Senior Portfolio Reflection

IST/SRA 440W Portfolio

Jon Mahoney

IST/SRA 440W

# Foreword

Over the course of the 2021 Spring semester, I have completed weekly lab assignments in the InfoSec Institute Cyber Range and completed reports for each exercise as my senior project. In using this cyber range, I have displayed my skills and knowledge from all my previous IST and SRA courses. For the interest of brevity, the following lab information will be split into the categories of Operating Systems, Networking, and Development Languages as these are typical areas of interest to many employers.

# Operating Systems

The first exercise regarding operating systems acts as an introduction to Linux. It involves the basic commands of the Linux environment as well as the basics of the file system. When discussing the Linux file system, it is important to understand the Linux Kernel. The kernel can be described as the heart of the Linux operating system. It controls both hardware and software through a package of modules. With an understanding in Linux file systems, creating files in a text editor becomes a streamlined process. Text editors play a critical role in Linux because of the criticality of automating and standardizing tasks through scripting. The last and arguably most valuable OS related concept would be Red Hat Enterprise Linux. RHEL is a Linux distribution which is known for supporting containerization, Kubernetes, and cloud computing. It provides additional functionality for viewing login History and information on system users such as permissions, users, groups, as well as information on the operating system.

# Networking

The networking exercises in the cyber range focus on configuring Cisco devices with a variety of networking applications and Cisco OS commands. A specific networking configuration which is critical to network security is an access control list. ACLs are used to create rules which regulate communication between devices on a network. Access control lists are crucial in enhancing security, but a general theme explored in the exercises is how security impacts efficiency. For example, in the IP routing exercises, static and dynamic routing are examined. Both static and dynamic IP routing solutions can be viable depending on the scale and needs of an organization as they each have their own pros and cons. Static IP routing works best for small organizations and it provides enhanced security over dynamic routing. Dynamic routing is much more suitable for scaling operations in large organizations. Throughout the exercises, utilities such as VPCs, VLANs, and hypervisors were used to interact with the different Cisco networking devices. By making use of the Cisco OS, the user must resolve an issue where two devices cannot communicate with each other as they belong to different VLANs. This issue is circumvented through a process known as Inter-VLAN routing with a router on a stick. The network management lab makes use of a Cisco tool referred to as Simple Network Management Protocol (SNMP) to simulate the duties of a network administrator. SNMP is used to collect information on devices on a given network for the purpose of modifying the devices or logging their activity.

# Development Languages

Within Python, the Bandit static analysis tool can be used to check Python code for common issues and works by converting code into a tree of nodes to be tested based on user specifications. After Bandit testing, a report is generated and displayed. Bandit works particularly well at flagging the different vulnerabilities that are known in Extensible Markup Language. Some of these vulnerabilities are related to different utilities that cooperate with XML. These utilities are external entity expansion, XInclude, and XSL. When discussing these concepts, it is important to address Cross-Site Scripting as it is one of the most common Python exploits. The exploit relies on including malicious code in sections of webpages that support user input, such as comments or reviews. Similarly to Python, C++ also has many infamous vulnerabilities. One of which is referred to as Integer Overflow and Underflow. Integer overflow and underflow is one example of an error that can arise from casting variables to incorrect data types. When these errors occur, it is important they are correctly handled which is why a significant section of the C++ exercises involves the best practices of error handling. Some common mistakes in C++ programs include the use of NULL pointers, lack of error handling, and bad switch statements. As a general rule of thumb, developers should limit the amount of possible error cases and be prepared for all of them.

# Reflection

Looking back at the completed total of the InfoSec Institute assignments, I can conclusively say I am more skilled in the areas of IST and SRA than I was at the beginning of the semester. While many of the labs involved concepts that I have seen in lower-level courses, there is often a valuable nuance to the presentation of these concepts that provides a deeper understanding of the material. With that being said, there are a few things I would do differently if I were to repeat the projects of this course. For instance, one concept that is not presented in a cyber range lab or course is writing skills. There have been a few instances where the overall quality of a lab report was lessened because my writing detracted from the message. In other words, I have some work to do when it comes to professional writing. As for ways I could improve my performance in the labs, there is no significant room for improvement. The lab assignments are constructed in a way that generally involves following instructions to complete the exercises. Aside from reading everything and actively thinking about the process in the lab, there is not exactly a way to improve in completing them. That being said, there were instances where I have made mistakes and figured out a way to get back on track with the exercise instructions. In the instances where I became completely lost, I would restart the activity and read through the instructions a little more carefully. The cyber range platform introduced some minor technical issues. While it was a rare occurrence, the cyber range would sometimes incorrectly mark a step in an exercise complete as well as failing to detect completion of some steps. When this occurred, it was often easy to determine, and a simple workaround would be to reboot the lab exercise.