Assignment 1

Problem 1

Reverse engineer the code given in the attached pdf files and prepare a detailed writeup. Clearly describe the following.

1. steps followed by the malware. Trace the exact sequence of instructions in the sapphire exploit, starting from the execution of the return inst.
2. Especially, answer what happens from jmp %esp.

0.1 Notes

- Since this is a network packet you wont be able to load it in IDA. But it is a small code, drawing a control flow graph will be helpful and efficient.
- Since this is reverse engineering do understand the whole binary in parts.
- You can use Internet to know about various systems calls made in the binary but citations are necessary.

Problem 2

Write a triton program to count the number of control transfer instructions. You have complete the emulate function in the given boilerplate code. The emulate function takes as input the 'pc' of a instruction and outputs an integer. Your function should return the number of Instructions.

0.2 Notes

- Installation Instructions for triton : `"https://triton.quarkslab.com/documentation/doxygen/#install_sec"`
- Documentation of triton: `https://triton.quarkslab.com/documentation/doxygen/py_triton_page.html`
- The code will be run against testcases which will be uploaded shortly.