

231901033 DATE : 19.03.2025

NAME: NAVEEN C H

**Aim:**

To practice stack-based buffer overflows.

**Procedure:**

- Deploy the virtual machine.
- Open the **oscp.exe** file for each overflow challenge.
- Complete the following tasks one by one:
  - **Task 2: OVERFLOW1**
  - **Task 3: OVERFLOW2**
  - **Task 4: OVERFLOW3**
  - **Task 5: OVERFLOW4**
  - **Task 6: OVERFLOW5**
  - **Task 7: OVERFLOW6**
  - **Task 8: OVERFLOW7**
  - **Task 9: OVERFLOW8**
  - **Task 10: OVERFLOW9**
  - **Task 11: OVERFLOW10**
- For each task, find the buffer size, control EIP, and run the exploit.



## Buffer Overflow Prep

Practice stack based buffer overflow.

100% 100% 45 min



10 10  
1110  
0101 01

Share your achievement

Start AttackBox

Help

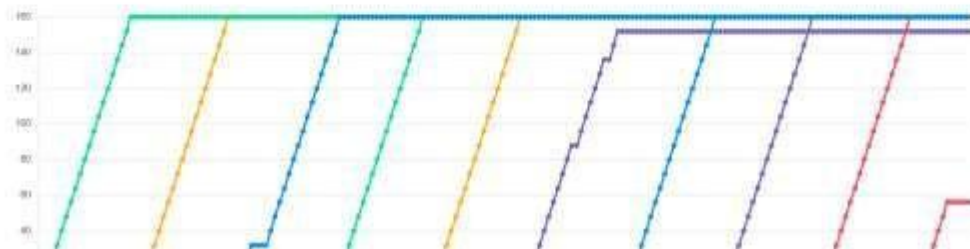
Save Room

1379

Options

Room completed (2019)

chart Scoreboard Write-ups



## TASK 2 oscp.exe - OVERFLOW1

What is the EIP offset for OVERFLOW1?

✓ Correct Answer

In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW1?

✓ Correct Answer

💡 Hint

## TASK 3 : oscp.exe - OVERFLOW2

What is the EIP offset for OVERFLOW2?

✓ Correct Answer

In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW2?

✓ Correct Answer

#### TASK 4 oscp.exe – OVERFLOW3

What is the EIP offset for OVERFLOW3?

✓ Correct Answer

In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW3?

✓ Correct Answer

#### TASK 5 : oscp.exe - OVERFLOW4

What is the EIP offset for OVERFLOW4?

✓ Correct Answer

In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW4?

✓ Correct Answer

#### TASK 6 : oscp.exe - OVERFLOW5

What is the EIP offset for OVERFLOW5?

✓ Correct Answer

In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW5?

✓ Correct Answer

#### TASK 7 : oscp.exe - OVERFLOW6

What is the EIP offset for OVERFLOW6?

✓ Correct Answer

In byte order (e.g. \x00\x01\x02) and including the null byte \x00, what were the badchars for OVERFLOW6?

✓ Correct Answer

#### 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?

\x00\x1d\x2e\xc7\xee

✓ Correct Answer

#### 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?

\x00\x04\x3e\x3f\xe1

✓ Correct Answer

#### TASK 11 : oscp.exe - OVERFLOW10

What is the EIP offset for OVERFLOW10?

537

✓ Correct Answer

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

**Result:**

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