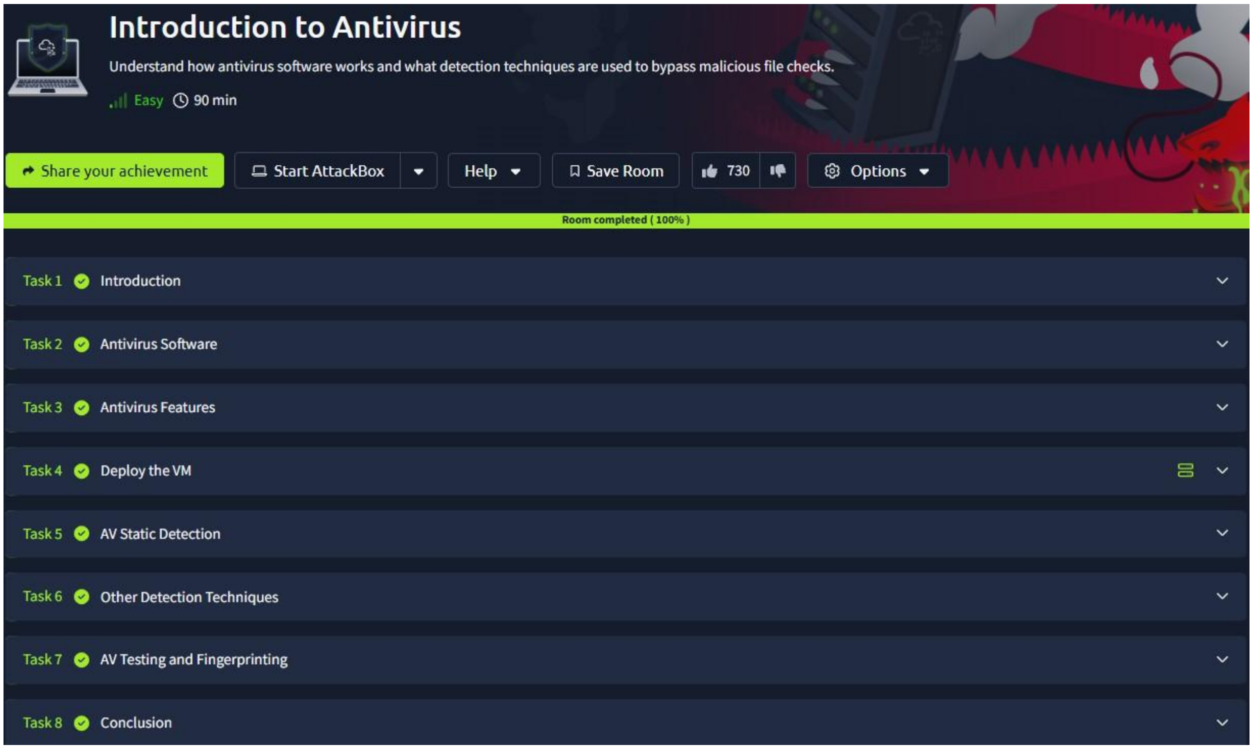
THARUN H **231901055**

EXERCISE 10
Explore Antivirus Detection Techniques

Aim: To understand how antivirus software detects malicious files and explore common techniques used to bypass these detections.



Introduction to Antivirus

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

Easy 90 min

Task 1 ✓ Introduction

Task 2 ✓ Antivirus Software

Task 3 ✓ Antivirus Features

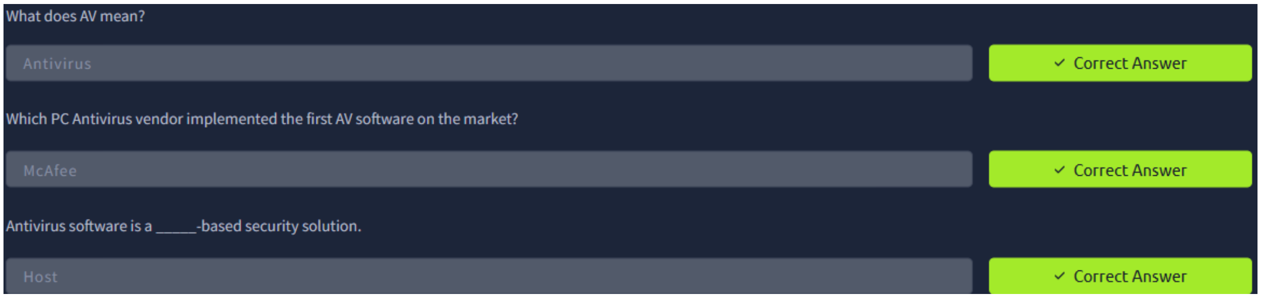
Task 4 ✓ Deploy the VM

Task 5 ✓ AV Static Detection

Task 6 ✓ Other Detection Techniques

Task 7 ✓ AV Testing and Fingerprinting

Task 8 ✓ Conclusion



What does AV mean?

Antivirus

✓ Correct Answer

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

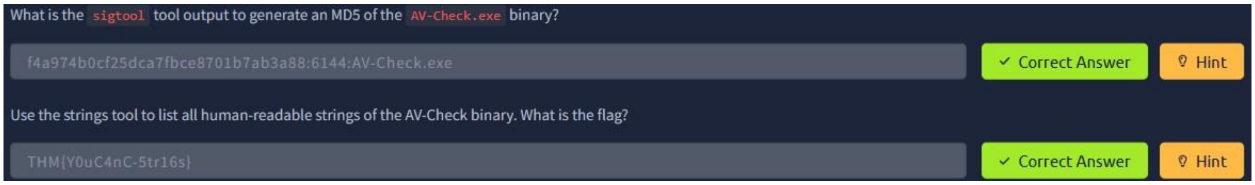
McAfee

✓ Correct Answer

Antivirus software is a _____-based security solution.

Host

✓ Correct Answer



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

f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Check.exe

✓ Correct Answer

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

THM{Y0uC4nC-5tr16s}

✓ Correct Answer

Result: Successfully learned antivirus detection mechanisms such as signature-based and heuristic analysis, and applied basic evasion techniques to bypass malicious file checks.