

Ans.1 — No Answer Needed

Join me Here for more updates

<https://www.linkedin.com/in/nitish-agrawal-3a4291178>

Tryhackme

Tryhackme Walkthrough

Cybersecurity

Network Security

Nitishagrawal



Follow

Written by Nitish Agrawal

41 Followers · 2 Following

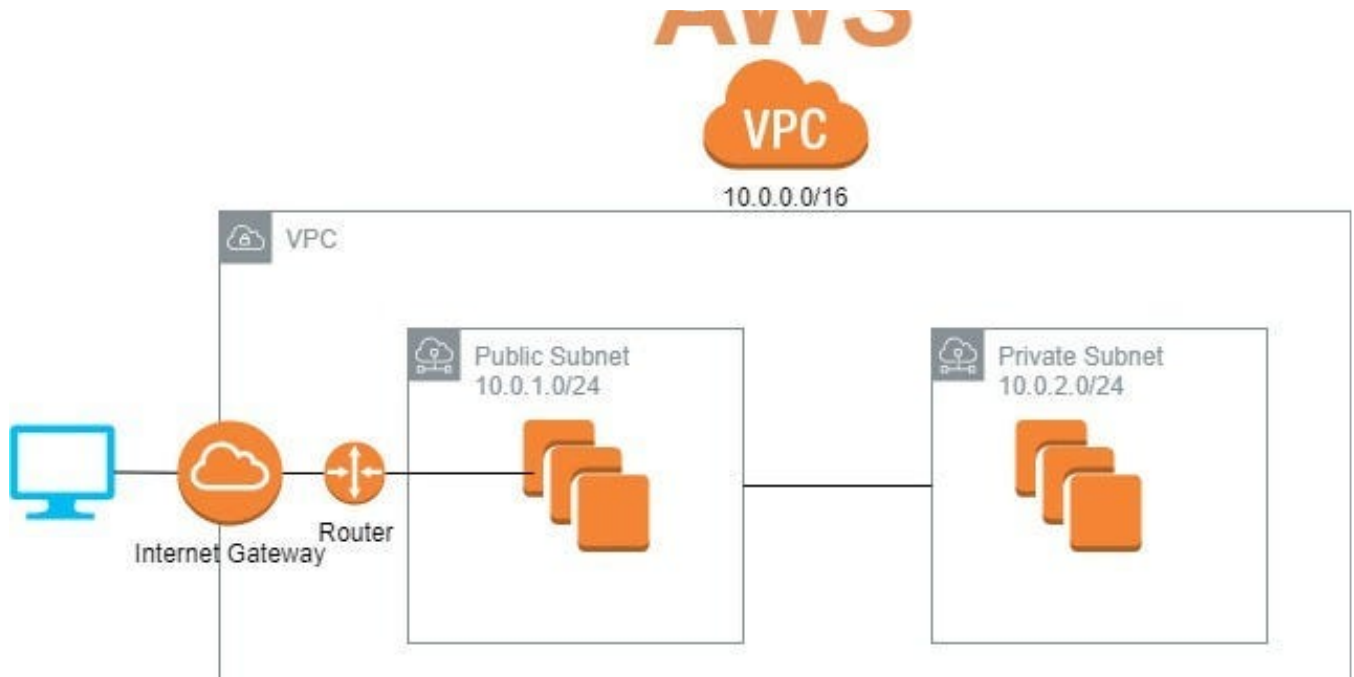
No responses yet



What are your thoughts?

Respond

More from Nitish Agrawal



Nitish Agrawal

The Benefits of Virtual Private Cloud (VPC) in AWS Cloud

Understanding Virtual Private Cloud (VPC) in AWS

Jun 13, 2023 8

WebSecurity Academy

CORS vulnerability with basic origin reflection

[Go to exploit server](#)

[Submit solution](#)

[Back to lab description >>](#)

LAB Not solved

[Home](#) | [My account](#)

WE LIKE TO
SHOP



Weird Crushes Game

★★★★★ \$78.93

[View details](#)



Picture Box

★★★★★ \$63.34

[View details](#)



Conversation Controlling Lemon

★★★★★ \$56.91

[View details](#)



More Than Just Birdsong

★★★★★ \$99.67

[View details](#)

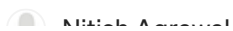
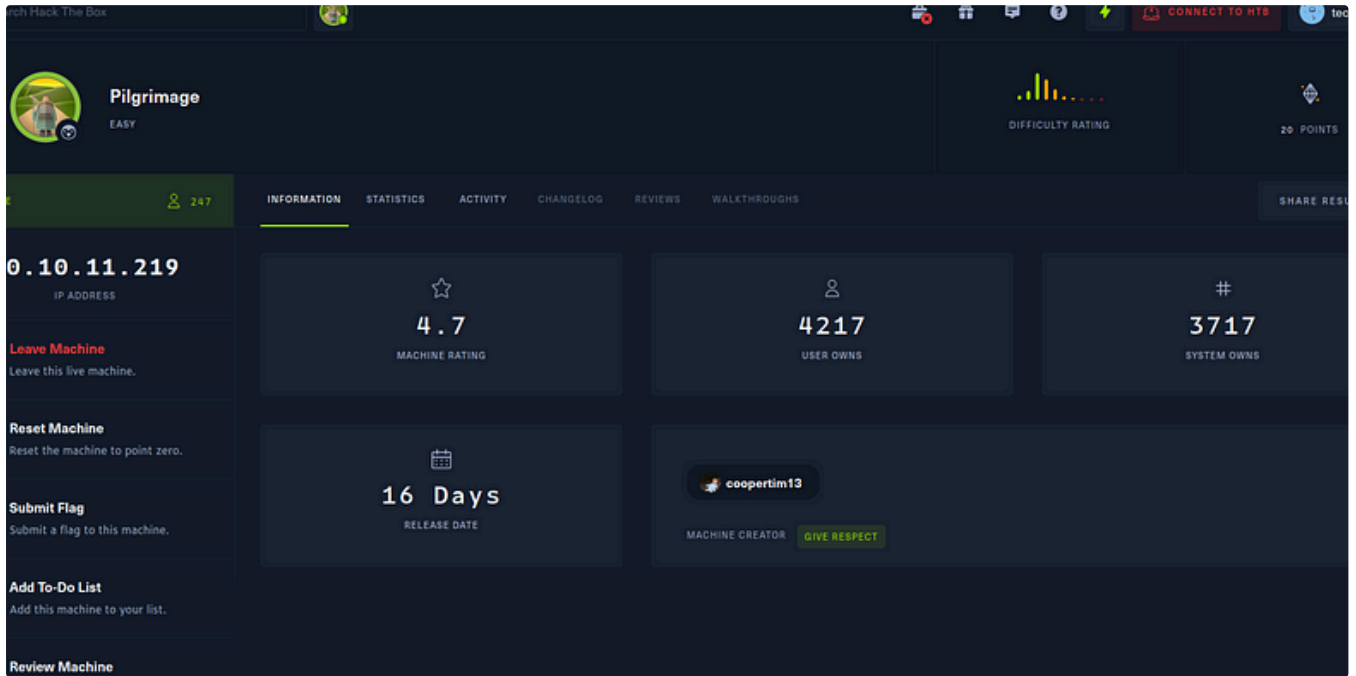


Nitish Agrawal

CORS vulnerability with basic origin reflection

What is CORS vulnerability

Jun 20, 2023



Nitish Agrawal

[Open in app](#)

Medium



Search

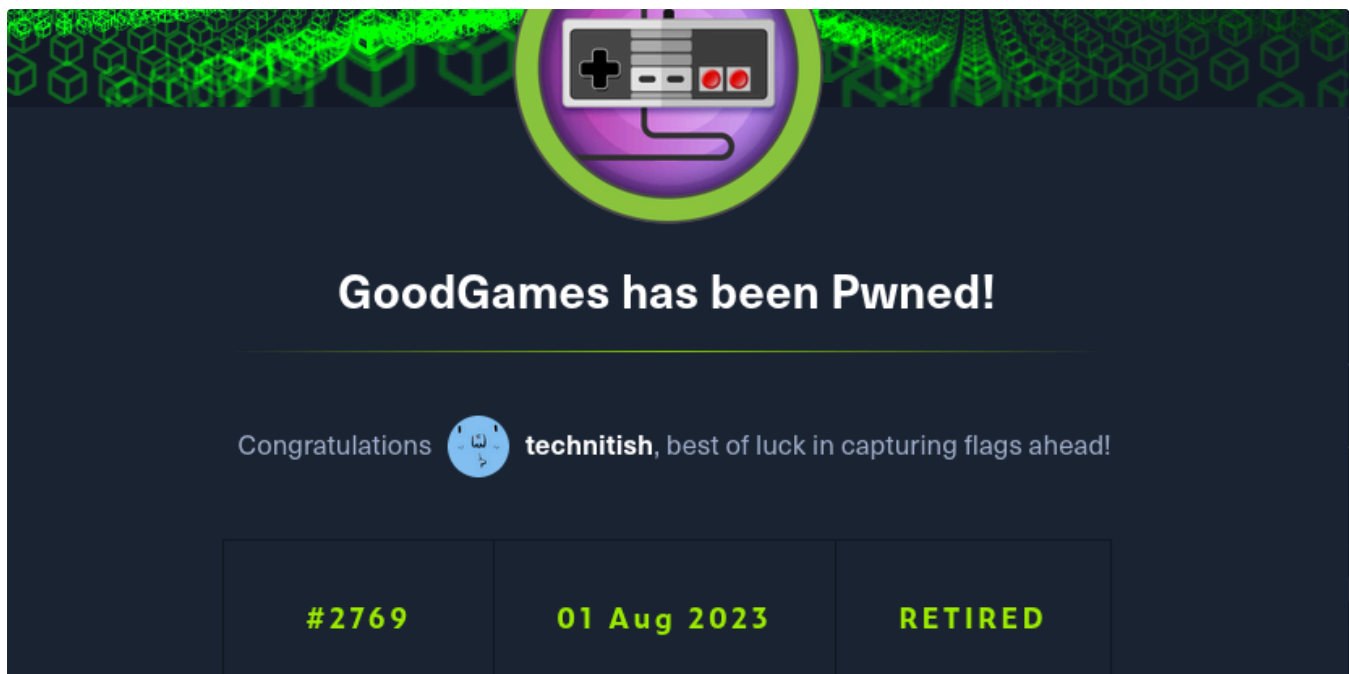


Jul 11, 2023



6





 Nitish Agrawal

GoodGames HTB Walkthrough

Aug 1, 2023  1




See all from Nitish Agrawal

Recommended from Medium

ents

	▼	User Name	▼	Name	▼	Surname	▼	Email
3		student1		Student1				studi
4		student2		Student2				studi
5		student3		Student3				studi
9		anatacker		Ana Tacker				
10		THM{Got.the.User}		X				
11		qweqwe		qweqwe				

<< < 1 > >>

 embosssdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

★ Aug 7, 2024 🖱 27



 IritT

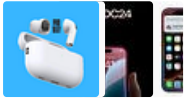
Nmap—TryHackMe Insights &Walkthrough

An in depth look at scanning with Nmap, a powerful network scanning tool.

Dec 23, 2024



Lists



Tech & Tools

22 stories · 381 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4353 saves



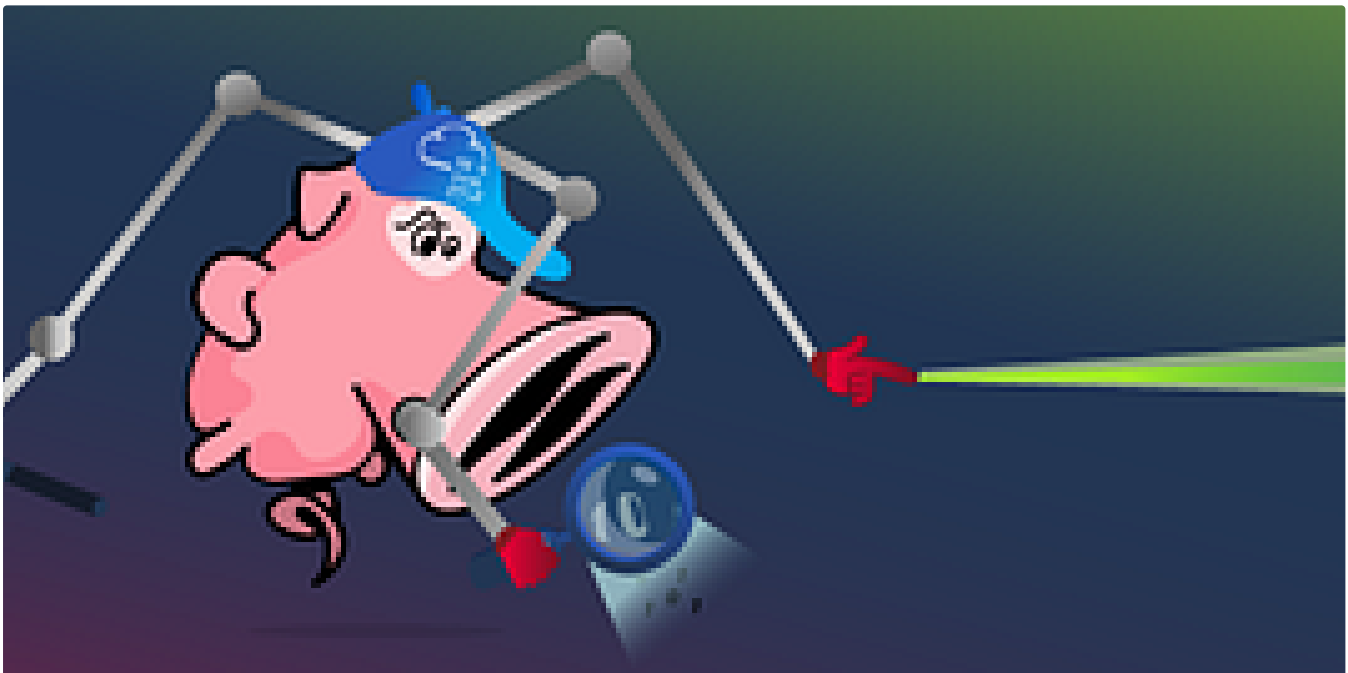
Staff picks

796 stories · 1560 saves



Natural Language Processing

1884 stories · 1530 saves



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

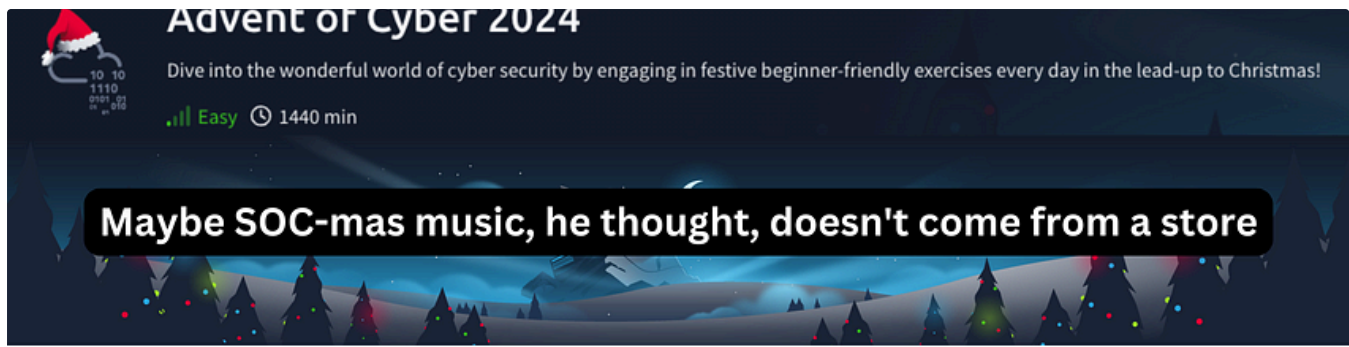


Nov 9, 2024



100





Day 1
Answers

cyberw1ng.medium.com



In System Weakness by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 1] Writeup with Answers | TryHackMe Walkthrough

Maybe SOC-mas music, he thought, doesn't come from a store?



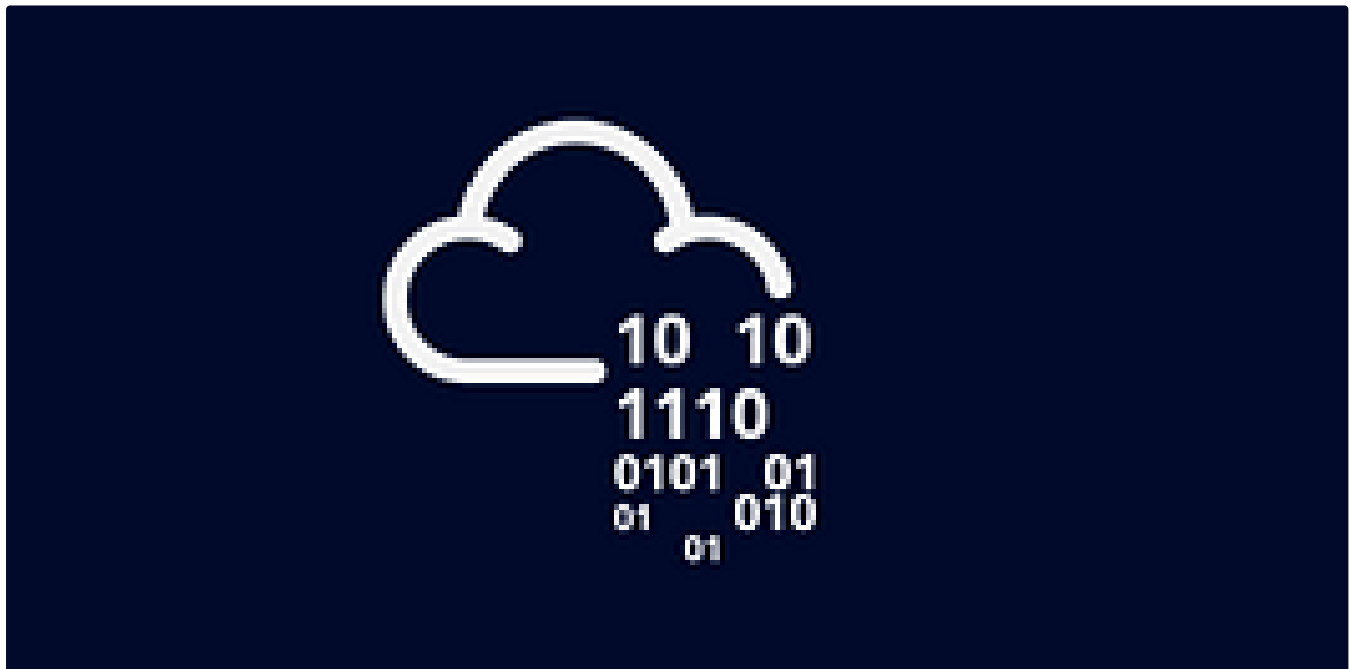
Dec 1, 2024



906



1

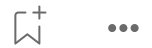


In T3CH by Axoloth

TryHackMe | Deja Vu | WriteUp

Exploit a recent code injection vulnerability to take over a website full of cute dog pictures!

★ Oct 13, 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



See more recommendations