

EX.No:10

Explore Antivirus Detection Techniques

DATE:16/04/2025

NAME: M.A.MADHESH

ROLL.NO:231901029

AIM:

To understand how antivirus software works and what detection techniques are used to bypass malicious file checks

TryHackMe

Dashboard Learn Compete Other

Access Machines Go Premium 1

Learn > Introduction to Antivirus

Introduction to Antivirus

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

Easy 90 min

Share your achievement Start AttackBox Help Save Room 734 Options

Room completed (100%)

- 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 02: Antivirus

Answer the questions below

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

Task 03: Antivirus Feature

Answer the questions below

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

Emulator

✓ Correct Answer

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

unpacker

✓ Correct Answer

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

No answer needed

✓ Correct Answer

Task 04: 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

✓ Correct Answer

Task 05: 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

✓ Correct Answer

🔍 Hint

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

THM[Y0uC4nC-5tr16s]

✓ Correct Answer

🔍 Hint

Task 06: Other Detection Technique

Answer the questions below

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

Dynamic Detection

✓ Correct Answer

Task 07: 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

✓ Correct Answer

Read the Above!

No answer needed

✓ Correct Answer