Name: Rushabh Vyas

Major: CIT – Information Security

Course: TECH 30010

Class: 7039

Company: Sandia National Laboratories –

7011 East Avenue

Livermore, CA 94550

Work dates: May 19, 2014 – July 31, 2014

Submission date: August 1, 2014

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Introduction:

I interned at Sandia National Laboratories in Livermore, California this summer. I worked under Information Assurance department. IA department has Center for Cyber Defenders program, which employs interns to work on information security/information assurance related projects. CCD program allows interns to work on real projects that are used by Sandia. The CCD program focuses on research in both defensive and offensive areas of information security such as intrusion detection and vulnerability analysis. [1] Jeremy Erickson runs the CCD program in California. Jeremy also runs Cyber Technologies Academy, which is program that teaches computer and computer security to high school students. [2]

Few days after I got accepted for the internship I got an email about the projects CCD was working on. There were more than 10 projects and interns got to select top five projects they preferred. We were to work on two projects for this summer. The projects I worked on were MegaReap, and Network Traffic Profiler. Each project typically had three or more interns working on it.

Network Traffic Profiler was a project about log analysis, network analysis, and anomaly detection. Goal of the project was to find "noisy" connections or connectors, detect DDoS, and detect port scans. We had to write tools that do analysis on logs, packet captures, and live network. This project was my fourth preference. I didn't think it would be too difficult or

---

[1] http://www.sandia.gov/careers/students_postdocs/internships/institutes/cyber_defenders.html

[2] https://share.sandia.gov/cta/

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

interesting, but I was wrong. Data analysis is very powerful, and can give you a lot of information about networks.

MegaReap project was my second preference. MegaReap project was about doing large scale malware analysis. We were using an open source tool called minimega, which was developed at Sandia.[3] Minimega was used for simulating android phones and doing mobile malware analysis.[4] Minimega is a tool that allowed us to create and control a large scale virtualized environment. Virtualization allows us to have one or more simulated computers on one physical computer. Our goal with this project was to develop a framework to dynamically analyze thousands of windows binaries (.exe files) to see how they behave.

Discussion:

Sandia describes itself as a national security laboratory.[5] Sandia National Labs is owned by Lockheed Martin, but works under Department of Energy. SNL does research and development in many areas, including nuclear weapons, energy, engineering, cybersecurity, bioscience, and simulation and modeling. Sandia National Labs has many different locations, but two main sites are in Albuquerque, New Mexico, and Livermore, California. [6] I worked at the Livermore, CA

[3] https://code.google.com/p/minimega/

[4] http://arstechnica.com/information-technology/2012/10/megadroid-300000-androids-clustered-together-to-study-network-havoc/

[5] http://www.sandia.gov/about/index.html

[6] http://www.sandia.gov/locations/index.html

site, and it has around 900 employees. [7] CA site had about CCD 15 interns. We had high school interns to interns who were working on their Masters and Doctorates.

Like any lab, SNL has a lab president and a lab director. Lab director for SNL is Paul Hommert. [8] We had organizations and sub-organizations. For example, I was under Computer Science and Information Systems organization. CS/IS had InfoSec organization. The InfoSec organization had Information Assurance organization. I was an intern under IA. Each organization has a manager, and secretary. Interns interacted with mentors and supervisor most of the time. Mentors directed the projects we were working on, and supervisor provided the support.

As I mentioned before, the projects I worked on were Network Traffic Profiler and MegaReap. Interns got to choose the week that start on. Another intern who started on the same day as I did was on the NTP project. We started working on the project on the first week. The mentor gave us freedom to write our code in any language that we wanted to. We started using Python because it was simple, and it got the work done. First part of our project was to parse the logs, and see what we can do with the data. Our goal was to come up with ways to find anomalies in the data and apply what we came up with. You can always look for attacks that you already know about or have signature for, but having an anomaly based system can help you find unknown attacks or signs of compromise. We had to determine what's normal before finding anomalies. We can't just look at the data we got and write signature based on it. Something that seems normal for large network may not be normal for small networks. Second big part of the project was to apply

---

[7] http://www.sandia.gov/locations/livermore_california.html

[8] http://www.sandia.gov/about/leadership/index.html

what we did to the logs to a live network. This project required me to know network communications, data analysis, statistics, and basic programming.

MegaReap project was about doing large-scale dynamic windows malware analysis. SNL did similar project called Andlantis, which was about large-scale dynamic analysis for Android applications. [9] I was the only intern working on this project for the first week; however, I did have help from the people who worked on Andlantis and my mentor so I could get everything up and running. I started by learning about the tool we were going to use, which was minimega. Minimega is a tool that allowed us to create virtual machines inside of a machine.[10] There are many applications that allow you to create virtual machines, but minimega allowed us to do this on a large-scale. It also allowed us to create virtual networks for the virtual machines. I had worked with virtual machine applications before, but this was hard to get used to at first. I did learn to use minimega and all its features. I documented the requirements to get minimega working so other interns on my project could use it. I also worked on collection and analysis part of this project. After you do get virtual machines going, you need to collect data and do analysis on it for it to be useful. I had done some computer forensics before but it had nothing to do with malware. I was new to malware analysis. I learned how to use qemu, Volatility/forensics, and image creation while doing this project.

Documentation:

Here are the project descriptions I got in the email.

---

[9] http://mostconf.org/2014/papers/s3p2.pdf

[10] https://code.google.com/p/minimega/

MegaReap

Design and implement a state-of-the-art content detonation and dynamic analysis platform for windows binary executables using large-scale virtualization technology. The purpose of this project is to create a highly scalable platform that takes malware from the Forensic Analysis Repository for Malware (FARM) and runs it in an instrumented virtual machine. Students will leverage the minimega framework to provide the scalability and will create a custom analysis framework using volatility.

Relevant Technologies:

* Python

* Go

* KVM virtualization

* OpenVSwitch Networking

* Volatility

Network Traffic Profiler

The network traffic profiler is a tool Sandia could use for cyber operations.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

At the very basic level, the profiler should be a program or script which can report which IP/port pairs and tuples are currently the most noisy on our network. "Noisy" might mean volume or it might mean number of connections. Other definitions of “noisy” are possible, and the intern is encouraged to think outside the box. In Phase 1 the program should do some statistics on the flow log files that we generate, which includes the IPs, the ports , connection durations, and number of bytes transferred. In addition to a "big talkers" output, the program should be able to report good PCAP/BPF filters that can be applied to IDS sensors in the case of unusually high volume but ultimately not all that important network traffic. For phase 2, the deliverable is a capability to monitor the network log data continuously, and alert when significant changes to the network profile is observed (e.g. n ew "big talkers", DDOS detection, internal scanners, etc.). Phase 3 is to create a sniffer/PCAP-based capability that performs the analyses from phase 1 and 2 in real time against live network traffic.

Anonymized network flow logs are currently available on the server, and additional

logs may be generated if needed. Full PCAP will need to be either generated to replayed from publicly available packet captures. Programs or scripts should be able to be run on commonly configured FreeBSD and Linux operating systems. Interns should have some basic knowledge of networking, statistics, and should have some prior programming or scripting skills. Optionally, interns with more advanced analytical knowledge such as machine learning and behavioral anomaly detection could offer more to the analytical portions of this project. Interns are encouraged to think outside the box with regard to the different analytical methods applied to the data.

Evaluation:

I learned to apply the things that I thought I would not use. I was taking Unix Programming this summer, and I learned to write bash scripts and use Linux commands. This course was really helpful with MegaReap project. I had to write a lot of bash scripts to automate processes. I was learning in the class, and doing the homework. I didn't care much about the homework. I was doing it just to complete it and most other students can do that as well. Applying what I learned in the class at work is what made this class helpful. I also took Quantitative Analysis courses (CIT 12000, 22000, 320000) which were also helpful. I never thought I would use statistics again, but I had to apply what I learned to Network Traffic Profiler project. NTP required us to

come up with ways to find abnormalities and that can't be done without doing statistics on the data you already have. NTP also required us to know networking and how network attacks work.

I would say that the internship work was challenging. I had to think outside of information security. The project did relate to InfoSec, but things that I did to make the projects work required more than just knowledge of InfoSec. I had to work with new applications, and new concepts. As I mentioned before, I had to learn how to use qemu, minimega, and Volatility amongst other tools. I learned about applied statistics, and data analysis for security purposes. Data analysis can be applied to many areas, and can give you a lot of information.

My education prepared me well, however it can always be improved. I am currently taking C/C++/Java classes from CS department, and I wish CIT had those classes. If you're going into information security, you'll need to have C/C++ knowledge, unless you're dealing with policies. It would also be great if we had class that just focused on bad security practices and identifying bad security practices in order to fix them. We do have Risk Assessment (CIT 45100) which is great; however it's not really technical, it covers policy related things. We also don't have many offensive security courses. CIT 40600 was the only class that had assignments that covered penetration testing/hacking, but it wasn't too difficult. We don't have malware analysis/reverse engineering focused class. 40600 had one assignment that covered malware analysis, but that isn't enough. Digital forensics class didn't cover malware analysis at all; it focused more on forensics that relates to law. Class that covered basic reverse engineering and binary file analysis would also be helpful. These things can be learned outside of class as well, but having an instructor who can guide you and give you feedback is really better.

I had a supervisor and mentors. Mentors typically come and talk to you two or three times a week about how your project is going, and guide you. We also had group meetings about projects every few weeks with the mentors. Supervisor also had meetings with us individually every few weeks to see how our projects were going. We also had a chat server setup where all the mentors and supervisors hung out. It was very helpful because we were able to ask questions if we had problems, and people who weren't on the project, but knew the answer would help.

My favorite part about the internship was working on the projects. I liked research and development environment. You don't always know the answer, but you research, and try things out. While in the process of researching and developing, you end up learning a lot of things that you can apply to other places. I also enjoyed working with other interns. We had a small group of interns, and we had lot interaction with each other. We were learning from each other. There were times when one intern was explaining a concept to another intern and everyone joined in to listen.

I can't think of anything too important they can improve. It would've been great if some mentors had taught us about the subjects they specialize in. Many of the mentors were working in areas that were interesting to me and other interns.

This work experienced has helped me expand my horizon. I picked up more skills and knowledge than I had before. I can apply these skills outside of information security field.

About Career Services:

I have gotten help with resume writing from career services, which was helpful. I also use ET Careers job search website, but I didn't find too many InfoSec related jobs. I mostly came across IT jobs, and I wasn't interested in them.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.