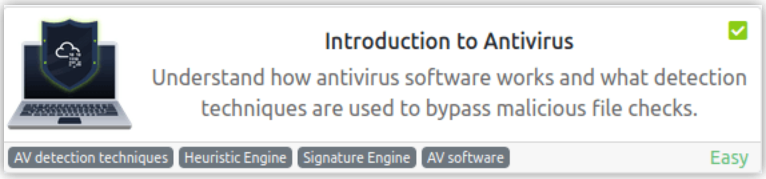
Invent Your Shit

Tryhackme – Introduction to Antivirus

Leave a Comment / CTF, Tryhackme / By admin

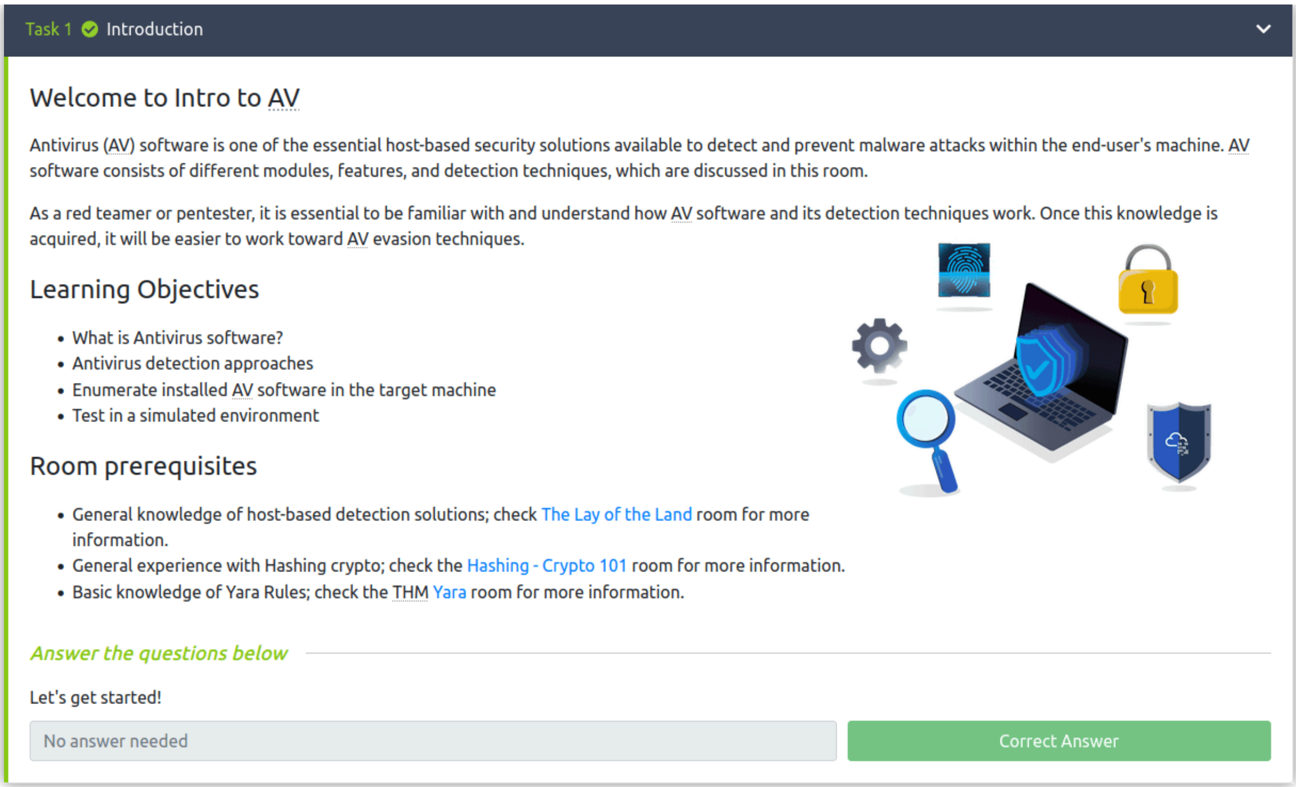
In this walk through, we will be going through the Introduction to Antivirus room from Tryhackme. In this room, we will understand how antivirus software works and what detection techniques are used to bypass malicious file checks. So, let's get started without any delay.


Introduction to Antivirus

Understand how antivirus software works and what detection techniques are used to bypass malicious file checks.

Table of Contents

Task 1 – Introduction



Welcome to Intro to AV

Antivirus (AV) software is one of the essential host-based security solutions available to detect and prevent malware attacks within the end-user's machine. AV software consists of different modules, features, and detection techniques, which are discussed in this room.

As a red teamer or pentester, it is essential to be familiar with and understand how AV software and its detection techniques work. Once this knowledge is acquired, it will be easier to work toward AV evasion techniques.

Learning Objectives

- What is Antivirus software?
- Antivirus detection approaches
- Enumerate installed AV software in the target machine
- Test in a simulated environment

Room prerequisites

- General knowledge of host-based detection solutions; check The Lay of the Land room for more information.
- General experience with Hashing crypto; check the Hashing - Crypto 101 room for more information.
- Basic knowledge of Yara Rules; check the THM Yara room for more information.

Answer the questions below

Let's get started!

No answer needed

Task 2 – Antivirus Software

Question 1 – What does AV mean?

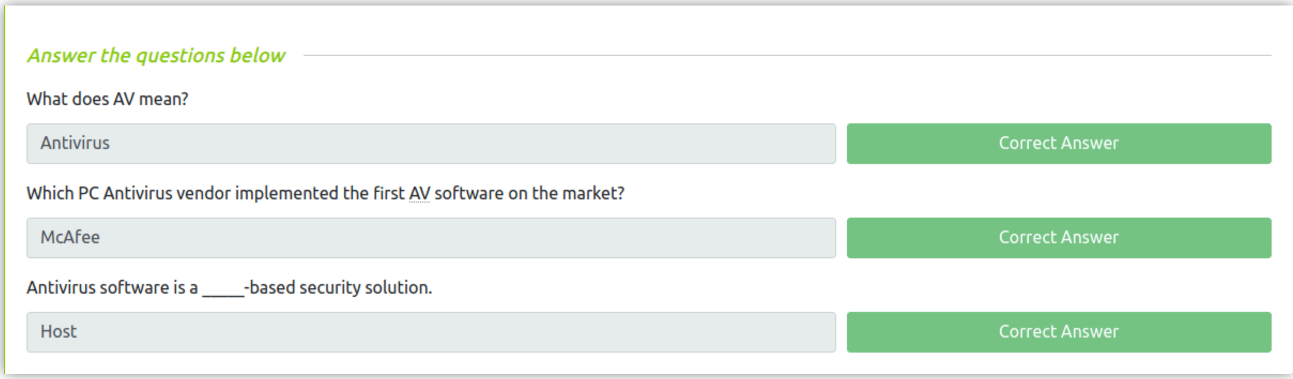
```
Antivirus
```

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
```



Answer the questions below

What does AV mean?

Antivirus

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

McAfee

Antivirus software is a _____-based security solution.

Host

Task 3 – Antivirus Features

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

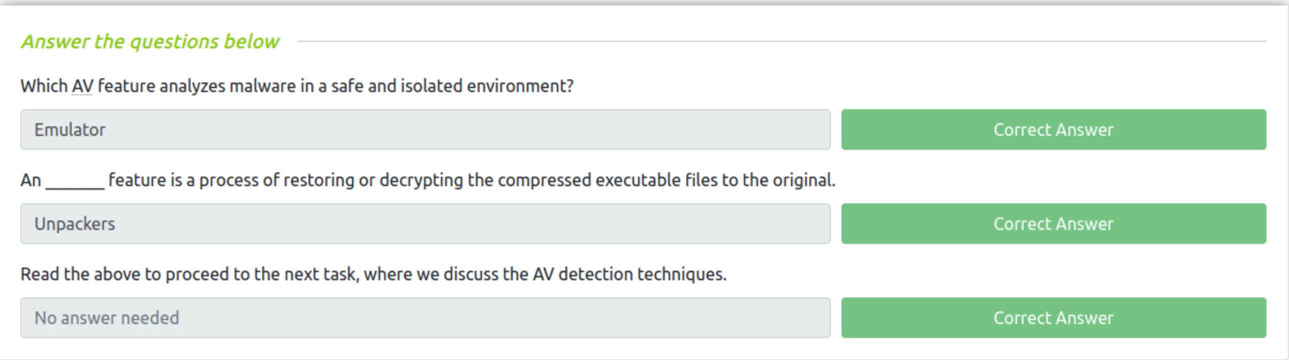
```
Emulator
```

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

```
Unpackers
```

Question 3 – Read the above to proceed to the next task, where we discuss the AV detection techniques.

```
Done
```



Answer the questions below

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

Emulator

An _______ feature is a process of restoring or decrypting the compressed executable files to the original.

Unpackers

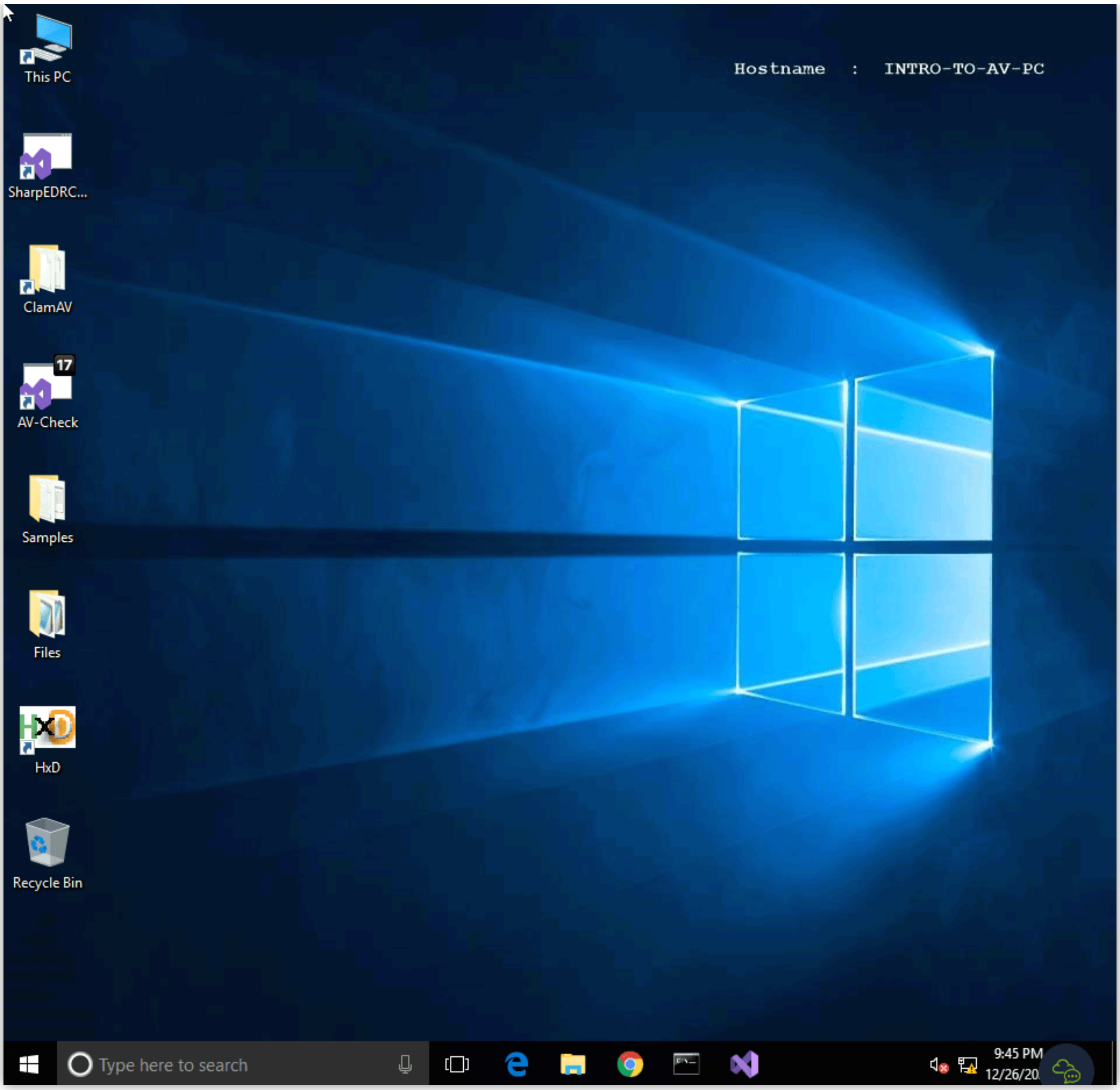
Read the above to proceed to the next task, where we discuss the AV detection techniques.

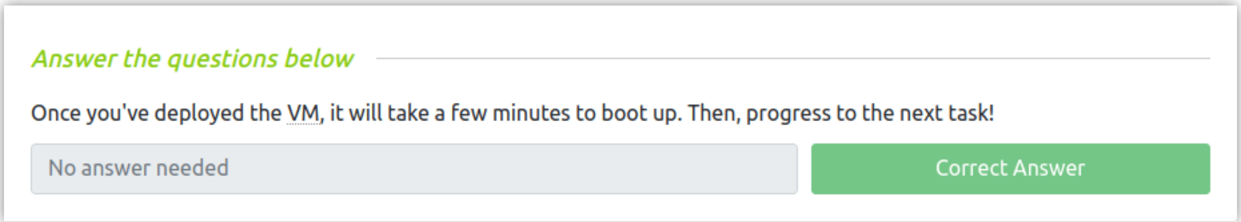
No answer needed

Task 4 – Deploy the VM

Question 1 – Once you've deployed the VM, it will take a few minutes to boot up. Then, progress to the next task!

```
Done
```





Answer the questions below

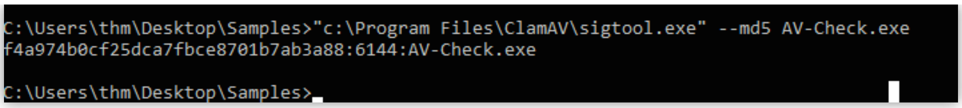
Once you've deployed the VM, it will take a few minutes to boot up. Then, progress to the next task!

No answer needed

Task 5 – AV Static Detection

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

```
"c:\Program Files\ClamAV\sigtool.exe" --md5 AV-Check.exe
```

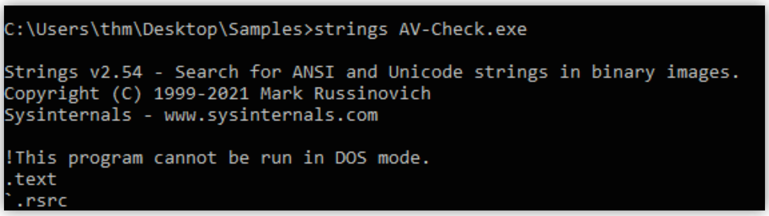


```
C:\Users\thm\Desktop\Samples>"c:\Program Files\ClamAV\sigtool.exe" --md5 AV-Check.exe
f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Check.exe

C:\Users\thm\Desktop\Samples>_
```

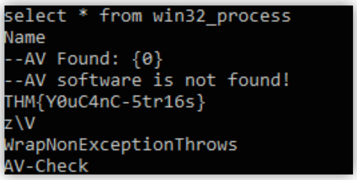
`f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Check.exe`

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

```
strings AV-Check.exe
```

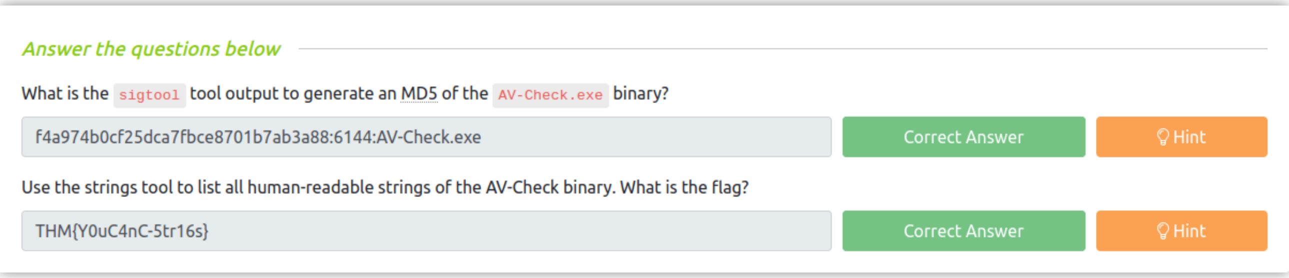


```
C:\Users\thm\Desktop\Samples>strings AV-Check.exe

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
.text
`.rsrc
```



```
select * from win32_process
Name
--AV Found: {0}
--AV software is not found!
THM{Y0uC4nC-5tr16s}
z\V
WrapNonExceptionThrows
AV-Check
```

`THM{Y0uC4nC-5tr16s}`



Answer the questions below

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

f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Check.exe

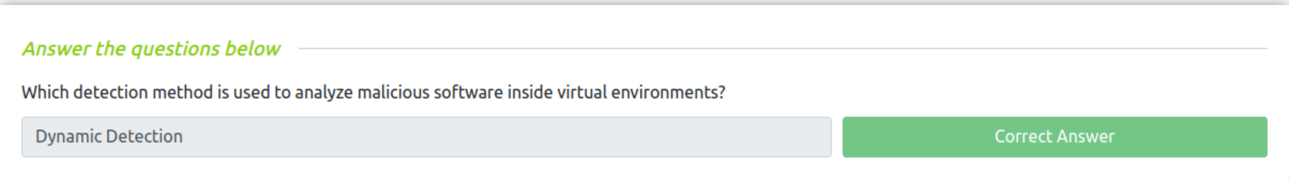
Use the strings tool to list all human-readable strings of the AV-Check binary. What is the flag?

THM{Y0uC4nC-5tr16s}

Task 6 – Other Detection Techniques

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

`Dynamic Detection`



Answer the questions below

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

Dynamic Detection

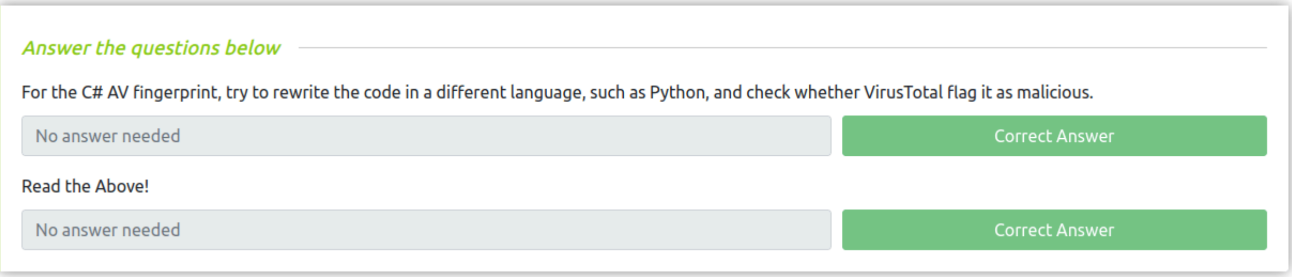
Task 7 – AV Testing and Fingerprinting

Question 1 – For the C# AV fingerprint, try to rewrite the code in a different language, such as Python, and check whether VirusTotal flag it as malicious.

```
Done
```

Question 2 – Read the Above!

```
Done
```



Answer the questions below

For the C# AV fingerprint, try to rewrite the code in a different language, such as Python, and check whether VirusTotal flag it as malicious.

No answer needed

Correct Answer

Read the Above!

No answer needed

Correct Answer

Task 8 – Conclusion

Task 8 - Conclusion

Also Read: DVWA – Weak Session IDs (Low/Med/High)

So that was **"Introduction to Antivirus"** for you. We looked into the basics of Anti-virus software and how it works. Post that, we took a deep dive into static malware detection and At last, completed the room by looking into Other detection techniques, malware testing and fingerprinting. On that note, i would take your leave and will meet you in next one. Till then, **"Happy hacking"**.

← Previous Post Next Post →

Related Posts

The Ultimate Guide on How to get started in CTFs?

The Ultimate Guide on How to get started in CTFs?
CTF, Cybersecurity / By admin

Tryhackme – Tutorial

Tryhackme – Tutorial
CTF, Tryhackme / By admin

Tryhackme - Nmap Walkthrough

Tryhackme – Nmap
CTF, Tryhackme / By admin

Leave a Comment

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

Type here..

□ I'm not a robot

reCAPTCHA
Privacy - Terms

Name*

Email*

Website

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

Post Comment »

Search...

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

Recent Comments

Varun on How to hack Android Phone using Kali Linux

Rahul on How to hack Android Phone using Kali Linux

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

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

July 2023

June 2023

May 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

A1 – Injection

A2 – Broken Auth & Session Management

A2 – Broken Auth & Session Mgmt.

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

Proving Grounds

Python

Python 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 now and head-start your hacking journey with us.

Quick Navigation

Home

Privacy

Whoami

Contact

Contact Us

Contact here

Join community