RITHIKA BASKAR 231901042

EXP NO: 5B **BUFFER OVERFLOW PREP**

DATE: 19/3/25

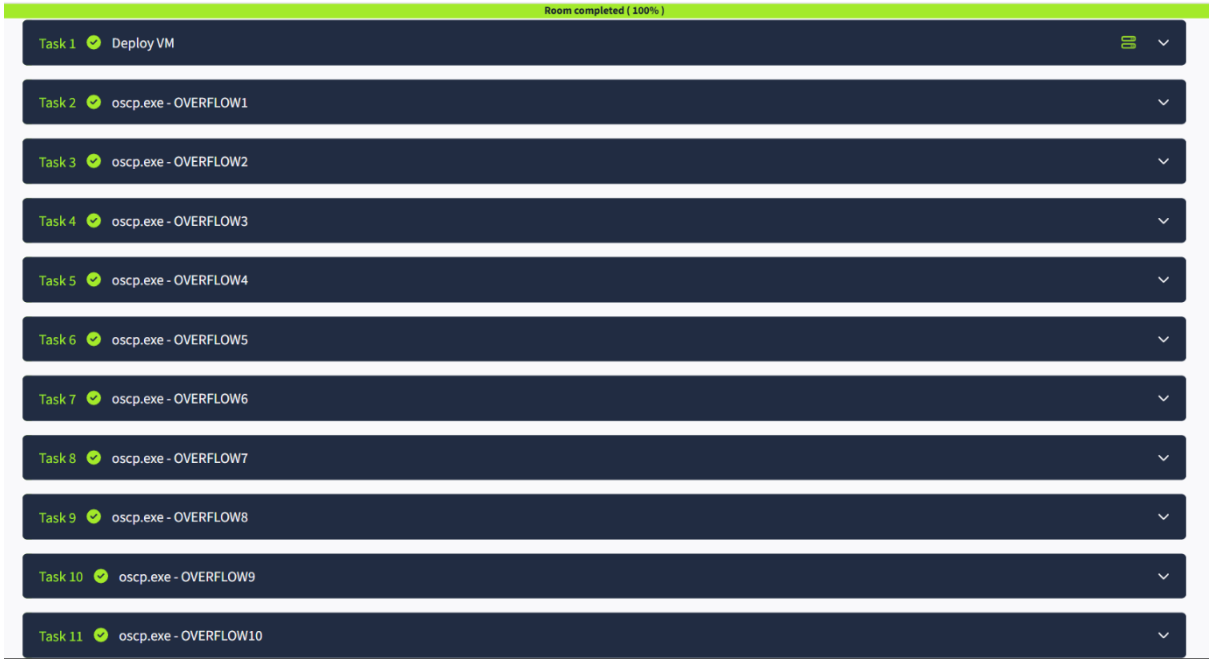
AIM:

To practice stack based buffer overflows.

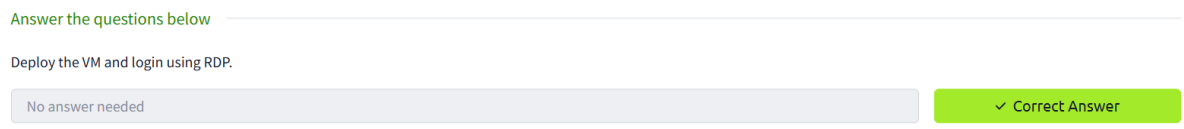
PROCEDURE:

Complete the given task as per the instructions.

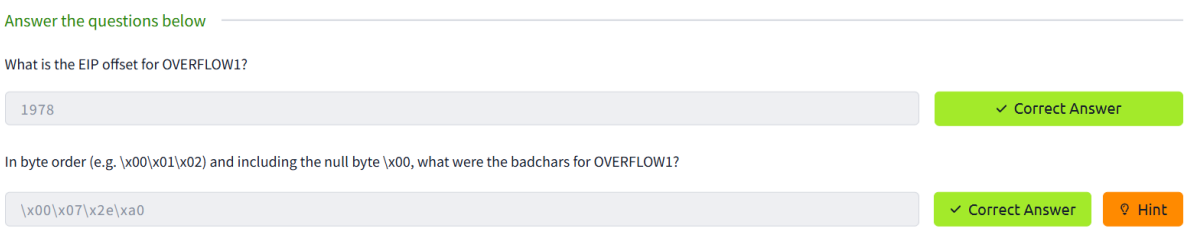
TASKS:



Task 1.



Task 2.



Task 3.

Answer the questions below

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 ✓ Correct Answer

Task 4.

Answer the questions below

What is the EIP offset for OVERFLOW3?

1274 ✓ Correct Answer

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

\x00\x11\x40\x5F\xb8\xee ✓ Correct Answer

Task 5.

Answer the questions below

What is the EIP offset for OVERFLOW4?

2026 ✓ Correct Answer

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

\x00\xa9\xcd\xd4 ✓ Correct Answer

Task 6.

Answer the questions below

What is the EIP offset for OVERFLOW5?

314 ✓ Correct Answer

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

\x00\x16\x2f\xf4\xfd ✓ Correct Answer

Task 7.

Answer the questions below

What is the EIP offset for OVERFLOW6?

1034 ✓ Correct Answer

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

\x00\x08\x2c\xad ✓ Correct Answer

Task 8.

Answer the questions below

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.

Answer the questions below

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.

Answer the questions below

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.

Answer the questions below

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:

Thus , stack based buffer overflows were practised.