EX NO: 10 EXPLORE ANTIVIRUS DETECCTION TECHNIQUES ROLL

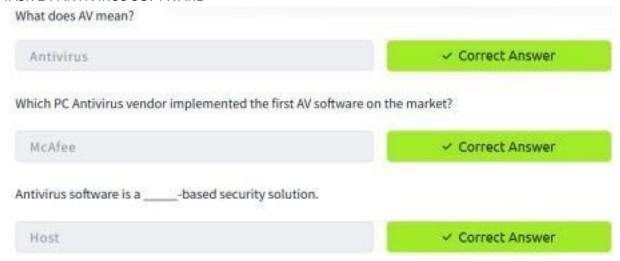
DATE:16/4/25 231901016

Jose Mugilan D

AIM:

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

TASK 2: ANTIVIRUS SOFTWARE



TASK 3: ANTIVIRUS FEATURES Which AV feature analyzes malware in a safe and isolated environment? Correct Answer Emulator An ______ feature is a process of restoring or decrypting the compressed executable files to the original. Correct Answer unpacker 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 V. Hint Use the strings tool to list all human-readable strings of the AV-Check binary. What is the flag? THM[YDuC4nC-5tr16s] Correct Answer O Hint TASK 6: OTHER DETECTION TECHNIQUES Which detection method is used to analyze malicious software inside virtual environments? Correct Answer Dynamic Detection

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.



CONCLUSION:

Thus the Anti virus experiment is successfully completed and executed