POLK STATE
Corporate College

Polk State College Apprenticeship Partnership in Information Technology (MAP IT)

Ethical Hacking

Eight-week course, Online, self-paced independent study
Total Course Cost: $836
Cost Breakdown: Credit Cost: $336, Books: $500
Cost covered by Grant: Lab Fees: $60, and one-time exam fee $599

This course emphasizes the techniques and methodologies applied for security-penetration testing. It includes hands-on instruction in various tools and methods used to analyze an information system to discover vulnerabilities and protect against information loss, cyber terrorism, and corporate espionage. The course provides an overview of fundamental security testing concepts, practical skillsets related to computer programming, and techniques to properly document a security test. In addition to exploring the legal and ethical ramifications of penetration testing, the student develops the ability to apply appropriate countermeasures that reduce the risk to an organization.

OJT Competencies: This training develops the student's ability to:

Responsibilities of ethical hackers

- Discriminate mechanisms of authorization and identify the aspects of the *Computer Fraud and Abuse Act* (CFAA) relative to federal crime.

Types of Pentest and Red Team Engagements
-Internal and External Network Pentests:

- Gain access to data, devices, or networks by uncovering vulnerabilities.

-Wireless Pentest:

- Discriminate among the types of attacks that affect wireless networks.

-Social Engineering and Phishing Assessment:

- Interpret and leverage pretexts to gain access to data, devices, or credentials.

-Physical Security Pentest:

- Recognize how to bypass security controls for people, processes, and property.

-Mobile Application Pentest:

- Recognize the vulnerabilities affecting iOS and Android applications.

-Web Application Pentest:

- Identify the top ten OWASP vulnerabilities for web applications and how to test them.

-Hardware Device Pentest:

- Demonstrate fluency regarding of hardware- related security vulnerabilities.

Red Team Operation:

- Recognize the objectives between a red team operation and pentest.
- Determine the scope of a pentest.
- Assess the scope of an engagement.
- Identify when an organization is authorized to grant permission versus when third-party authorization is required.
- Determine how to properly capture an organization’s needs.
- Recognize how to mitigate scope-creep requests from an organization.
- Identify engagement boundaries to avoid illegally accessing out-of-scope areas.
- Recognize the lifecycle of a pentest.
- Apply passive and active open-source intelligence (OSINT) to perform reconnaissance against an organization.
- Execute a successful vulnerability scan against the perimeter of a network and its applications.
- Leverage vulnerabilities to gain access to networks, devices, or applications.
- Document the vulnerabilities of an organization and make recommendations in a way that demonstrates risks to the organization.