

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



THM | Introduction to Antivirus



Mansoor Barri · [Follow](#)

2 min read · Aug 8, 2022



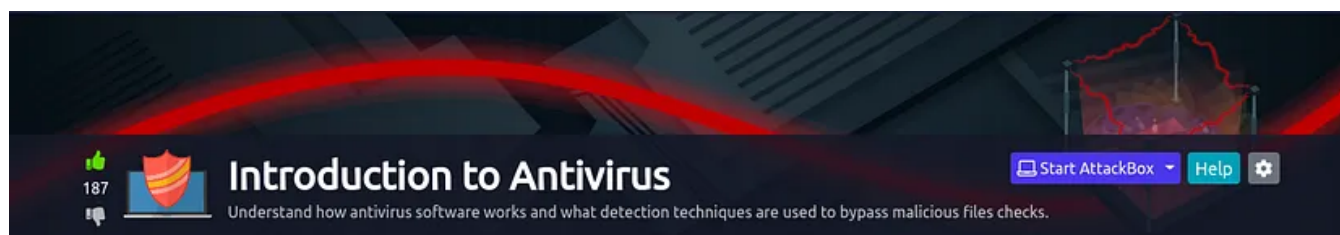
Listen



Share

... More

Room: <https://tryhackme.com/room/introtoav>



visit mansoor.cf/introtoav for detailed answers*

Task 1 Introduction

no answer needed

Task 2 — Antivirus Software [answers are from the text]

Question 1: What was the virus name that infected John McAfee's PC?

~ brain

Question 2: Which PC Antivirus vendor implemented the first AV software on the market?

~ McAfee

Question 3: Antivirus software is a _____-based security solution.

~ host

Task 3 — Antivirus Features [answers are from the text]

Question 1: Which AV feature analyzes malware in a safe and isolated environment?

~ *emulator*

Question 2: An _____ feature is a process of restoring or decrypting the compressed executable files to the original.

~ *unpacker*

Question 3

no answer needed

Task 4 — Deploy the VM

no answer needed

Task 5 — AV Static Detention

Question 1: What is the sigtool tool output to generate an MD5 of the AV-Check.exe binary?

explanation: open cmd and type this command:

```
c:\Program Files\ClamAV\sigtool.exe" --md5  
c:\Users\thm\Desktop\Samples\AV-Check.exe"
```

Question 2: Use the strings tool to list all human-readable strings of the AV-Check binary. What is the flag?

explanation open cmd and type these commands:

```
cd Desktop/Samples  
strings AV-Checks.exe | findstr "THM"
```

Task 6 — Other Detection Techniques [answer is from the text]

Question 1: Which detection method is used to analyze malicious software inside virtual environments?

~ *Dynamic Detection*

Task 7 & 8

no answer needed

that's it 🙌

Open in app ↗

Medium

🔍 Search



Follow

Written by Mansoor Barri

6 Followers · 1 Following

Profile designed to share technology content about Penetration testing, Linux and Windows.

No responses yet




What are your thoughts?

Respond

More from Mansoor Barri




 Mansoor Barri

Getting Started — PhoneInFoga

Brief

Aug 12, 2023



 Mansoor Barri

Hugo vs WordPress: A Performance and SEO Comparison

Hugo and WordPress are two well-known content management systems for building and maintaining websites. While both platforms have...

Apr 12, 2023 🖱 3




 Mansoor Barri

The Ultimate Guide to GitHub On Linux

Context

Apr 14, 2024



 Mansoor Barri

Get a Free SSL Certificate for Your GoDaddy Subdomain using SSL Generator

Prerequisites


Apr 5, 2023 🖱 2



See all from Mansoor Barri

Recommended from Medium



 Nisha P

Exploiting EternalBlue (MS17-010): A Walkthrough and Protection Measures

A detailed walkthrough of how to exploit the Eternal Blue vulnerability on a Windows 7 Ultimate machine, covering both manual and automated...

Nov 3, 2024 🖱 60





 In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60

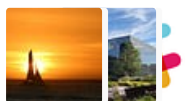


Lists



Staff picks

804 stories · 1587 saves



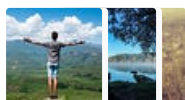
Stories to Help You Level-Up at Work

19 stories · 924 saves



Self-Improvement 101

20 stories · 3240 saves



Productivity 101

20 stories · 2739 saves



IritT

CyberChef: The Basics—Crypto 101—Defensive Security Tooling-Cryptography-TryHackMe Walkthrough

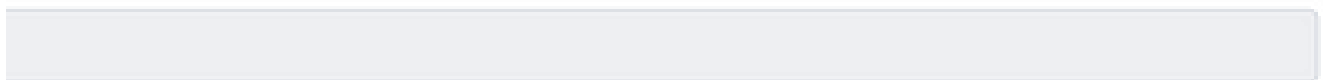
This room is an introduction to CyberChef, the Swiss Army knife for cyber security professionals.

Nov 2, 2024



erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa

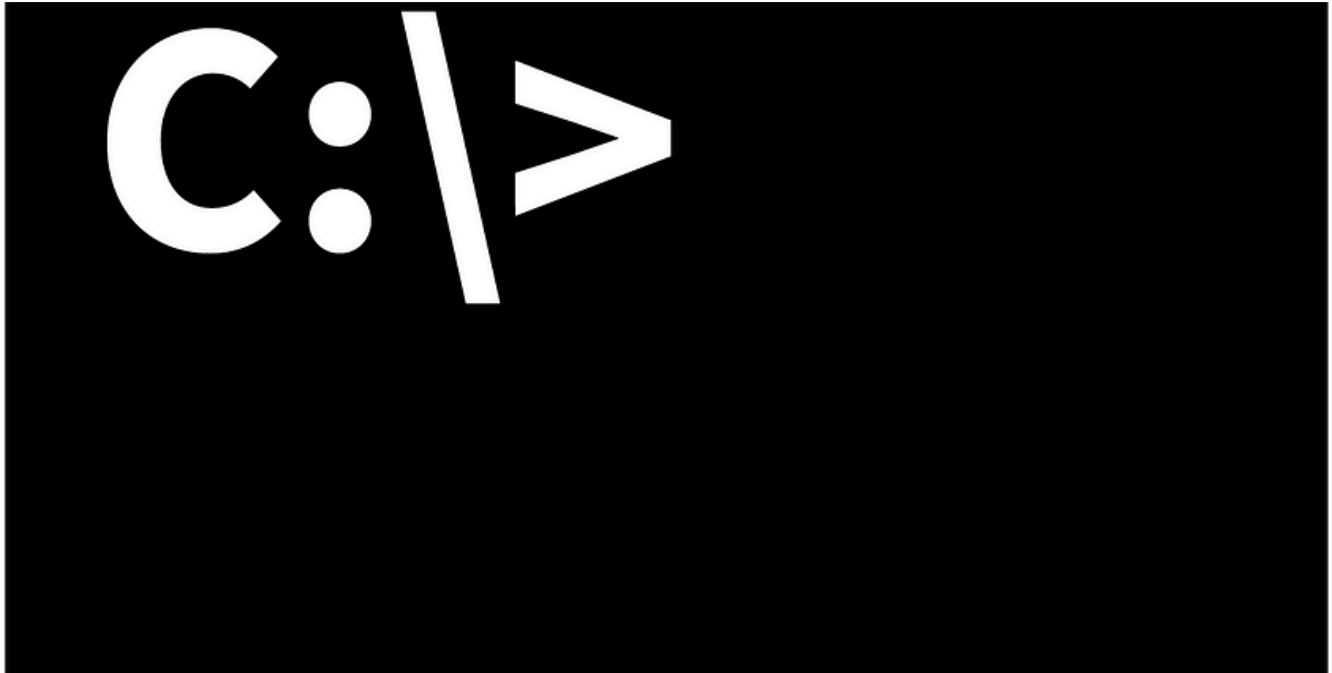


Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024



In System Weakness by Sunny Singh Verma [SuNnY]

Windows Command Line [CyberSecurity 101 Learning Path] TryHackMe Writeup | Detailed Walkthrough |...

Windows Command Line is a Part of The Learning Path From the Newly updated Cyber Security 101 Path on TryHackMe

Oct 26, 2024 🖱 67





TheHiker

Silver-Platter , TryHackMe Walkthrough | TheHiker

Hello everyone, today I'll be covering the "Silver-Platter" room on TryHackMe. I think that this room is great for intermediate students...

Jan 12  27[See more recommendations](#)