CPE 435 Portfolio

Kollin Labowski

CPE 435 – Computer Incident Response

West Virginia University

Table of Contents

Cover Letter…………………………………………………………………..……………3

Self-Evaluation……………………………………………………………………………4

Class Record………………………………………………………………………………5

Appendix……………………………………………………………………………………7

Incident Response Toolkit…………………………………………………………...7

Record of Best Work……………………………………………………………….....8

Kollin Labowski

kkl0009@mix.wvu.edu | (571) 287-1234 | 1014 Rawley Ave, Morgantown WV, 26505

To:

Roy Nutter

West Virginia University

LANE Department of Computer Science and Electrical Engineering

395 Evansdale Dr

Morgantown, WV 26506

My name is Kollin Labowski, and I am a member of the class of 2022 at the LANE Department of Computer Science and Electrical Engineering at West Virginia University. I am majoring in Computer Science with an area of emphasis in Cybersecurity and a minor in Mathematics. I have over 5 years of programming experience in Java, C, Python, PHP, and other languages. I have about a year of experience using various cybersecurity tools such as Kali Linux to enforce proper security practices and to perform penetration tests. I am also an intern at the Stephenson Stellar Corporation, where I perform security and validation tests and research on 5G-capable devices. Currently I am taking CPE 435 through the LANE Department, a class which focuses on Computer Incident Response.

In this class, I have learned all sorts of different techniques for conducting investigations on different computer systems. This class taught me about many of the different government policies and regulations regarding computer forensic investigations. This class also included a comprehensive overview of the Fourth Amendment to the Bill of Rights, which deals with searches and seizures. Additionally, this class helped me understand the process of completing an investigation, including writing a warrant and collecting information.

As this portfolio will demonstrate, CPE 435 also taught me about many different tools that could be used to recover data in a computer investigation. Some tools, such as Nmap, are useful for scanning ports on remote networks. Others, such as Dirbuster, are helpful for investigating web applications and locating hidden directories. Some tools, such as Wireshark, are used for tracking packets sent to and from a system. Many of these tools can be used on different types of operating systems, from Windows, to Linux, to Android, and more. Overall, this class was very informative, and provided me with a lot of experience in computer forensics that closely mimicked the real world.

Sincerely,

Kollin Labowski

Self-Evaluation

This class was very informative and introduced me to a lot of new tools that could be used in computer forensic investigations. I found the lectures to be interesting, and I learned something I did not already know every time, whether it was about forensic tools or government policies. My favorite part of the course was being able to participate in the National Cyber League (NCL) competition. This competition was very challenging, but I learned so much about many of the different tools, particularly those available on Kali Linux. By the end of the individual competition, I was very pleased with my placement in the 98th percentile of the country, and I was excited for the team game, which I also found to be very fun. I spent many hours learning about the different tools used in NCL and spent a long time trying different strategies to solve the difficult challenges in the competition. This is one of the main reasons I believe I deserve to receive an A in this course.

In addition to my hard work spent learning about the different tools for NCL, I have also attended every lecture, and was very interested in learning more about computer forensics. I now believe I have a very strong understanding of the process of forensic investigations, and the government rules and regulations regarding them, particularly the Fourth Amendment. Through NCL and various lectures throughout the semester, I now believe I have a thorough understanding of password cracking, network scanning, web application investigations, packet analysis, open-source intelligence gathering, and other topics relating to finding information in a computer forensics scenario. Overall, I believe I have put forth my best effort in every assignment and competition for this class, and as a result I believe I will be coming out of the class knowing much more about computer forensics than I did going in. For these reasons, I believe I deserve to earn an A in this course.

Class Record

The CPE 435 covered multiple key learning objectives. One of these core objectives was to cover the proper and legal procedures for performing investigations, and the legal basis thereof. About half of the class was spent on this topic, with a significant portion of it being dedicated specifically to the Fourth Amendment and its various applications. Several lectures were dedicated to this topic, and open discussion about whether certain scenarios were covered by the Fourth Amendment or not was encouraged. The first homework assignment in this class related directly to this learning objective. The assignment focused on a particular practice regularly used by law enforcement, geofencing. Geofencing is a way for law enforcement to collect data from the phones of individuals who were in a certain location at a time. The purpose of doing this is to attempt to find information about crimes that have taken place in certain locations, however some may argue that it violates the Fourth Amendment of the Constitution because it is a form of search and seizure. This assignment was a great way to introduce a real-life application of the Fourth Amendment where the solution is not particularly clear and is open for debate. If this situation is analyzed under a broader scope, it can be used to show that laws and government policies are not always all black and white, and there exist situations where the law is more of a gray area.

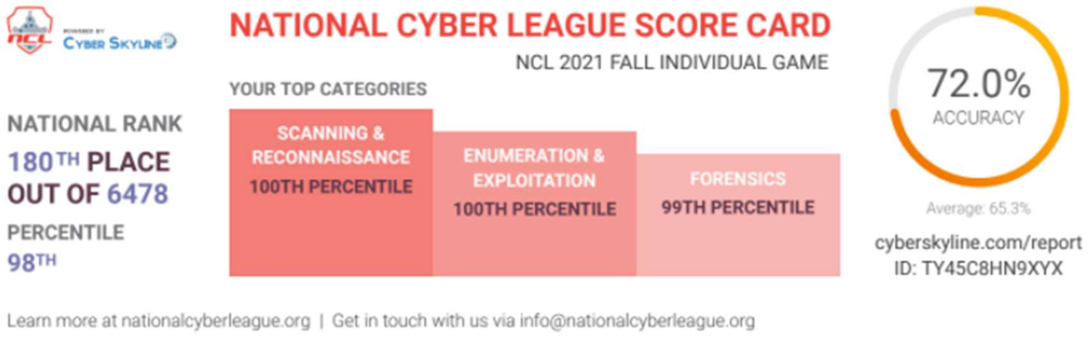
One of the other core objectives covered in CPE 435 was to provide a technical basis for Cyber Defense. While roughly the first half of the class focused on law and government policies, the second half of the class focused on many of the different tools and strategies to use in Cyber Defense. Some of the different aspects of cybersecurity discussed included password cracking, network analysis, log analysis, web application exploitation, cryptography, and a few others. For each of these different aspects of Cyber Defense, several specific tools were introduced to use. For password cracking, John the Ripper and Hashcat are two notable tools discussed in class. For network analysis, Nmap was one of the most important tools discussed, for its ability to scan ports on remote machines. For cybersecurity practices related to steganography, a field closely related to cryptography, tools such as Digital Invisible Ink were introduced. Discussing each of these different aspects of Cyber Defense and their respective tools led to participation in the National Cyber League cybersecurity competition. This difficult competition was an incredibly informative way to learn about these tools in a hands-on environment. It also acted to apply what was discussed in class to a collection of realistic scenarios. It was very satisfying to solve a tricky challenge by remembering something that was discussed in class and finding the hidden flags.

The final project for the class incorporated all the learning objectives into a single assignment. It was designed to mirror how a real computer forensic investigation would work. Like in a real investigation, the project required the receipt of a warrant before collecting specific information. It also involved the use of some cybersecurity tools discussed in class, such as Hiren's BootCD PE, a tool used to gain access to a password-protected disk drive, which was found on a website mentioned in class. The project also involved collecting information that was relevant to what was allowed in the warrant, and like in a real investigation, only evidence covered by the received warrant would be valid. As such, the project encouraged careful consideration of whether evidence was relevant to the case. Additionally, the project served as an introduction to writing full forensic reports and went over the various information which they should contain. Overall, the project was a great way to combine everything that was learned throughout the semester into one large project.

Incident Response Toolkit

Tool Name	Use of Tool	Link to Tool
John the Ripper	Cracking password hashes	https://www.openwall.com/john/
Hashcat	Cracking password hashes	https://hashcat.net/hashcat/
Wireshark	Network traffic analysis	https://www.wireshark.org/download.html
Nmap	Port scanning	https://nmap.org/download.html
Digital Invisible Ink Toolkit	Finding steganographic messages in images	http://diit.sourceforge.net/download.php
Dirbuster	Find hidden directories on a web application	https://www.kali.org/tools/dirbuster/
GDB	Debugging compiled programs	https://www.sourceware.org/gdb/
Ghidra	Reverse engineering compiled programs	https://ghidra-sre.org/
Jeffrey's Image Metadata Viewer	Viewing image metadata	http://exif.regex.info/exif.cgi
Python	Running and compiling Python programs	https://www.python.org/downloads/
Grep	Search for specific instances of text in files	http://gnuwin32.sourceforge.net/packages/grep.htm
Metasploit	Exploiting known service vulnerabilities	https://www.metasploit.com/download
Kali Linux	Linux environment with preinstalled penetration testing tools	https://www.kali.org/get-kali/
GCC	Compile C programs	https://gcc.gnu.org/install/download.html
Vim	Terminal text editor	https://www.vim.org/download.php
Dig	Find information about web servers	https://www.tecmint.com/install-dig-and-nslookup-in-linux/
Testdisk	Recover deleted files	https://www.cgsecurity.org/wiki/TestDisk
7zip	Zip and extract files	https://www.7-zip.org/
Hiren's BootCD PE	Gain access to a Windows 7 machine without a password	https://www.hirensbootcd.org/

Record of Best Work



POWERED BY CYBER SKYLINE

NATIONAL CYBER LEAGUE SCORE CARD

NCL 2021 FALL INDIVIDUAL GAME

YOUR TOP CATEGORIES

SCANNING & RECONNAISSANCE	ENUMERATION & EXPLOITATION	FORENSICS
100TH PERCENTILE	100TH PERCENTILE	99TH PERCENTILE

NATIONAL RANK
180TH PLACE
OUT OF 6478

PERCENTILE
98TH

72.0%
ACCURACY

Average: 65.3%

cyberskyline.com/report
ID: TY45C8HN9XYX

Learn more at nationalcyberleague.org | Get in touch with us via info@nationalcyberleague.org

Item Description: The scouting report for my NCL Individual Game results. My final ranking was 180 out of 6,478, which is in the 98th percentile.

Reflection:

This competition was where I was able to put everything I learned about Cyber Defense and Incident Response to the test in a hands-on environment. I spent the entire weekend working hard and putting in my best effort on every challenge. While I had heard about many of the tools in class, it was not until I had an opportunity to use them myself that I became confident in my ability to use them. Participating in this competition also got me really excited about cybersecurity, and I enjoyed the competition so much that I intend to compete in it again next semester.

In preparation for the next time I compete in NCL, I will continue to learn about the different cybersecurity tools, especially those included in Kali Linux. Having a solid background in the different tools we discussed in class was what allowed me to do so well this semester, but I know that with more practice and experience, I can do even better in the future. By improving my skills with these various cybersecurity tools, I will not only be more prepared for the next competition, but the skills will translate directly into any career I may find myself in which focuses on cybersecurity.