Stack based buffer overflow attacks

DATE: 19.03.2025 NAME: JAISURYA

ROLL NO: 231901063

AIM:

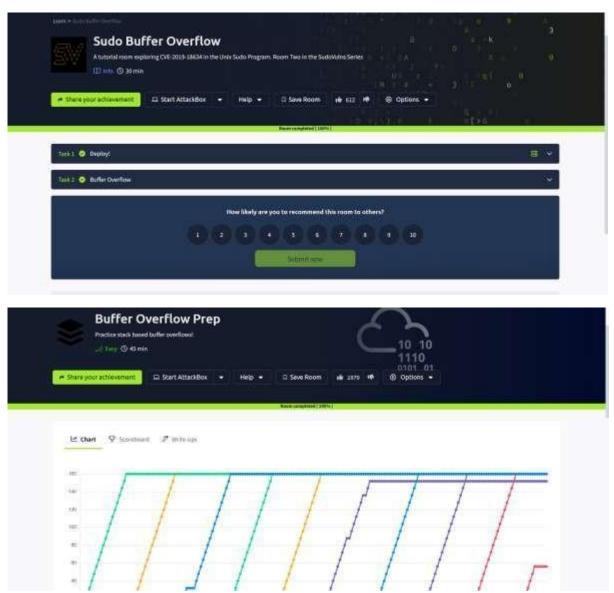
EX.NO: 5

Sudo Buffer Overflow

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

Buffer Overflow Prep

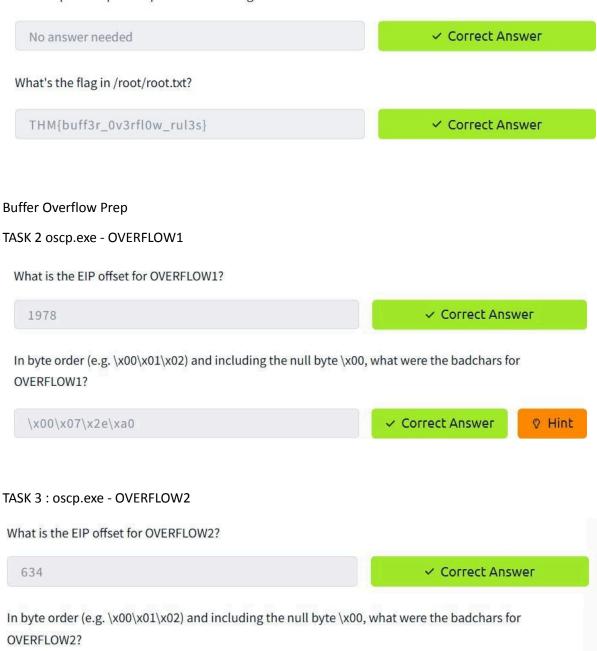
Practice stack based buffer overflows!



TASK 2: BUFFER OVERFLOW

Use the pre-compiled exploit in the VM to get a root shell.

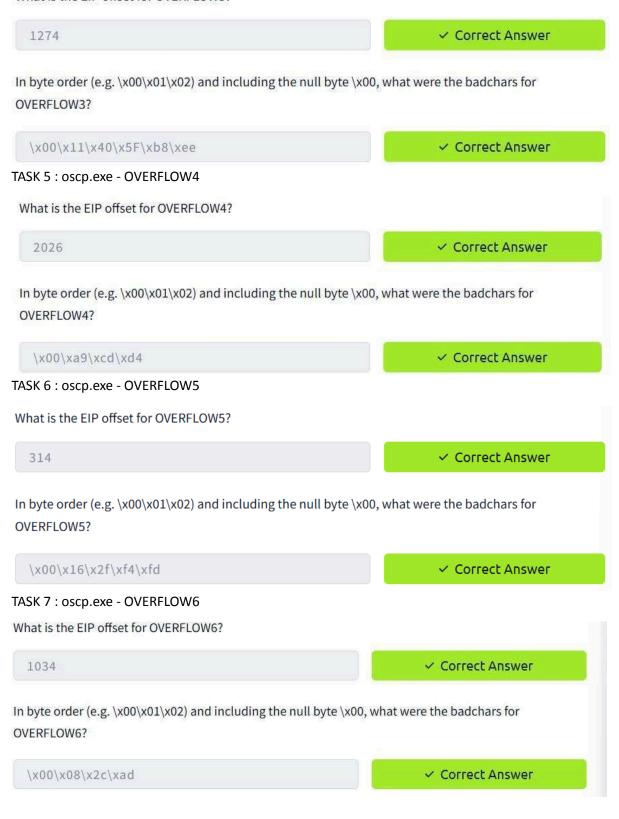
 $\x00\x23\x3c\x83\xba$



✓ Correct Answer

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? $x00\\x8c\\xae\\xbe\\xfb$ ✓ Correct Answer 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?** ✓ Correct Answer $x00\x1d\x2e\xc7\xee$ 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?** $x00\x04\x3e\x3f\xe1$ ✓ Correct Answer TASK 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:

Tryhackme platform Stack based buffer overflow attacks task is successfully completed.