deerwalk
training center

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:

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

Required Textbooks

- Mary Aiken, “The Cyber Effect”, Random House.
- Peter Kim, “The Hacker Playbook 3”, Peter Kim.
- Helden Wong, “Cyber Security: Law and Guidance”, Bloomsbury Professional.

Prerequisites

- Basic knowledge about programming, bits/bytes, procedures, classes,

computer architecture, etc. If you just have 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 read/write codes in JavaScript (self-study and practice).
- There is no prior educational level requirement for this course. Anyone from 10+2 student to someone who is doing her PHD in Genetic Engineering is welcome to take this course.
- 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 I

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

Week II

- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats

Week III

- 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 IV

- 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.