|  |
| --- |
|  |
| Capstone Experience  IST 894 |
| Semester Overview and Reflection  Scott Finlon |

Table of Contents

[1. Semester Overview 3](#_Toc89898845)

[2. Reflection 5](#_Toc89898846)

# Semester Overview

The overall goal of this capstone class is to provide a hands-on experience that sums up various technologies, techniques, skills, and thought processes that we’ve encountered in this curriculum. While the primary focus changed week to week, there were several larger points that could be categorized as primary skills to have as a security professional. Some of these skills that were needed and displayed were research, versatility, thinking on your feet, programming, cryptography, multiple operating systems, and forensics.

Most of the class took place in the US Cyber Range, and it’s safe to assume that most students haven’t had experience in what a cyber range can and can’t offer or do, so a logical first step was to research various cyber ranges and identify a way to score and compare them to see what ones were best based on features and price. Next, we look a more extensive look at the Linux/Unix/Unix-like (\*nix) operating systems. In the professional world, many security tools run exclusively in \*nix because the control you have over the hardware because the operating system is open source and easily extendable. The next few labs stayed focused on the concept of \*nix based tools and command line applications. There was a lab on password cracking with John the Ripper, and then a good analysis of block cipher encryption methods and later in the course we also analyzed and compared a few symmetric and asymmetric encryption types like ccrypt and GPG. We were then able to demonstrate in what circumstance it was better to use one mode of operation or encryption type over another.

After that, we spent a couple of weeks on network security and tools, which I believe is the core functionality that most of information security revolves around. We took a very brief look at Snort, learned how rules are written and how to tune them, analyzed a packet capture, and then ingested the logs into a frontend for Snort to analyze. Then we configured a host-based firewall to restrict what traffic could ingress and egress the virtual machine. The next lab utilized Nmap to scan for open ports and services/applications that were listening and then to use Metasploit to exploit vulnerabilities that we identified via scanning to gain unauthorized access. We then took it a step further and used msfvenom to tailor our own Windows exploit. Later in the semester we looked at other network reconnaissance techniques by using whois, nslookup, and dig to find more information about various resources and endpoints on the internet.

The next few weeks focused on web application security, network forensics, and windows forensics. For the web application security, we used the Damn Vulnerable Web Application, which is a commonly used intentionally vulnerable web application used for training, to demonstrate and carry out various SQL injection attacks. We spent a week doing network forensics, analyzing a packet capture to identify and retrieve various data points that were obscured or deleted to identify the perpetrator. Finally, the last two weeks of labs were focused on Windows memory and registry forensics. We used RegRipper to analyze an extracted Windows Registry hive file, and then Volatility to analyze a Windows memory capture.

Several of the labs were intensive, and some of the labs were light on the work required. One of the hardest things each week was making sure that the lab report met the minimum requirements for screenshots and references. Many of these labs I could have done without referencing anything because of the work experience that I have, however while some of the labs did take much longer to complete than others there were no situations that were not fully resolved each and every week.

# Reflection

I feel that the overall experience of this course is on a good start. Whether you call it Information Security, Cyber Security, or just Security the amount of things that are your responsibility is huge. A security professional can, and probably should find a few specialized topics that they are interested in and focus on them in order to really be good at their job. That’s not to say that smaller companies don’t have a one employee security office where the individual is in charge of network security, application security, database security, vulnerability scanning, compliance, risk, policy and many other topics as well. This discrepancy between singularly focused individuals and umbrella security professionals can normally be attributed to the company they work for, and since many of the students taking this curriculum and this course aren’t employed yet nor do they know what specifically they want to do, it’s hard if not impossible to have one singular curriculum of labs for everyone.

I feel that the weight of expectations and effort for several labs were quite imbalanced. Some of the more basic Linux and network tool labs were quite short and didn’t go into many, if any, details about why certain applications/techniques were used, and then the Windows forensics labs were quite detailed and actually had some parts that weren’t just scripted for the students to do which actually forces you to think. A lot of the labs were entirely written out do step a, then b, then c now write a report on it, not enough gave building blocks about why things were being done which then required the students to put those new skills and thought processes to the test on their own. All in all, with the above difficulties in mind, I will reiterate that this course is off to a good start. If it was up to me, I would rework some of the labs to put in more open ended questions that forced individuals to think on their feet.

# Jobs Descriptions

|  |  |  |
| --- | --- | --- |
| Job Title | Description | Skills required |
| Penetration Tester | Performs various offensive attacks against their own companies resources to identify vulnerabilities before they can be exploited by an outside attacker. | * Understand Network protocols * Advanced knowledge of operation systems * Advanced programming knowledge * Knowledge of various exploits and vulnerabilities |
| Security Network Engineer | Install, manage, control network security appliances, ensure logs are collected and are being analyzed appropriately. Develop new tools for enhancing visibility in the network. | * Extensive knowledge of network protocols * Knowledge of programming * Extensive knowledge of routing protocols * Knowledge of various operating systems |
| Windows Security Engineer | In charge of maintaining Active Directory and patch management to ensure that all Windows machines are effectively managed and patched as fast as possible. | * Knowledge of PowerShell * Understanding of Active Directory * Extensive understanding of the Windows operating system * Quality assurance skills to test patches and ensure they are successful |
| Information Security Analyst | Monitor and analyze logs and data that is being collected to identify intrusions, weaknesses, and other incidents as fast as possible. | * Ability to work with programming scripts * Knowledge of various network protocols * Knowledge of organizational baselines * Ability to analyze logs to identify patterns that don’t match |