|  |  |  |
| --- | --- | --- |
| Course # | James Riley Dorough | Target System Network Prep Continued |
| CSIS 462 | **16MAR22** | **Semester Week 10, Lab 6** |

Title

* Outline future for offensive operations for the last duration of the semester

Introduction

Through the last few weeks of the semester, there are a few different objectives that still need to be met. Some of these are red team labs. Others are reporting and presenting to the blue team. Most of the work from here on will be documenting all operations against blue team networks. This includes cleaning red team malware from the target networks and exfiltrating personal code or exploits. This document will outline my planning process as it stands for the remainder of the semester.

Discussion

As we approach the end of the semester. I intend to focus on increasingly noisy attacks to encourage blue team members to seek out the methods I used or the services I exploited to break into their boxes. I also intend to participate in mild damage to their boxes in ways of annoyance or misdirection to allow them to learn how to fix their systems and the tools/ binaries available to them. There still are a few required labs to meet, and I will focus on those before I engage in additional practice.

The two uncompleted labs so far are the covert persistence and hash exploitation labs. I will finish these and then move on with additional activities to provide more reporting and exposure in the upcoming full penetration testing report, lessons learned report, and the two live presentations to the blue team. After these objectives have been met, I plan on working with some of the more experienced students in our course and on the MACCDC team to learn new, more noticeable, alterations I can make to blue team systems. After all this, I plan to recover some of my code, mostly PowerShell. However, this should be simple as my code is hosted on the red team’s clone of the target network.

Conclusion

The finish line is in sight, but we’re not there yet. I plan to finish strong and use the next few weeks to continue learning new TTPs and utilities for penetration testing. I hope the blue team has been able to learn from my work so far, and I intend to give them more problems over the next few weeks. I will most likely continue to focus on Windows and PowerShell as I am very unfamiliar with offense and defense on that OS. I will need to experience to help prepare me for the Air Force’s cyber training pipeline.