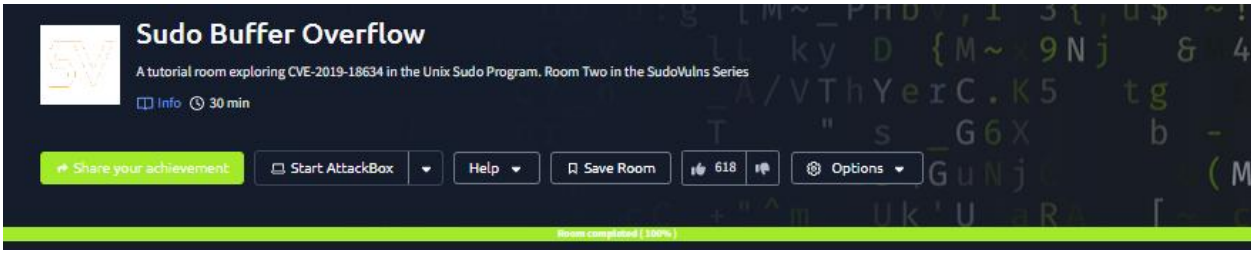
EXERCISE 5A
Stack based buffer overflow attacks

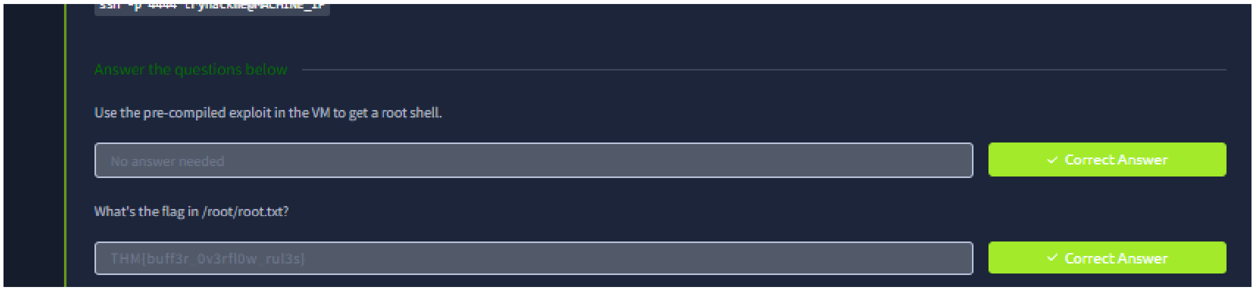
AIM:

To explore and analyze CVE-2019-18634, a buffer overflow vulnerability in the Unix Sudo program, and understand its exploitation and mitigation.



Sudo Buffer Overflow

A tutorial room exploring CVE-2019-18634 in the Unix Sudo Program. Room Two in the SudoVulns Series



```
ssh -p 4444 tryhackme@MACHINE_IP
```

Answer the questions below

Use the pre-compiled exploit in the VM to get a root shell.

No answer needed

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

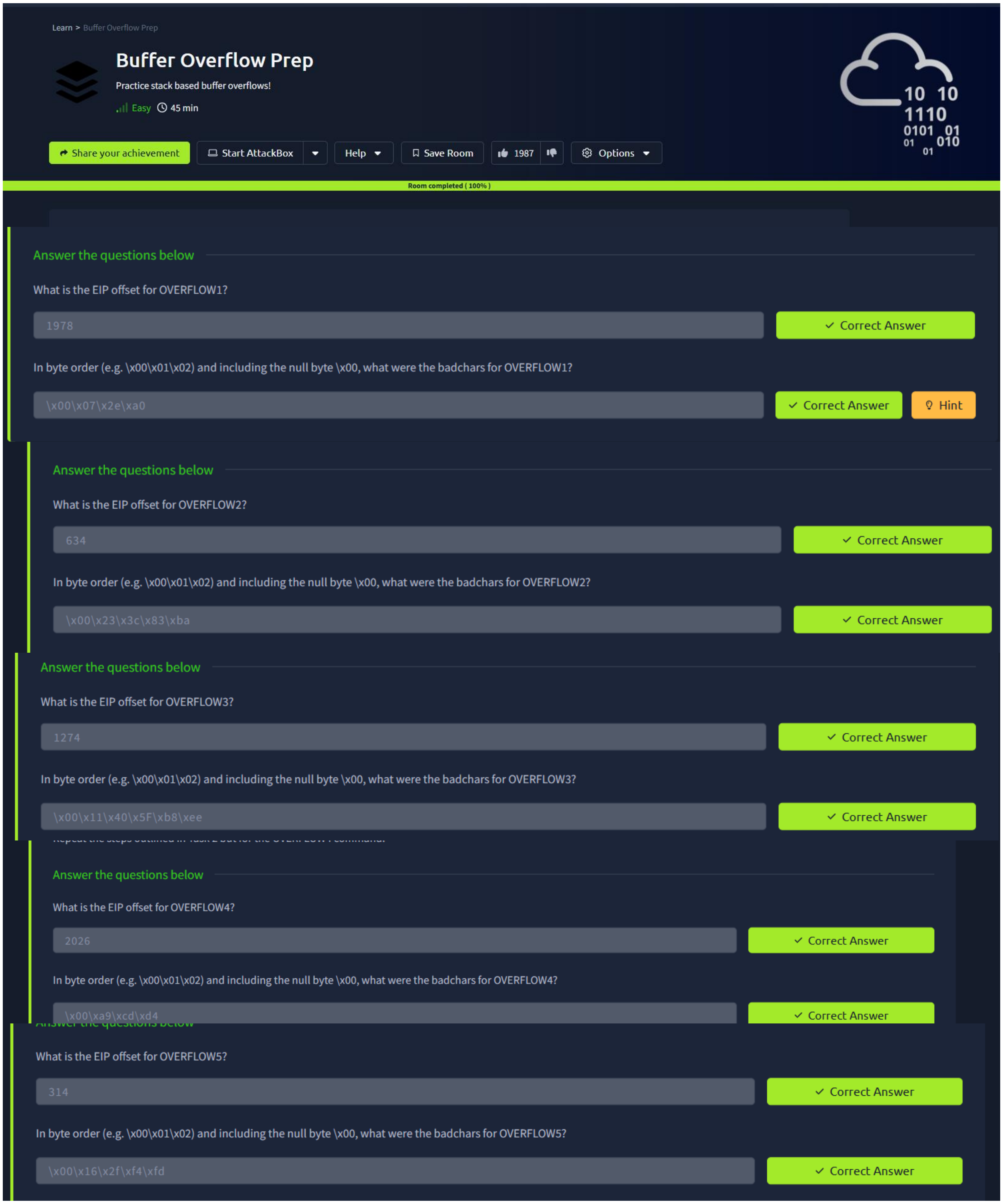
THM{buff3r_0v3rfl0w_rul3s}

RESULT:

The vulnerability was successfully analyzed, demonstrating potential privilege escalation. Mitigation measures, including updating Sudo to version 1.8.31 or later, were recommended to prevent exploitation.

EXERCISE 5B
Stack based buffer overflow attacks

Aim: To understand and exploit stack-based buffer overflows by overwriting memory beyond a buffer’s limit.



Buffer Overflow Prep

Practice stack based buffer overflows!

Easy 45 min

Room completed (100%)

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

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

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

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

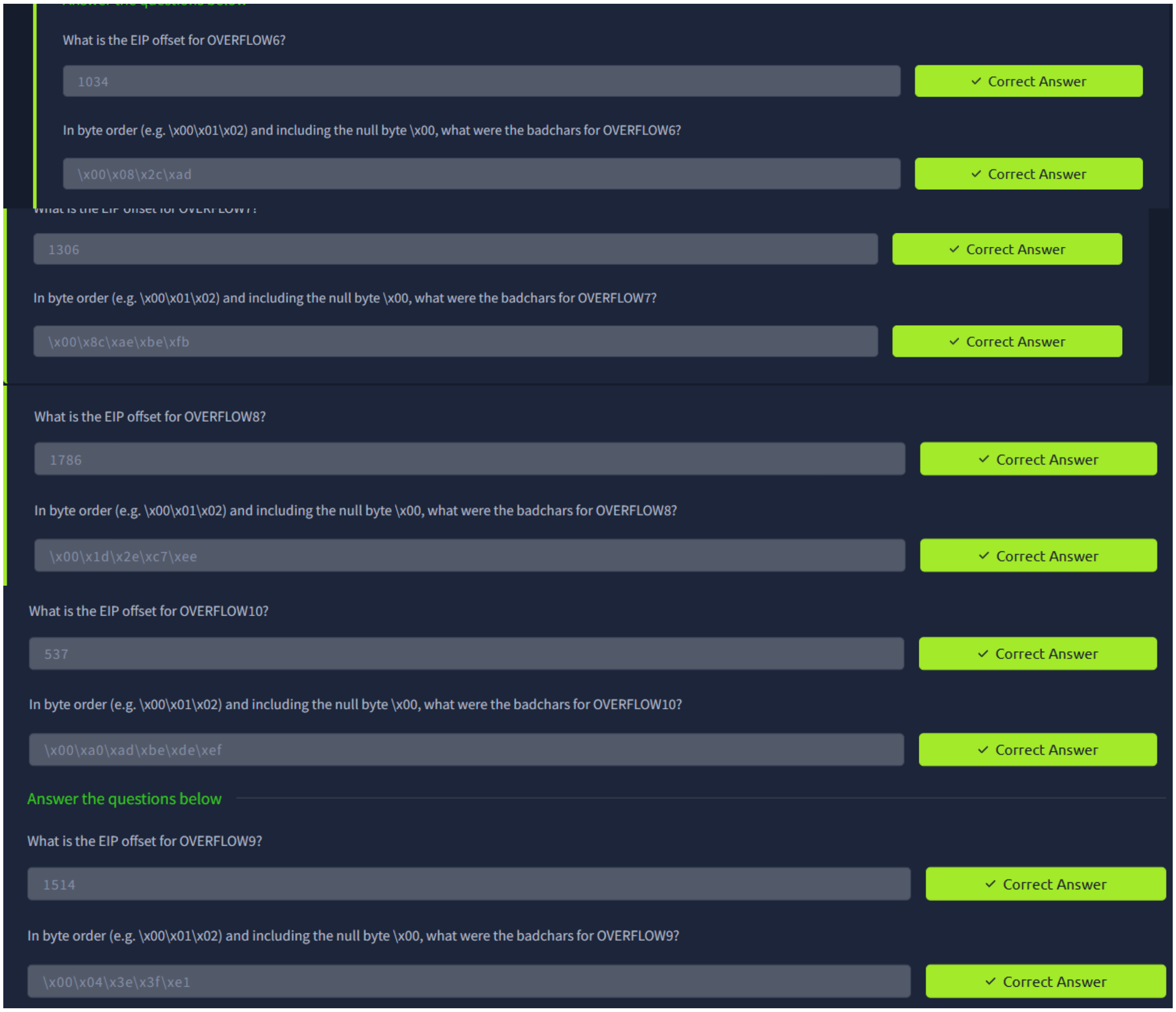
Answer the questions below

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



Answer the questions below

What is the EIP offset for OVERFLOW6?

1034

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

\x00\x08\x2c\xad

What is the EIP offset for OVERFLOW7?

1306

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

What is the EIP offset for OVERFLOW8?

1786

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

What is the EIP offset for OVERFLOW10?

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

Answer the questions below

What is the EIP offset for OVERFLOW9?

1514

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

Result: Successfully exploited the buffer overflow to overwrite the return address and redirect program execution.