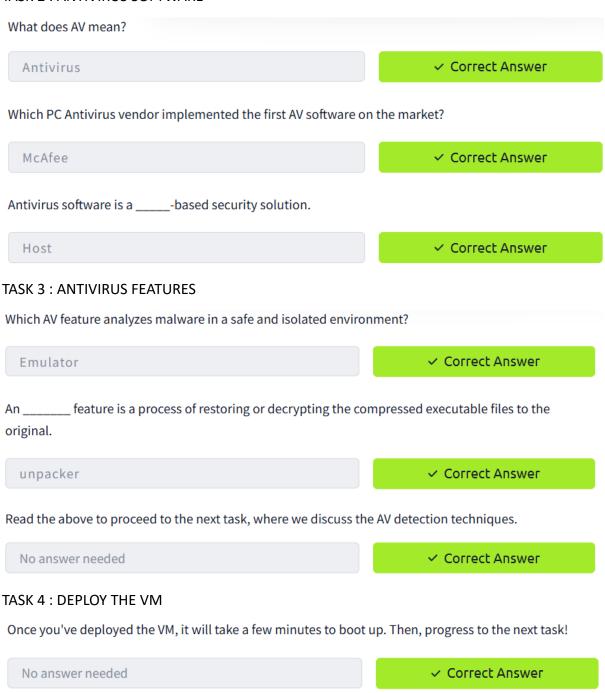
EX NO : 10 EXPLORE ANTIVIRUS DETECCTION NAME : KAVIYA V

DATE: 16.04.2025 TECHNIQUES ROLL NO: 231901020

#### AIM:

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 <u>sigtool</u> tool output to generate an MD5 of the <u>AV-Check.exe</u> binary?

f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Chec

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

✓ Correct Answer

## 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.



# **CONCLUSION:**

Tor network for anonymous communication task is successfully explored.