Stack based buffer overflow attacks

DATE: 27.03.2025 NAME: SIVARANGINI Y

ROLL NO: 231901051

AIM:

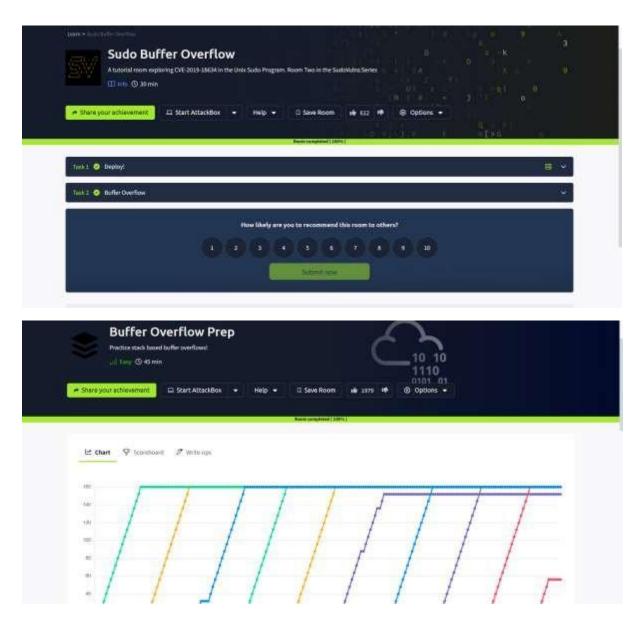
EX.NO: 5

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

What's the flag in /root/root.txt?

THM{buff3r\_0v3rfl0w\_rul3s}

Correct Answer

What's Correct Answer

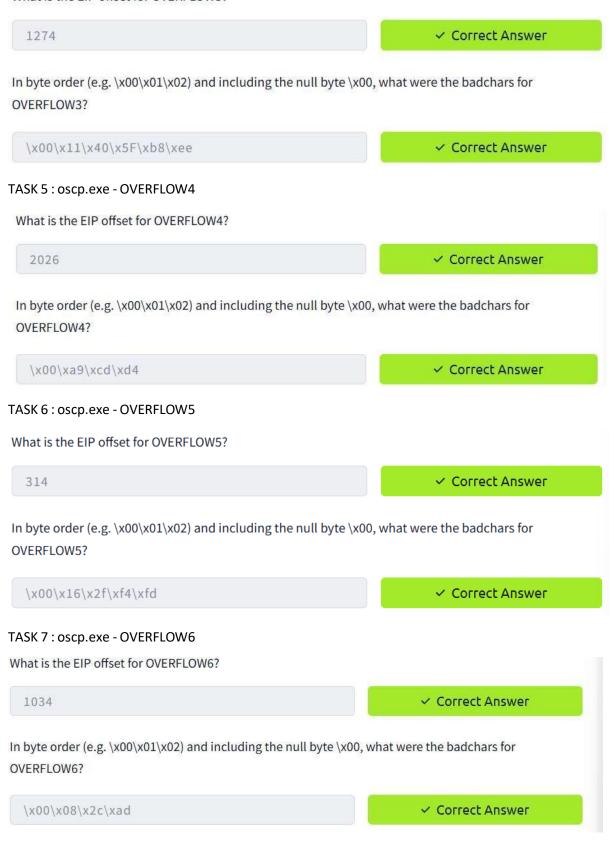


## What is the EIP offset for OVERFLOW2? 634 Correct Answer In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW2? \x00\x23\x3c\x83\xba

TASK 3: oscp.exe - OVERFLOW2

## 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.  $\times 00 \times 01 \times 02$ ) and including the null byte  $\times 00$ , what were the badchars for OVERFLOW7? ✓ Correct Answer  $x00\\x8c\\xae\\xbe\\xfb$ 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?** ✓ Correct Answer  $\x00\x1d\x2e\xc7\xee$ TASK 10: oscp.exe - OVERFLOW9 What is the EIP offset for OVERFLOW9? 1514 ✓ Correct Answer 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:

 $Try hackme\ platform\ Stack\ based\ buffer\ overflow\ attacks\ task\ is\ successfully\ completed.$