Stack based buffer overflow attacks

ROLL NO: 231901020

DATE: 19.03.2025 NAME: KAVIYA V

AIM:

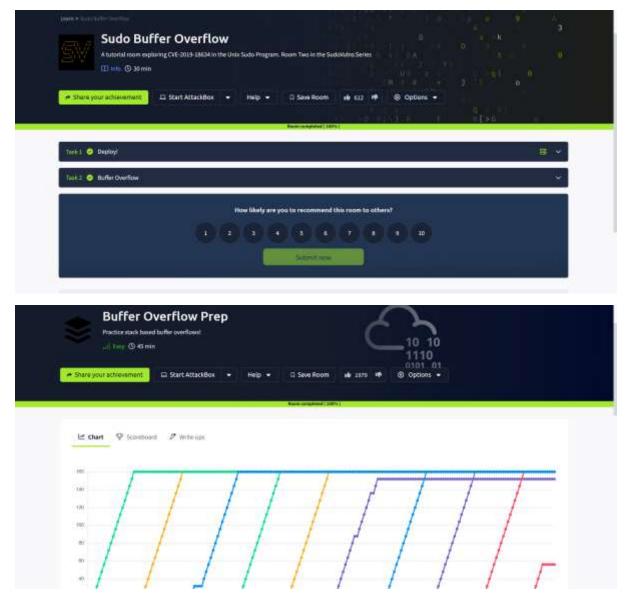
EX.NO: 5

Sudo Buffer Overflow

Exploring CVE-2019-18634 in the Unix sudo program. Room two in the SudoVulns series

Buffer Overflow Prep

Practice stack based buffer overflows!



TASK 2: BUFFER OVERFLOW

Use the pre-compiled exploit in the VM to get a root shell. No answer needed ✓ Correct Answer What's the flag in /root/root.txt? THM{buff3r_0v3rfl0w_rul3s} ✓ Correct Answer **Buffer Overflow Prep** TASK 2 oscp.exe - OVERFLOW1 What is the EIP offset for OVERFLOW1? ✓ Correct Answer 1978 In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW1? \x00\x07\x2e\xa0 ✓ Correct Answer ♥ Hint TASK 3 : oscp.exe - OVERFLOW2 What is the EIP offset for OVERFLOW2? ✓ Correct Answer 634 In byte order (e.g. $\x00\x01\x02$) and including the null byte $\x00$, what were the badchars for

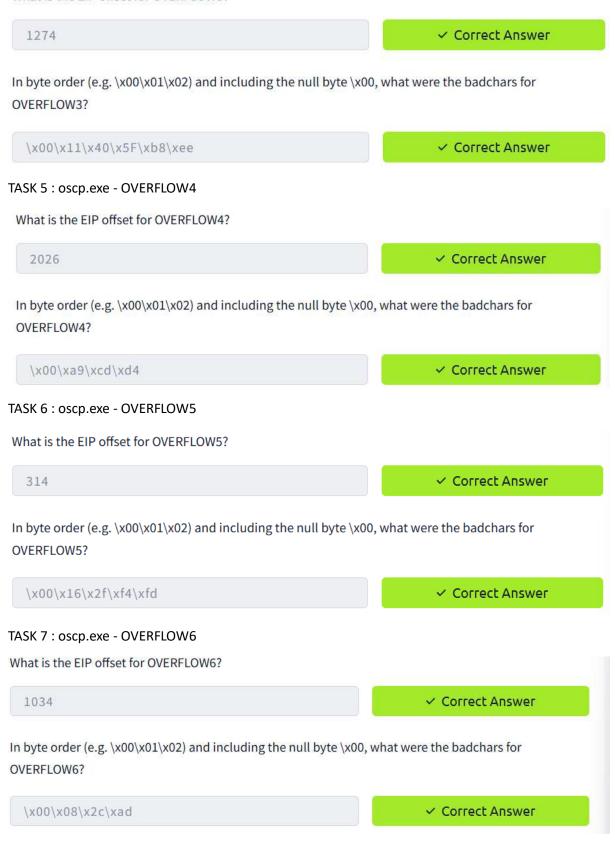
✓ Correct Answer

OVERFLOW2?

x00x23x3cx83xba

TASK 4 oscp.exe – OVERFLOW3

What is the EIP offset for OVERFLOW3?



TASK 8 : oscp.exe - OVERFLOW7

What is the EIP offset for OVERFLOW7?

1306 ✓ Correct Answer In byte order (e.g. $\x00\x01\x02$) and including the null byte $\x00$, what were the badchars for **OVERFLOW7?** ✓ Correct Answer $x00\\x8c\\xe\\xbe\\xfb$ TASK 9: oscp.exe - OVERFLOW8 What is the EIP offset for OVERFLOW8? 1786 ✓ Correct Answer In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for **OVERFLOW8?** $\x00\x1d\x2e\xc7\xee$ ✓ Correct Answer TASK 10: oscp.exe - OVERFLOW9 What is the EIP offset for OVERFLOW9? ✓ Correct Answer 1514 In byte order (e.g. $\x00\x01\x02$) and including the null byte $\x00$, what were the badchars for **OVERFLOW9?** ✓ Correct Answer x00x04x3ex3fxe1TASK 11: oscp.exe - OVERFLOW10 What is the EIP offset for OVERFLOW10? ✓ Correct Answer 537 In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW10? $x00\xa0\xad\xbe\xde\xef$ ✓ Correct Answer

CONCLUSION:

 $\label{thm:completed} \textbf{Tryhackme platform Stack based buffer overflow attacks task is successfully completed.}$