NAME: HARINI.D.S   **ROLL NO: 231901009**

Buffer Overflow Prep

EX.NO:05

DATE: 19-03-2025

AIM:

Practice stack based buffer overflows!

PROCEDURE:
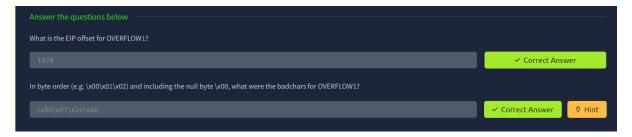
- Task 1 Deploy VM
- Task 2 oscp.exe - OVERFLOW1
- Task 3 oscp.exe - OVERFLOW2
- Task 4 oscp.exe - OVERFLOW3
- Task 5 oscp.exe - OVERFLOW4
- Task 6 oscp.exe - OVERFLOW5
- Task 7 oscp.exe - OVERFLOW6
- Task 8 oscp.exe - OVERFLOW7
- Task 9 oscp.exe - OVERFLOW8
- Task 10 oscp.exe - OVERFLOW9
- Task 11 oscp.exe - OVERFLOW10

Task 1 Deploy VM :

Answer the questions below

Deploy the VM and login using RDP.

No answer needed   ✓ Correct Answer

Task 2 oscp.exe - OVERFLOW1:

Answer the questions below

What is the EIP offset for OVERFLOW1?

1978   ✓ Correct Answer

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 :

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 oscp.exe - OVERFLOW3:

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 oscp.exe - OVERFLOW4 :

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 oscp.exe - OVERFLOW5 :

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 oscp.exe - OVERFLOW6 :

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 oscp.exe - OVERFLOW7 :

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 oscp.exe - OVERFLOW8 :

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 oscp.exe - OVERFLOW9 :

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 oscp.exe - OVERFLOW10 :

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 the Buffer Overflow Prep is completed using tryhackme platform.