Anonymous

EDUCATION

Purdue University
College of Science
BS in Computer Science
Expected Grad. Summer 2019
CS GPA:3.4

COURSEWORK

Modern Binary Exploitation(RPI-SEC)
Forensics of Malware(Graduate)
Operating Systems
Cryptography
Embedded Systems
Systems Programming
Computer Architecture
Computer Security

INTERESTS

Linux Kernel Programming
Linux Implant Development
Hypervisor Development
Hypervisor Exploitation
Embedded System Exploitation
Reverse Engineering

LANGUAGES

C, C++, Python, x86/ARM Assembly

ORGANIZATIONS

CERIAS Research Group
ACM Security Club

10.20.2018

EXPERIENCE

Trail of Bits December 2018 - January 2019
Security Research Intern Remote

- In the winter I will work on extending the Manticore symbolic execution engine to the Ethereum virtual machine.

MIT Draper Laboratory January 2018 – Current
Engineering Co-Op/(Part time remote) Cambridge, MA

- Developed automated vulnerability detection tools utilizing program analysis techniques like taint analysis.

Federal Reserve Bank of Chicago June 2017 – August 2017
Security Engineering Intern Chicago, IL

- Architected and developed real time threat intelligence software
- Deployed and developed specific extensions to Google Rapid Response
- Analyzed the behavior of several different malware samples to test the effectiveness of different tools

Purdue University Aug 2016 – Jan 2018
Security Researcher – Jan 2017 – Jan 2018 West Lafayette, IN

- Researched and analyzed the signatures of Windows kernel-mode and user-mode rootkits in memory.

Teaching Assistant (Python) – Aug 2016 – May 2017 West Lafayette, IN

- Taught over 130 students entry level programming concepts like object orientated design and GUI programming.

Sandia National Laboratories Jun 2015 – Aug 2015
Enterprise CyberSecurity Intern Livermore, CA

- Worked on building back-end solutions to our in-house virtualization software, Minimega, which allowed us to model and perform tests on enterprise networks.
- Created user configuration options for Minimega by using Python.

CURRENT PROJECT(S)

SVC3 IP Camera – (Reverse Engineering/Exploitation Proj.)
I purchased an IP Camera on Amazon and am currently reverse engineering the firmware with the goal of finding new vulnerabilities.

Hypervisor Rootkit – (Dev. Project)
While reading about hypervisor based rootkits like Bluepill and Subvirt, I noticed that none were open source. I am going to make a very simple POC hypervisor based rootkit to open source it.