EXPLORE ANTIVIRUS DETECCTION

NAME: NAVEEN CH

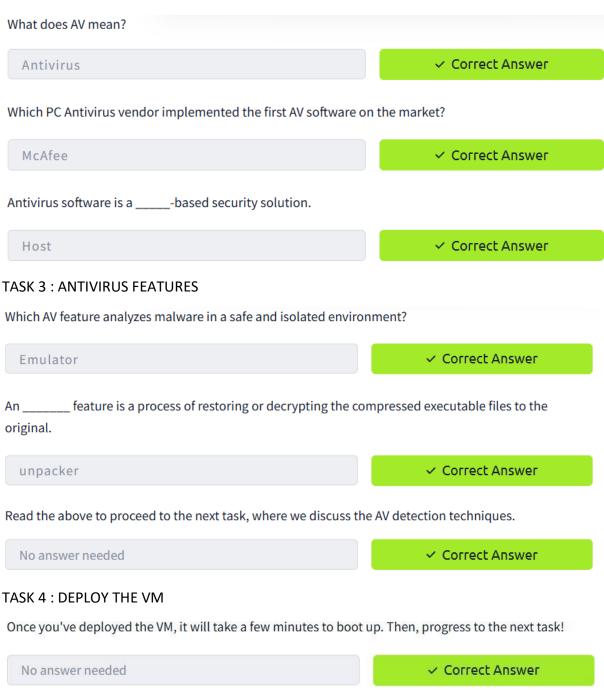
DATE: 16.04.2025 TECHNIQUES. ROLL NO: 231901033

AIM:

EX NO: 10

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

TASK 2: ANTIVIRUS SOFTWARE



TASK 5: AV STATIC DETECTION

What is the sigtool tool output to generate an MD5 of the AV-Check.exe binary? Q Hint f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Chec ✓ Correct Answer Use the strings tool to list all human-readable strings of the AV-Check binary. What is the flag? Correct Answer ∀ Hint THM{Y0uC4nC-5tr16s} **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. ✓ Correct Answer No answer needed Read the Above!

✓ Correct Answer

CONCLUSION:

No answer needed

Tor network for anonymous communication task is successfully explored.