




## Tryhackme – Intro to Endpoint Security

Leave a Comment / CTF, Tryhackme / By admin


In this walk through, we will be going through the Intro to Endpoint Security room from Tryhackme. In this room, we will learn about the fundamentals of endpoint security monitoring, essential tools, and high-level methodology. It gives an overview of determining a malicious activity from an endpoint and mapping its related events. So, let's get started.



### Intro to Endpoint Security

Learn about fundamentals, methodology, and tooling for endpoint security monitoring.

security soc endpoint logs

Easy 

## Task 1 – Room Introduction

## India to Dubai

from India

At the end of this room, we will have a threat simulation wherein you need to investigate and remediate the infected machines. This activity may require you first to understand the fundamentals of endpoint security monitoring to complete it.

Now, let's deep-dive into the basics of Endpoint Security!

*Answer the questions below*

I have read the introduction task.

No answer needed

Correct Answer

## Task 2 – Endpoint Security Fundamentals

**Question 1** – What is the normal parent process of services.exe?

**wininit.exe**

**Question 2** – What is the name of the network utility tool introduced in this task?

**TCPview**

*Answer the questions below*

What is the normal parent process of services.exe?

wininit.exe

Correct Answer

What is the name of the network utility tool introduced in this task?

TCPview

Correct Answer

## Task 3 – Endpoint Logging and Monitoring

**Question 1** – What is the PowerShell cmdlet for viewing Windows Event Logs?

**Question 2** – Provide the command used to enter OSQuery CLI.

**osqueryi**

**Question 3** – What does EDR mean? Provide the answer in lowercase.

**Endpoint Detecion and Response**

*Answer the questions below*

What is the PowerShell cmdlet for viewing Windows Event Logs?

Get-WinEvent

Correct Answer

Provide the command used to enter OSQuery CLI.

osqueryi

Correct Answer

What does EDR mean? Provide the answer in lowercase.

Endpoint Detecion and Response

Correct Answer

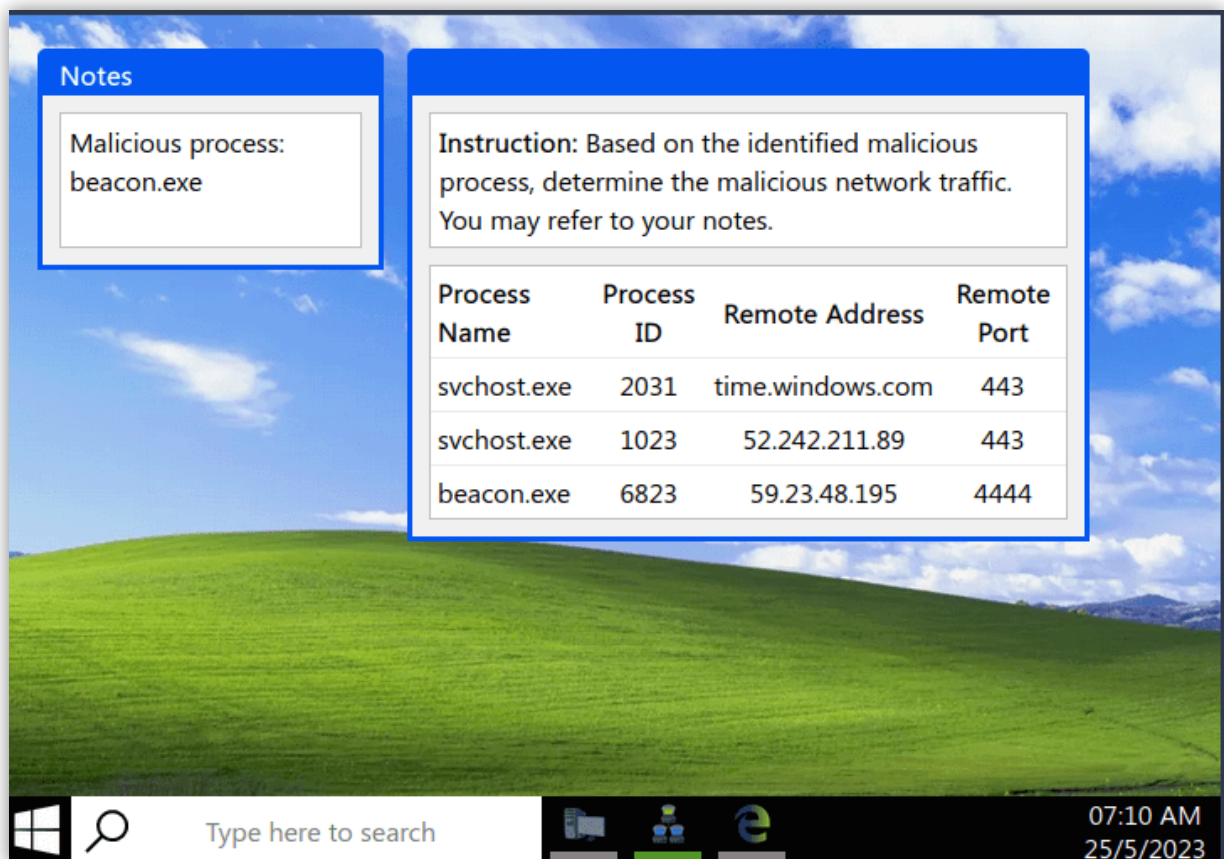
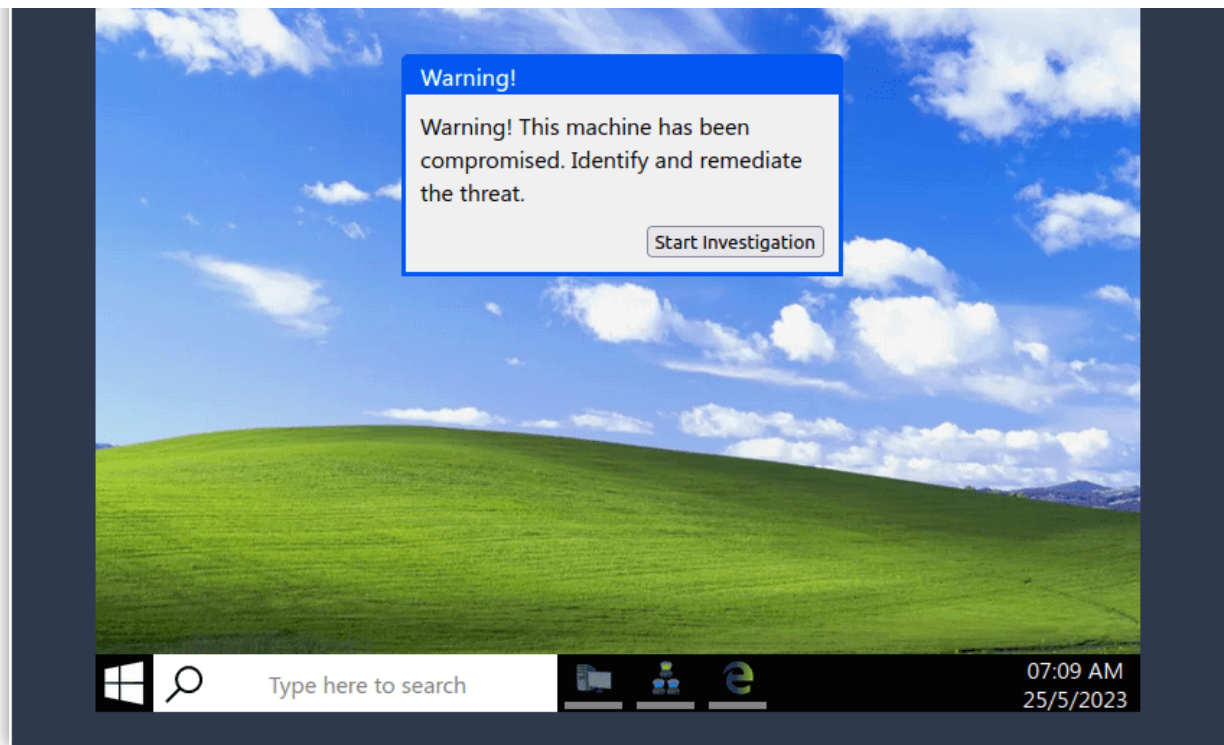
**Trending**

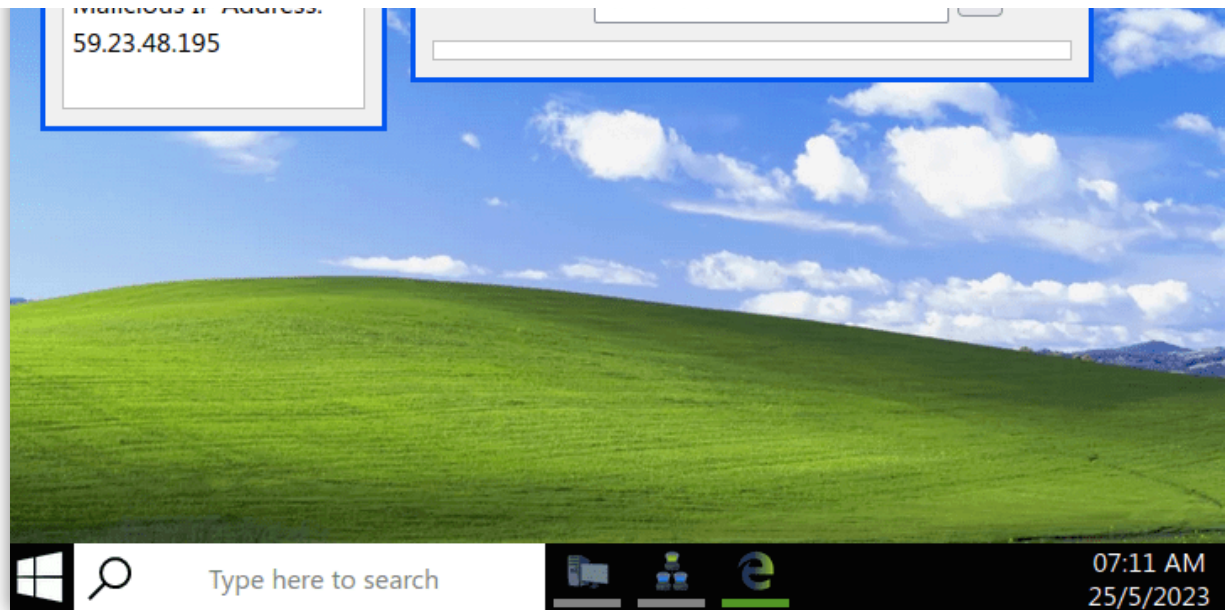
**I created a Music Player in Python – “Pythiofy”**

## Task 4 – Endpoint Log Analysis

**Question 1** – Click on the green View Site button in this task to open the Static Site Lab and start investigating the threat by following the provided instructions.

**Done**

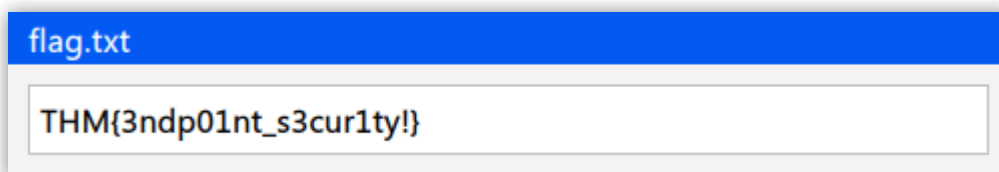
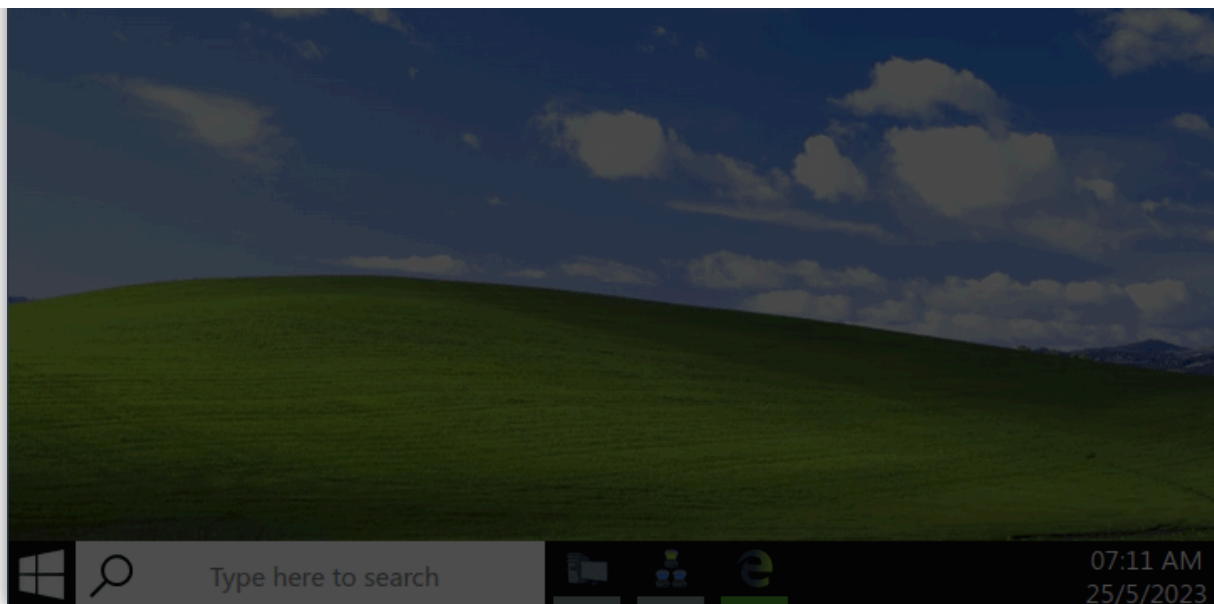




**Instruction:** Find all machines affected using the discovered IP address and eradicate the threat.

Search:

Computer Name	Remote IP Address	Action
WKSTN-1	59.23.48.195	<button>Remediate</button>
WKSTN-2	59.23.48.195	<button>Remediate</button>
WKSTN-3	59.23.48.195	<button>Remediate</button>
WKSTN-4	59.23.48.195	<button>Remediate</button>



**THM{3ndp01nt\_s3cur1ty!}**

#### Answer the questions below

Click on the green View Site button in this task to open the Static Site Lab and start investigating the threat by following the provided instructions.

No answer needed

Correct Answer

Provide the flag for the simulated investigation activity.

THM{3ndp01nt\_s3cur1ty!}

Correct Answer

## Task 5 – Conclusion

In conclusion, we covered the basic concepts of Endpoint Security Monitoring:

- **Endpoint Security Fundamentals** tackled Core Windows Processes and Sysinternals.
- **Endpoint Logging and Monitoring** introduced logging functionalities such as Windows Event Logging and Sysmon and monitoring/investigation tools such as OSQuery and Wazuh.
- **Endpoint Log Analysis** highlighted the importance of having a methodology such as baselining and event correlation.

You are now ready to deep-dive into the Endpoint Security Monitoring Module. To continue this path, you may refer to the list of rooms mentioned in the previous tasks:

- [Core Windows Processes](#)
- [Sysinternals](#)
- [Windows Event Logs](#)
- [Sysmon](#)
- [OSQuery](#)
- [Wazuh](#)

*Answer the questions below*

I have completed the Introduction to Endpoint Security Monitoring room.

No answer needed

Correct Answer

## Also Read: Tryhackme – Internal

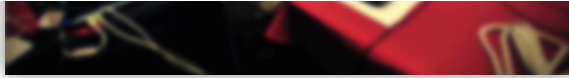
So that was “**Intro to Endpoint Security**” for you. In this room we covered the fundamentals of Endpoint security, looked into some logging and monitoring solutions and endpoint log analysis. At last, we tested the theory we have learned throughout the room with a series of questions based on a simulated investigation environment. On that note, i will take your leave but remember to “**Keep Defending**”.

← Previous Post

Next Post →

## Related Posts





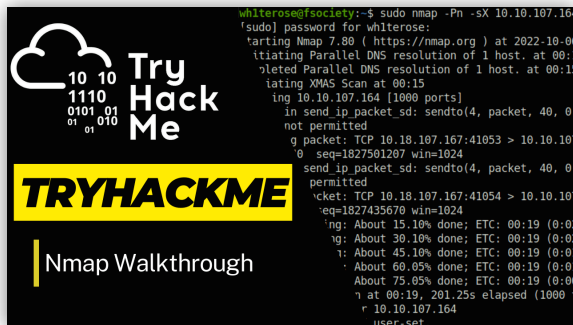
## The Ultimate Guide on How to get started in CTFs?

CTF, Cybersecurity / By admin



## Tryhackme – Tutorial

CTF, Tryhackme / By admin



## Tryhackme – Nmap

CTF, Tryhackme / By admin

# Leave a Comment

Your email address will not be published. Required fields are marked \*

Type here..





☐ Save my name, email, and website in this browser for the next time I comment.

**Post Comment »**



## Recent Posts

How to hack Android Phone using Kali Linux

Steganography: Hiding secrets like Mr. Robot

How Hackers Become Anonymous While Hacking

Hacking Windows via WhatsApp Messenger RCE

Hacking Windows with Fake Captchas

Vulnab - Media on Vulnlab – Feedback

How to hack Android Phone using Kali Linux on How Hackers Become Anonymous While Hacking

ali on How to hack Android Phone using Kali Linux

student of class 10 2024-25 on Kali-whoami – Stay Anonymous while hacking

## Archives

November 2024

October 2024

August 2024

July 2024

June 2024

May 2024

April 2024

March 2024

February 2024

January 2024

December 2023

November 2023

October 2023

September 2023

August 2023

March 2023

February 2023

December 2022

November 2022

September 2022

August 2022

July 2022

November 2021

May 2021

April 2021

November 2020

October 2020

September 2020

August 2020

July 2020

June 2020

May 2020

April 2020

June 2019

## Categories

A1 – Injection

A3 – Cross Site Scripting (XSS)

A3 – Sensitive Data Exposure

A4 – Insecure Direct Object References

A4 – XML External Entities

A5 – Broken Access Control

A5 – Security Misconfiguration

A6 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Cross Site Scripting (XSS)

Android hacking

bWAPP

Computer Science

CTF

Cybersecurity

DVWA

Electronics 101

Hack The Box

Labs

Mutillidae

Opsec

OSCP Prep

Pentesting

Programming

Projects

Research

Social Engineering

tech news

Tryhackme

Uncategorised

Vulnlab

Web Server Hacking

WebApp Hacking

Webgoat

## Meta

Log in

Entries feed

Comments feed

WordPress.org

# Who are we ?

Invent Your Shit is an online portal designed for hackers which helps them to learn ethical hacking and cybersecurity online for free. Join

# Quick Navigation

[Home](#)

[Privacy](#)

[Whoami](#)

[Contact](#)

## Contact Us

 [Contact here](#)

 [Join community](#)

Copyright © 2025 Invent Your Shit | Powered by Invent Your Shit