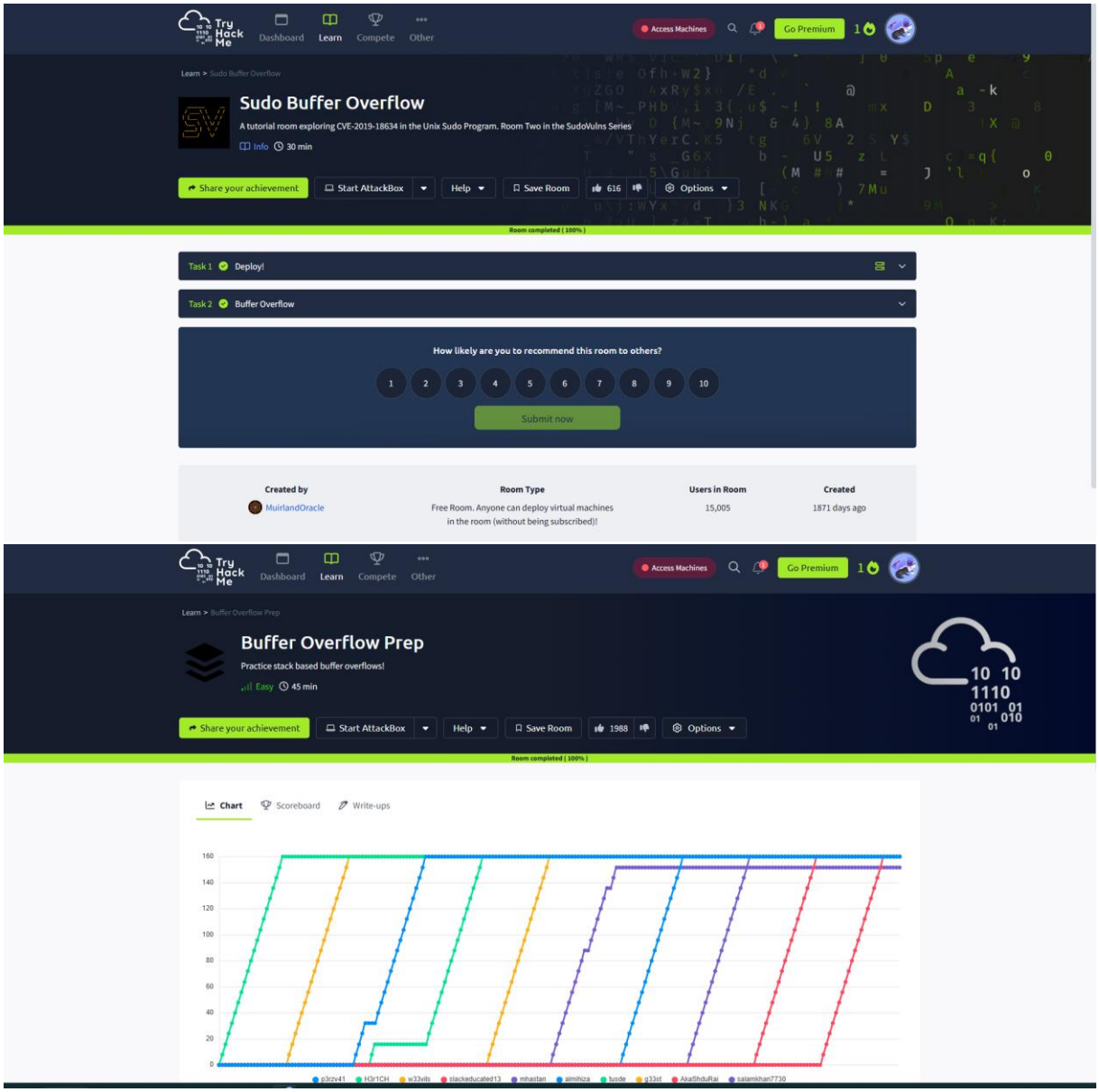
Ex.no: 5 Roll no:231901004

DATE: 02.04.2025

Stack based buffer overflow attacks

AIM:

Sudo Buffer Overflow



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

No answer needed ✓ Correct Answer

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

THM{buff3r_0v3rfl0w_rul3s} ✓ Correct Answer

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

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

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

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

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

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

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

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

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

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