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

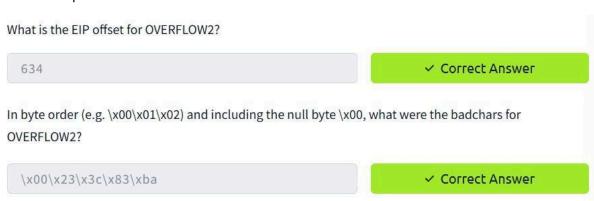- For each task, find the buffer size, control EIP, and run the exploit.

TASK 2 oscp.exe - OVERFLOW1

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

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

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

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

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

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

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.