Introduction to Cyber Security

Nature of the course: Theory + Practical

Total hours per day: 2 hours

Course duration: 4 weeks

Course Summary

This course covers cyber security, ethical hacking, ethical hacking phases, and numerous attack vectors, preventing countermeasures, Bug Bunty Hunting, Penetration Testing, and Forensics, among other topics.

This will give you an insight into how hackers think and act maliciously, allowing you to better build up your security infrastructure and protect against future attacks. Organizations can increase their system security measures by understanding system flaws and vulnerabilities, lowering the chance of an incident.

Completion Criteria

After fulfilling all of the following criteria, the student will be deemed to have finished the Module:

1. Has attended 90% of all classes held
2. Has received an average grade of 80% on all assignments
3. Has received an average of 60% in assessments
4. The tutor believes the student has grasped all of the concepts and is ready to go on to the second module.

Required Text Books

- The Cyber Effect
- The Hacker Playbook 3: Practical Guide To Penetration Testing
- Cyber Security: Law and Guidance

Prerequisites

- Basic knowledge about programming, bits/bytes, procedures, classes, computer architecture, etc. If you just have a theoretical knowledge that is perfectly okay but you should have strong convictions on what programming is, and what you hope to achieve from this class.
- Willing and eager to spend at least 10-20 hours (varying from student-to-student) per week outside of the training class to self-study and practice.
- If you are only interested in theory and have no interest/patience in spending at least 10 hours every week throughout the duration of the course, then this course might not be for you.
- If you have absolutely no idea about programming or do not see yourself doing programming in the next six -odd months, then this class may not be for you!

Course Details

WEEK 1

Introduction to Cyber Security
Introduction to Ethical Hacking
Introduction to Bug Bounty Hunting
Introduction to Penetration Testing

WEEK 2

Foot printing and Reconnaissance
Scanning Networks
Enumeration
Vulnerability Analysis
System Hacking
Malware Threats

WEEK 3

Web Server & Web Application Hacking
SQL Injection
Network Attacks and Defense Strategies
Network Security Threats, Vulnerabilities, and Attacks
Network Security Controls, Protocols, and Devices
Network Security Policy Design and Implementation

WEEK 4

Host Security
Secure Firewall Configuration and Management
Secure IDS Configuration and Management
Network Traffic Monitoring and Analysis

LABS

Lab assignments will focus on the practice and mastery of contents covered in the lectures; and introduce critical and fundamental problem-solving techniques to the students.

Learning Outcomes

- To secure an IT infrastructure, analyze and fix security risks in networks and computer systems
- How to design, develop, test and evaluate secure software
- To handle enterprise security risks, develop rules and processes
- Assess and convey the human role in security systems, with a focus on ethics, social engineering flaws, and training
- Interpret and analyze security occurrences forensically.
- Able to understand and implement R programming from a statistical standpoint