EX NO : 10 EXPLORE ANTIVIRUS DETECCTION NAME : JASON FREDDY

DATE : 16.04.2025 TECHNIQUES ROLL NO : 231901014

AIM :

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

TASK 2 : ANTIVIRUS SOFTWARE

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 3 : ANTIVIRUS FEATURES

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 4 : DEPLOY THE VM

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 5 : AV STATIC DETECTION

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

f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Chec ✓ 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 6 : OTHER DETECTION TECHNIQUES

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

Dynamic Detection ✓ Correct Answer

TASK 7 : AV TESTING AND FINGERPRINTING

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

CONCLUSION :

Tor network for anonymous communication task is successfully explored.