Research Report

Where I’ve started and where I’ve come…

* Project euler
  + Reviewing c programming techniques
  + Review of math and critical thinking
* Linux
  + Learning the command line
* Hacking: the art of exploration
* Microcorruption
* Exploit-exercises: protostar
  + Stack attack!
* Reverse-engineering
  + Ida pro
  + Hacking solitaire
  + Patching code and hands on exploitation
* Frostbite
  + Using QEMU/KVM
  + Coding a qemu command
    - Hello world
  + Coding a more practical command
    - Looking at ip network connection and flagging for information from “the bad guys”
  + Using QMP
  + Very simple network communication/interception demonstration
    - Good guy and bad guy (filter-work for more efficient data processing)
      * Check for the source and destination addresses and distinguish between the bad guy and the good guy…success!

Introduction

- learning x86 architectural details

* intro to exploitation
* getting familiar with QEMU/KVM architecture
* write a plugin to QEMU (custom QMP) for use on frostbite
* analyze malware without letting it know you’re analyzing it
  + accomplish this via virtual machines
* relation of exploitation with planes (manned and unmanned)
  + technological shift towards automation

Background

Methodology

Results

Conclusion