

TryHackMe Walkthrough: Principles of Security



Esther Adwets · [Follow](#)

5 min read · Jan 7, 2024



Listen



Share



More



Hello Hackers!

Here is a walkthrough of one simple room on Try Hack Me. It is among the first few rooms in the Jr. Penetration Tester path, and hopefully, I will be able to cover a few

more from that path.

If you are super new to cybersec, don't fret; this room is very beginner-friendly, and even better, I will do my best to make this the best walkthrough for you.

Discover a few information security concepts that may be used to safeguard data and prevent system misuse. The room is available at <https://tryhackme.com/room/principlesofsecurity>.

Let's go!

Task 1: Introduction

Defence in Depth: In simple terms, this is the use of many different layers of security to an organization's system and data in the hope that these layers will provide redundancy in an organization's security perimeter.

Now, imagine if an attacker wanted to exploit the system of a company you work at. However, there are many layers to get through before getting to the main system.

These many layers would demand so much time. And by the time they reach the innermost layer, they will most likely have been caught. Additionally, getting through all these security layers requires resources!

Task 2: The CIA Triad

In cyber security, the main principles of security are:

Confidentiality: Data is protected from unauthorized access and misuse.

Integrity: The data cannot be altered by unauthorized people. Data remains unchanged during storage, transmission, and usage without altering the information.

Availability: This means that data is available and accessible by authorized users whenever they need to access it.

Questions:

1. What element of the CIA triad ensures that data cannot be altered by unauthorized people? *Ans: Integrity*

2. What element of the CIA triad ensures that data is available? *Ans: Availability*

3. What element of the CIA triad ensures that data is only accessed by authorized people? *Ans: Confidentiality*

Task 3: Principles of Privileges

It is crucial for every organization to define levels of access to the information technology systems each individual requires. For example, a Junior Penetration Tester just joining the team will not have the same level of access/powers as the systems admin, or Network engineer.

Levels of access given to each person are determined primarily by the individual's role in the organization, and the sensitivity of the information being stored on the system.

To assign and manage the access and rights of each person, we use two key concepts, namely:

Privilege Identity Management (PIM); Used to translate a user's role within the organization.

Privilege Access Management (PAM); From the name, it essentially manages privileges a system's role has, among other things such as enforcing security policies such as password management, auditing policies and reducing attack surface a system faces.

Questions:

- 1. What does the acronym "PIM" stand for?** *Ans: Privilege Identity Management*
- 2. What does the acronym "PAM" stand for?** *Ans: Privilege Access Management*
- 3. If you wanted to manage the privileges a system access role had, what methodology would you use?** *Ans: PAM*
- 4. If you wanted to create a system role that is based on a user's role/responsibilities with an organization, what methodology is this?** *Ans: PIM*

Task 4: Security Models Continued

According to a security model, any system or piece of technology storing information is called an information system.

A security model is used to define information security rules and policies within a computer system.

Below are some popular effective security models used to achieve the three elements of the CIA triad. (Do you remember them?)

The Bell-La Padula Model : This model is used to achieve confidentiality and governs access based on security labels and clearance levels. The key security levels are Top Secret, Secret, Confidential and Unclassified. The access modes are Read(R) and Write (W).

What does this mean?

1. **No Reading Up:** If you have a lower-level secret, like “Secret,” you can’t look at higher-level secrets, like “Top Secret.”
2. **No Writing Down:** If you have a higher-level secret, you can’t change or write things to a lower-level secret.

So, it’s like a set of rules making sure people only see and change secrets at their own level or lower. It’s focused on keeping secrets confidential and doesn’t really talk much about making sure information is correct.

This model is popular within governmental and military organizations because members of the organizations are presumed to have already been vetted and presumed trustworthy.

(Check for the advantages and disadvantages in the room content.)

The Biba Model: While Bell-LaPadula is more about keeping secrets safe, Biba is about making sure the information you have is trustworthy and doesn’t get messed up. (Integrity)

It applies the rule to objects(data) and subjects (users), and can be simply put as No write up, no read down.

1. **No Writing Up:** You can change or write information to your level or a lower level.
2. **No Reading Down:** Biba says you can only read information from a higher level if you’re at a lower level.

Questions

1. What is the name of the model that uses the rule “can’t read up, can read down”? *Ans: The Bell-La Padula Model*

2. What is the name of the model that uses the rule “can read up, can’t read down”? *Ans: The Biba Model*

3. If you were a military, what security model would you use? *Ans: The Bell-La Padula Model*

4. If you were a software developer, what security model would the company perhaps use? *Ans: The Biba Model*

Of Note: The Biba model is applied in scenarios prioritizing integrity over confidentiality. It finds utility in settings like software development, ensuring developers access only the code essential for their tasks without requiring entry to sensitive information such as databases.

Task 5: Threat Modelling & Incident Response

Threat modelling is like making a plan to protect something important, such as a computer system or a building. It involves thinking carefully about what bad things might happen (threats) and figuring out how to stop or reduce those bad things from happening.

Imagine you’re guarding a castle — you want to know where the doors and walls might need extra protection. In threat modelling, we find out what bad things could happen to a computer system and where it’s most vulnerable.

It’s a way to stay one step ahead of potential problems by identifying and preparing for them.

The threat modelling process is very similar to a risk assessment made in workplaces. Essentially, the principles all return to Preparation, Identification, Mitigations and Review.

Threat Modelling is however complex and an effective threat model includes Threat Intelligence, Asset Identification, Mitigation Capabilities and Risk Assessment.

To help with this, there are frameworks such as **STRIDE** (Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of Service and Elevation of privileges) and **PASTA** (Process for Attack Simulation and Threat Analysis).

Questions

1. What model outlines “Spoofing”?

Ans: STRIDE

2. What does the acronym “IR” stand for?

Ans: Incidence Response

3. You are tasked with adding some measures to an application to improve the integrity of data, what STRIDE principle is this?

Ans: Tampering

4. An attacker has penetrated your organization’s security and stolen data. It is your task to return the organization to business as usual. What incidence response stage is this?

Ans: Recovery

And that’s the end! Till the next walkthrough! 😊💻

Cybersecurity

Tryhackme Walkthrough

Penetration Testing

Learning To Code


Vulnerability



Follow

Written by Esther Adwets

19 Followers · 7 Following

 - Penetration Tester, or Ethical Hacker. I shifted to hashnode, and here is the link to my latest articles: <https://essadwets.hashnode.dev>

No responses yet



What are your thoughts?

Respond

More from Esther Adwets

AUTHOR: NANA AMA ATOMBO-SACKY

Description

Do you know how to use the web inspector?


Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.
Its current status is:

NOT_RUNNING

Launch
Instance

Hints 

 Esther Adwets

WebDecode Pico CTF Walkthrough

In cyber security, it is important to have a deep knowledge of what you intend to secure. For instance, understanding how the web works.

Aug 16, 2024 🖱 1



Answer the questions below

Some of these questions will require the use of a static site to answer the task questions, while others require the use of the Attack Box and the Forest VM.

Esther Adwets

Nmap Live Host Discovery | TryHackMe (THM)

As I have mentioned before, knowledge is power. This is especially true when you want to target a network. The more you know about the...

Feb 4, 2024 🖱 6



Asymmetric Encryption/Public Key Cryptography

KEY FEATURES

- 🔑 Uses Dual Keys; **Public key** and **Private Key**.
- 🔑 Digital Signatures: Allows senders to sign messages, verifying their identity.
- 🔑 Secure Key Exchange: Enables two parties to create a shared secret key safely, without the need to send the actual key. E.g the **Diffie-Hellman algorithm**.
- 🔑 Slow processing: Because it involves more complex mathematical operations.
- 🔑 Protocols that use Assymetric encryption algorithm include: * **SSH** * **SSL/TLS**
 * **Pretty Good Privacy (PGP)** * **Internet Key Exchange (KIE)**
 * **S/MIME (Secure/Multipurpose Internet Mail Extensions)**

Esther Adwets

What is Asymmetric Encyption

Asymmetric encryption, also known as Public key cryptography, is a type of encryption that uses different keys to encrypt data. These keys...

May 15, 2024  51  1



Open in app ↗

Medium



Search



Esther Adwets

Congestion Control Algorithms and How They Manage Data Transmission Rates to Avoid Network...

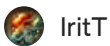
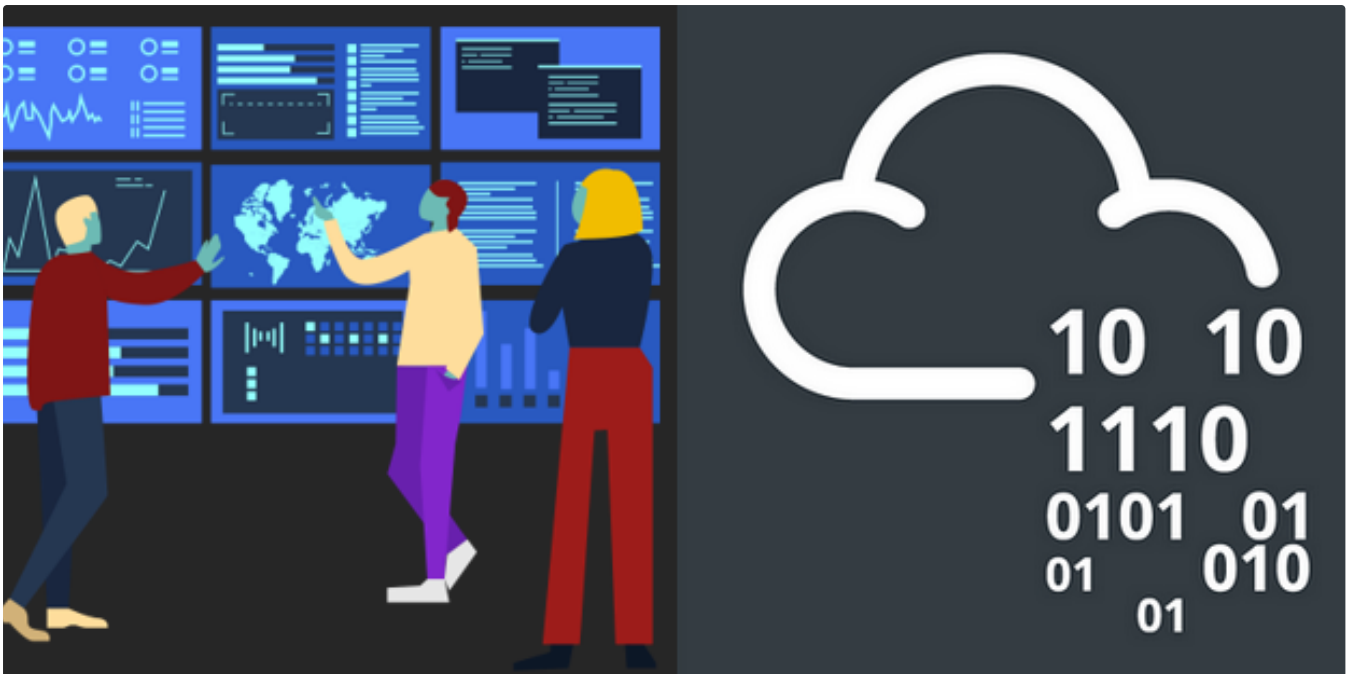
The rapid evolution of technology has led to a growth in the number of internet-connected devices, leading to an expansion of networks, and...

Aug 2, 2024



See all from Esther Adwets

Recommended from Medium



IritT

Security Operations—Introduction to Defensive Security-TryHackMe Walkthrough

Learn about Security Operations Center (SOC): its responsibilities, services, and data sources.

Oct 7, 2024



In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



Lists



Tech & Tools

22 stories · 377 saves



General Coding Knowledge

20 stories · 1841 saves



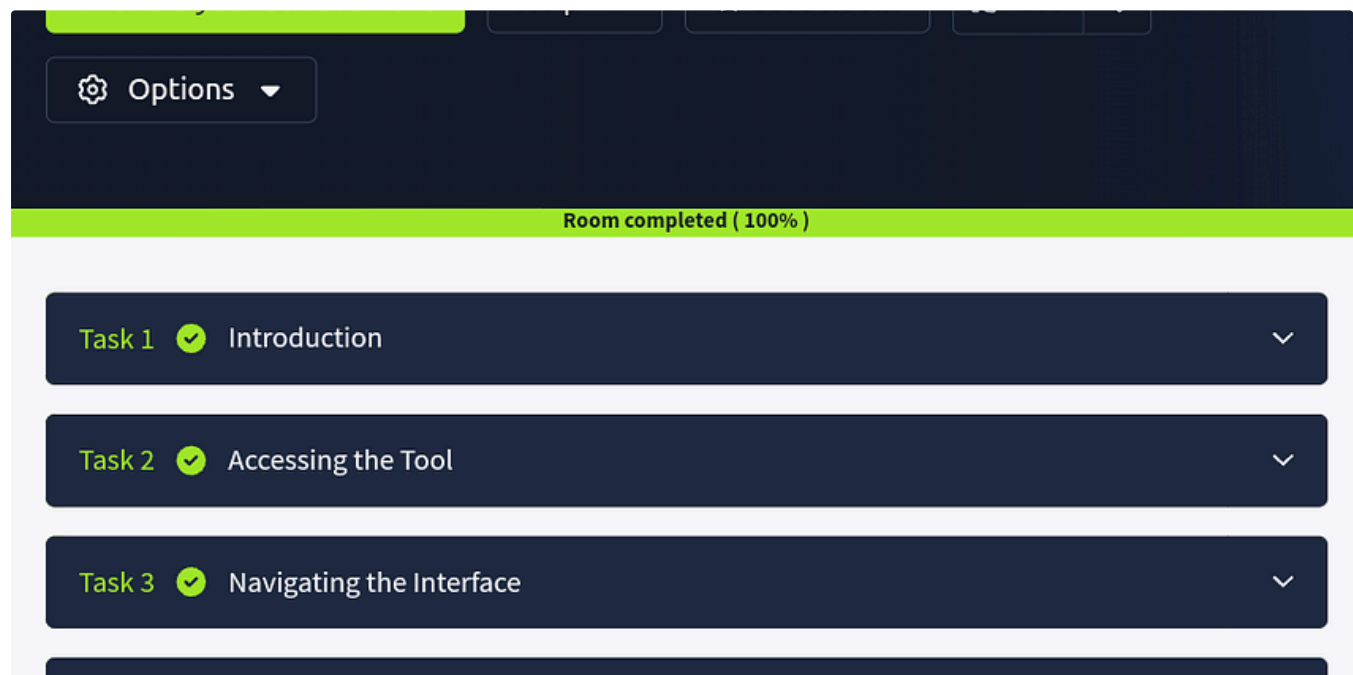
data science and AI

40 stories · 308 saves



Best of The Writing Cooperative

67 stories · 466 saves



Jawstar

CyberChef: The Basics Tryhackme Write up

Tryhackme

★ Nov 7, 2024 🖱 8



Procmon	Tracks system activity, especially for malware research, troubleshooting, and forensics.
Process Explorer	Provides insights into the parent-child relationship of processes, DLLs loaded, and paths.
HxD	Examines or alters malicious files via hex editing.
Wireshark	Investigates network traffic for unusual activity.
CFF Explorer	Generates file hashes for integrity verification and validates system file sources.
PEStudio	Static analysis tool for studying executable file properties without execution.
FLOSS	Extracts and de-obfuscates strings from malware programs using advanced



rutbar

TryHackMe—FlareVM: Arsenal of Tools | Cyber Security 101 (THM)

Arsenal of Tools In this task, we'll introduce you to tools inside FlareVM, which offers specialized tools for forensics, incident...




Oct 23, 2024



12



Cyber Security 101 > Defensive Security Tooling > FlareVM: Arsenal of Tools



FlareVM: Arsenal of Tools

Learn the arsenal of investigative tools in FlareVM.

🟢 Easy ⌚ 40 min

[Share your achievement](#) [Badge](#) [Help](#) [Save Room](#) [40](#) [Options](#)

Room completed (100%)

Task 1 Introduction

Task 2 Arsenal of Tools

Task 3 Commonly Used Tools for Investigation: Overview

Task 4 Analyzing Malicious Files!

Task 5 Conclusion




Jawstar

FlareVM: Arsenal of Tools

CYBER SECURITY 101 Tryhackme Write up

★ Oct 29, 2024 🖱 37 💬 1



 rutbar

TryHackMe—Search Skills | Cyber Security 101 (THM)

Evaluation of Search Results

★ Oct 26, 2024 💬 1



See more recommendations