Cyber Operations

Prerequisites: Students may come from Computer Science, Network and Security Administration, Cyber Operations, or related fields. Each student is expected to bring experience in networking, scripting/programming, and Windows/UNIX environments.

# Course Description

Working individually and in teams, students will cover several areas surrounding Cyber Operations. The course will be comprised of several hands-on and lab-based activities that require a demonstration and understanding of relevant areas. The lab activities are designed to follow the technical and professional approaches to solving cyber operation tasks.

Lab and instructional topics come from skill and problem requirements identified by industry and government alike.

Each module requires a deliverable from the students. Most often, the deliverables are documentation showing the process and successful solution to requested tasks. Students primarily demonstrate their lab work through screenshots, scripts, and presentation of topics.

**Objectives:**

* The student will learn to proper tools and techniques for conducting penetration testing and security audits. Students will be able to demonstrate an understanding of and apply skills in the following areas:
* Phases of penetration testing including reconnaissance, scanning, exploitation, post exploitation & maintaining access, and reporting on Windows and Linux systems.
* Gathering open source intelligence (OSINT) information from a variety of sources.
* Advanced search operators to find and profile information passively.
* Active port scanning techniques and firewall evasion methods.
* Vulnerability scanning with multiple products and custom scripts along with interpreting and understanding results/exploitability.
* Exploitation of systems using open source and custom developed scripts and code.
* Pivoting through a system to attain higher levels of access, privilege escalation, or a more favorable standpoint in the network.
* Secure password retrieval and password cracking methodologies including brute-force, wordlist, rainbow tables, and GPUs.
* Maintaining access, installing backdoors, and establishing persistence in a network.
* Writing basic exploit code for use in frameworks such as Metasploit.
* Reporting and interpreting results to clearly demonstrate vulnerabilities within a framework.

**Materials:**

Required Text

 No text is specifically required for the completion of this course; however, supplemental materials listed may help with the configuration and execution of tools to be used in labs.

A machine or lab environment capable of running 2-4 virtual machines simultaneously will be necessary to complete lab exercises.

Additional Materials

1. **The Hacker Playbook 2: Practical Guide To Penetration Testing**

Peter Kim

ISBN-10: 1512214566

Publisher: CreateSpace Independent Publishing Platform

1. **Basics of Hacking & Penetration Testing, 2nd Ed**

Pat Engebretson

ISBN-10: 0124116442

Publisher Syngress

**Technical Specifications:**

Students must have high-speed internet access and administrative permissions on their PC. Windows or Mac operating systems are preferred; you are welcome to use other operating systems as well but be aware we may not have documentation available for all other \*nix variants.

Students will need a virtualization environment (e.g. VMware Worksataion Player or Virtual Box) or have the ability to hose VMs.

**Grading:**

Grading will be composed of labs, quizzes, and exams/projects. The graded activities are point-based.

|  |  |
| --- | --- |
| **Assessment Mechanism** | **Points** |
| Labs | 20 |
| Exams | 50 |
| Quizzes | 10 |

**Course Schedule:**

See the attached Excel document: **Cyber Operations Weekly Schedule.xlsx**