Portfolio Reflection

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

April 30th, 2025

Table of Contents

Semester Overview

Throughout the semester, I completed a various practical labs and video courses that collectively addressed a broad range of tools, technologies, and techniques common in the realm of cybersecurity.

Reconnaissance was one of the first topics I was introduced to, and one of the most frequently reoccurring ones throughout the lab. I learned how Nmap can help gather useful information about target machines, such as open ports and running services, and how the process of network scanning can be automated with scripting languages such as Bash and Python. I also practiced passive reconnaissance techniques, including conducting WHOIS and DNS lookups.

Web application security was another reoccurring subject. I both exploited and learned how to mitigate various common web app vulnerabilities, including insecure direct object references (IDOR), directory traversal, and cross-site scripting (XSS). Weak input validation was the primary vector through which most of these vulnerabilities are exploited.

I also explored security issues arising the use of outdated or obsolete network services. Specifically, I examined a critical vulnerability in shared by Telnet and FTP — credentials for both protocols are transmitted in plain text and can be seen by anyone monitoring network traffic. In modern times, Telnet has been supplanted by SSH and FTP by SFTP, so this

vulnerability is unlikely to have much real-world relevance, but it nonetheless demonstrated to me the importance of using secure software.

Another key area I studied was privilege escalation — specifically through lateral movement. I was guided through the process of using ProxyChains and SSH tunneling to pivot between hosts, seeing for myself how attackers can use illegitimate access to one machine to reach other machines deeper within the network. I also learned of various ways attackers might try to maintain their access even after system updates or reboots, such as by installing backdoors or meddling with antivirus programs.

Several labs had me respond to cyber incidents that had already occurred or were actively ongoing. In one instance, I used tcpdump and Wireshark to capture and analyze network traffic for signs of unauthorized activity; in another, I learned how to preserve the integrity of incident evidence using hashing algorithms; in another, I sought to identify and remove a malicious backdoor script and an associated cron job.

While most of the course content was technical in nature, I did spend some time learning about cybersecurity leadership. I explored the various responsibilities of the Chief Information Security Officer (CISO), and the strategic role they play in aligning security policies with business priorities. I learned of how the CISO acts as a bridge between technical teams and business executives and how they help build trust, stability, and resilience throughout an organization's cyber functions.

Reflection

I found that I was generally able to complete all of the lab assignments on time and without too much difficulty. Most of the difficulties I did encounter were related to the lab platform itself; the virtual machines were often slow and sluggish, which made it frustrating to carry out simple tasks. There were also difficulties introduced by InfoSec overhauling its cyber range platform partway through the semester, introducing a new feature where users would be occasionally required to correctly respond to short answer and multiple choice questions in order to proceed. There were several occasions where the platform would not accept answers that, by all appearances, should have been correct. These issues were eventually resolved, but they significantly hindered my progress at the time.

I do not believe there is much I could have done to improve my performance on the lab assignments, generally speaking. There is one lab on which I received poor marks as a result of a procedural error in which I forgot to include a certificate of completion and update the table of contents prior to submitting, but that was not because of any failure on my part to understand the lab content or competently write about it. Apart from that, and a couple of early labs on which I received minor deductions for underdeveloped technical overviews, I received perfect marks on all of the lab assignments, so there is — more or less by definition — nothing I could have done better.