Buffer Overflow Prep

EX.NO:05

DATE: 19-032025

AIM:

Practice stack based buffer overflows!

PROCEDURE:

- Task 1 Deploy VM
- Task 2 oscp.exe OVERFLOW1
- Task 3 oscp.exe OVERFLOW2
- Task 4 oscp.exe OVERFLOW3
- Task 5 oscp.exe OVERFLOW4
- Task 6 oscp.exe OVERFLOW5
- Task 7 oscp.exe OVERFLOW6
- Task 8 oscp.exe OVERFLOW7
- Task 9 oscp.exe OVERFLOW8
- Task 10 oscp.exe OVERFLOW9
- Task 11 oscp.exe OVERFLOW10 Task 1 Deploy VM:



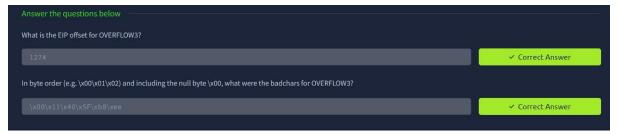
Task 2 oscp.exe - OVERFLOW1:



Task 3 oscp.exe - OVERFLOW2:



Task 4 oscp.exe - OVERFLOW3:



Task 5 oscp.exe - OVERFLOW4:



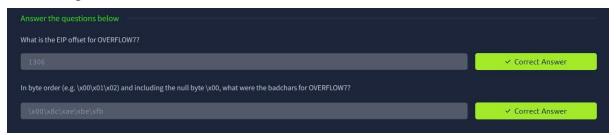
Task 6 oscp.exe - OVERFLOW5:



Task 7 oscp.exe - OVERFLOW6:



Task 8 oscp.exe - OVERFLOW7:



Task 9 oscp.exe - OVERFLOW8:



Task 10 oscp.exe - OVERFLOW9:

Answer the questions below	
What is the EIP offset for OVERFLOW9?	
	✓ Correct Answer
In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW9?	
	✓ Correct Answer

Task 11 oscp.exe - OVERFLOW10:



RESULT:

Thus the Buffer Overflow Prep is completed using tryhackme platform.