Thesis Project Portfolio

Building a Cyber Range for UVA Computer Science Students

(Technical Report)

An Analysis of the Effects of Open-Source Cyber Weapons

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Chase Hildebrand

Spring, 2024

Department of Computer Science

Table of Contents

Executive Summary

Since the inception of the internet, hackers have made it their mission to exploit its vulnerabilities. As the number of connected devices increases each year, so does the number of cyberattacks targeting them. These attacks are becoming more sophisticated and rampant, highlighting a serious problem: there are not enough people to defend our networks from these threats. Addressing the gap in the future cyber workforce starts with enhancing students' educational experience in their collegiate years. Unfortunately, while the University of Virginia (UVA) has resources for computing research, those resources are either restricted to a select group or insufficient for simulating realistic environments conducive for cultivating practical skills. My technical project is an undertaking to build a cyber range for UVA students, enabling them to get more hands-on experience with cybersecurity. Additionally, when teaching cybersecurity, it is incredibly helpful to use the open-source software written by the cybersecurity community to emulate how attackers attack. However, an increasing number of attackers are abusing publicly available open-source tools to attack their victims. My STS project focuses on a somewhat controversial subset of these tools—command and control frameworks—which are tools that let attackers control their victim's systems remotely, and aims to dig deeper to better understand the extent to which these frameworks are helping or hurting the security of our society.

My STS paper seeks to investigate how different groups use open-source C2 frameworks to understand the extent to which building and releasing these malicious software is harmful or helpful to the security of our society. Using Actor-Network Theory (ANT), I found that while attackers make ample use of open-source C2 frameworks, so do many students, security researchers, and penetration testers. A significant portion of these tools were built by security professionals to test their defensive tools, share new techniques or vulnerabilities, and teach cybersecurity. Students use them to learn how to attack and thus defend systems, researchers use them to test cutting-edge intrusion detection systems, and penetration testers use them to simulate adversaries. Because these tools are both so useful and complex, forcing everyone who needs them to write them from scratch will likely cause significant wasted effort in the security community. Overall, the benefit gained from allowing and encouraging the cybersecurity community to release open-source frameworks outweighs the risk of the havoc that attackers cause with them.

To address the infrastructure deficit at UVA, our team designed and implemented a cyber range to provide students with hands-on cybersecurity experience. The cyber range serves as a sandbox for simulating realistic networks, enabling students to gain practical experience attacking or defending enterprise-grade systems. This platform will also enable club leaders, competition organizers, and instructors to easily set up lab environments for workshops, competitions, and classes. The cyber range is designed with scalability, reliability, and user experience in mind. Currently, it can support up to 200 simultaneous students and 2000 simultaneous virtual machines, but is designed to easily scale to account for future needs. The cyber range is a cluster consisting of eighteen servers: three for storage, three for control, and twelve for compute. We chose OpenStack as our virtualization platform and Ceph as our storage solution due to their scalability, extensibility, automation support, documentation, and community support. Future work will focus on developing user-friendly automation to enable users to rapidly create large virtual environments with ease.

Building a cyber range for UVA students and preserving the openness of open-source command and control frameworks are significant steps in alleviating the cybersecurity skill issue both in industry and within the UVA community.