EX.NO:10 **NAME:KALAIYARASI.M**

DATE:9/4/25 **ROLLNO:231901503**

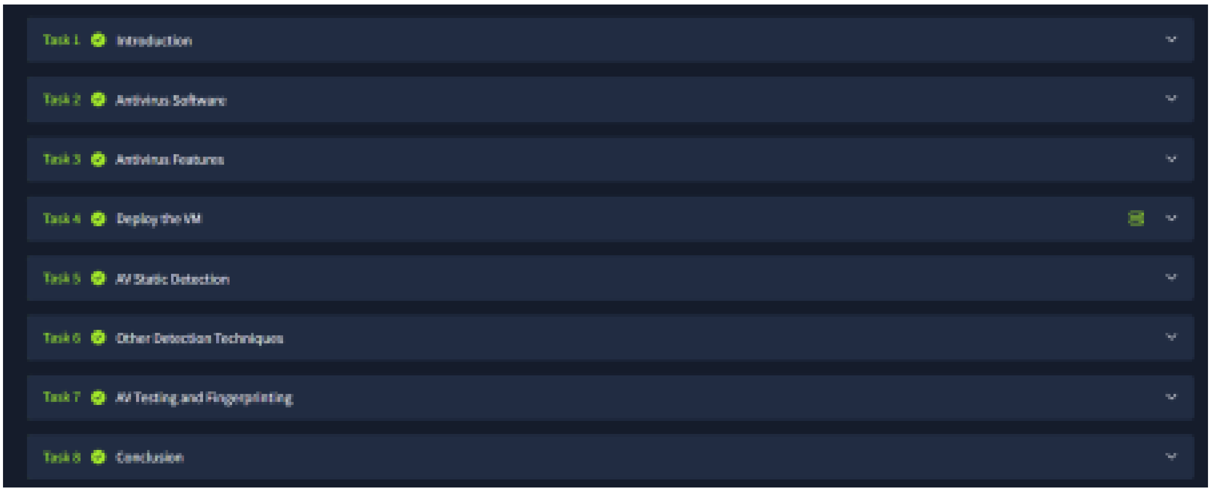
Introduction to Antivirus

AIM:

To learn about antivirus software and detection techniques used to bypass malicious file checks.

PROCEDURE:

Complete the given task as per the instructions.



Task 1 ✓ Introduction

Task 2 ✓ Antivirus Software

Task 3 ✓ Antivirus Features

Task 4 ✓ Deploy the VM

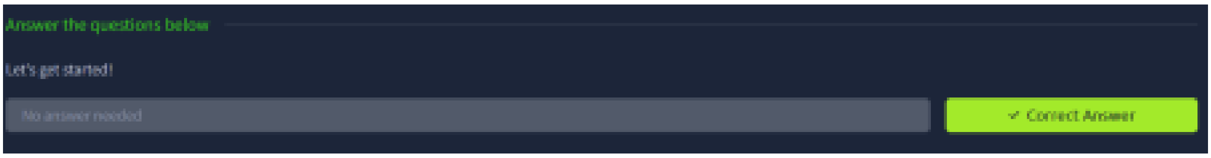
Task 5 ✓ AV Static Detection

Task 6 ✓ Other Detection Techniques

Task 7 ✓ AV Testing and Fingerprinting

Task 8 ✓ Conclusion

Task 1:Introduction

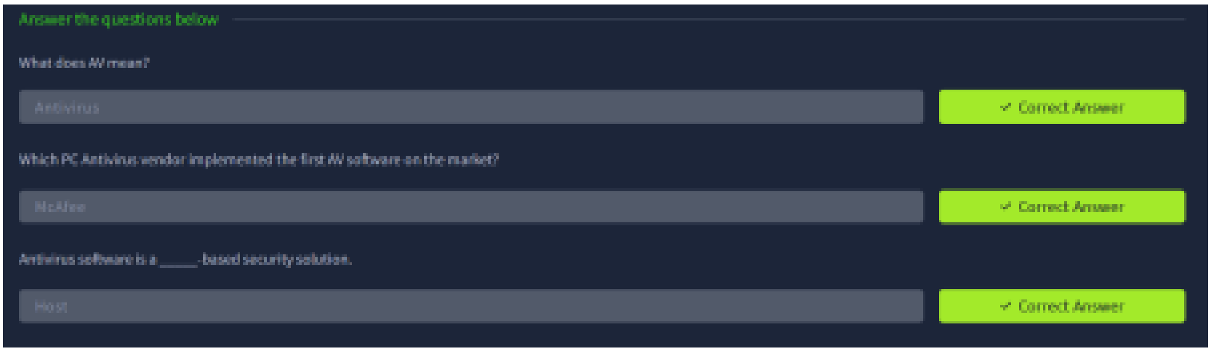


Answer the questions below

Let's get started!

No answer needed

Task 2:Antivirus Software



Answer the questions below

What does AV mean?

Antivirus

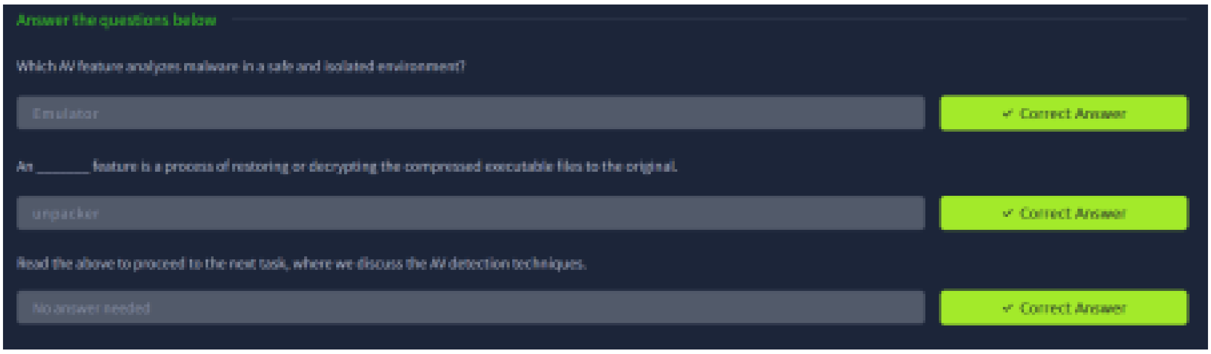
Which PC Antivirus vendor implemented the first AV software on the market?

McAfee

Antivirus software is a _____-based security solution.

Host

Task 3:Antivirus Features



Answer the questions below

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

Emulator

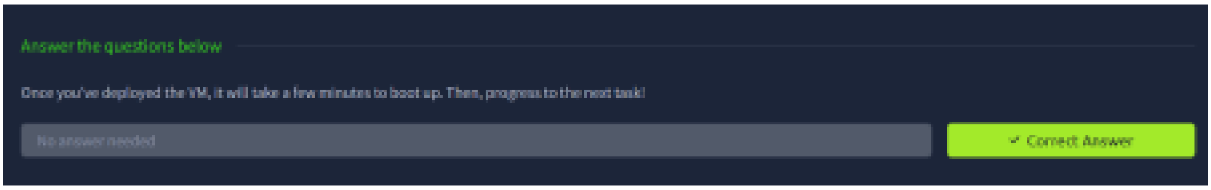
An _______ feature is a process of restoring or decrypting the compressed executable files to the original.

unpacker

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

No answer needed

Task 4:Deploy the VM

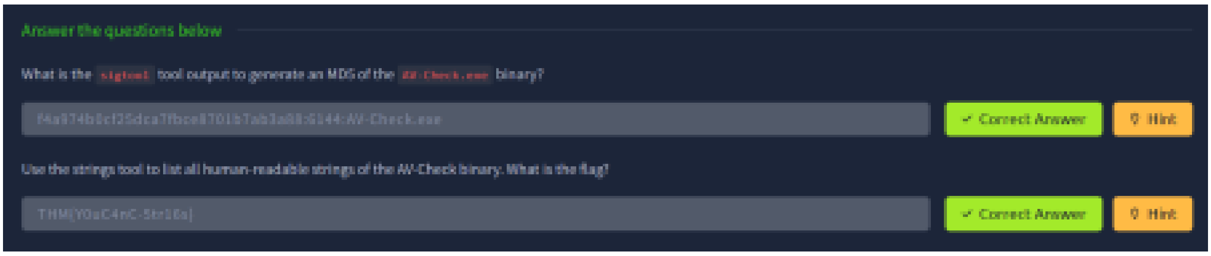


Answer the questions below

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



Answer the questions below

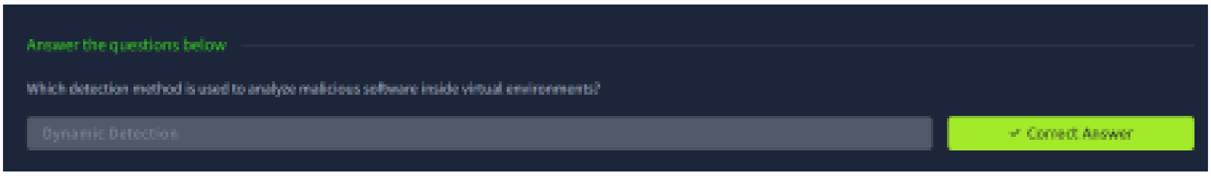
What is the `sigtool` tool output to generate an MD5 of the `AV-Check.exe` binary?

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

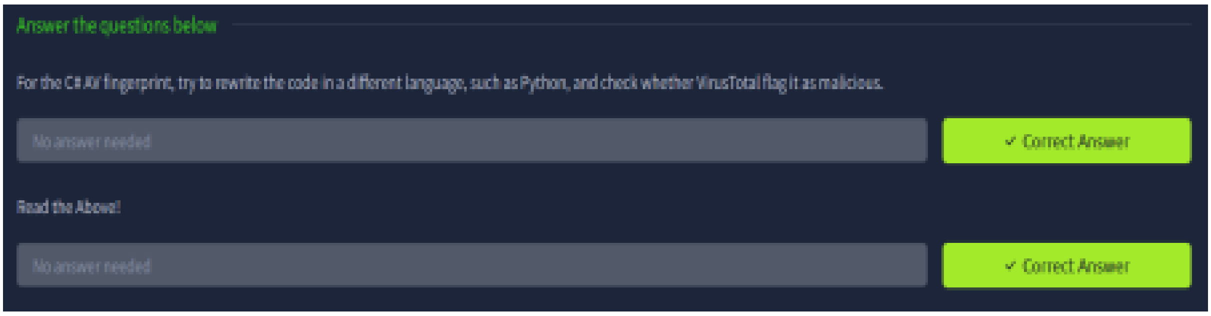


Answer the questions below

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

Dynamic Detection

Task 7:AV Testing and Fingerprinting



Answer the questions below

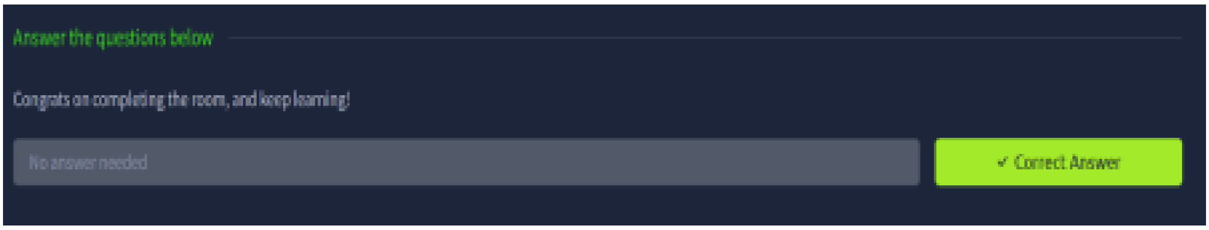
For the C# AV fingerprint, try to rewrite the code in a different language, such as Python, and check whether VirusTotal flag it as malicious.

No answer needed

Read the Above!

No answer needed

Task 8:Conclusion



Answer the questions below

Congrats on completing the room, and keep learning!

RESULT:

Thus, the experiment is completed successfully in try hack me platform.