PENETRATION TESTING, CERTIFICATE OF ACCOMPLISHMENT

3_CE_PENTST

This Certificate of Accomplishment will provide students with a foundation in the field of Penetration Testing. The courses include fundamental skills needed in information security, cybersecurity principles, ethical hacking, and penetration testing. The emphasis on hands-on security practices and vulnerability testing will provide students with the foundational skills needed for an entry-level career in penetration testing. Topics covered will include computer and network security, infrastructure and operational security, risk mitigation, ethics, hardware vulnerabilities, hacker techniques, and security policies and procedures.

Program Level Student Learning Outcomes

1. Given a lab scenario, use vulnerability testing tools to find system vulnerabilities.
2. Explain the process of leveraging information to prepare for exploitation.
3. Using report writing and handling best practices, report on findings and remediation.

Certificate Graduation Requirements

A Certificate is awarded upon completion of the required coursework with a grade of C or higher in each course. To receive the certificate, the student must file a petition for graduation during his/her final semester. In addition:

Certificate of Accomplishment

- Students must also earn a minimum of 12 units of coursework at Coastline, excluding experiential credit.
- A student with prior experience may be excused from certain certificate courses.
- 50 percent of the certificate program's units must be completed at Coastline no matter how the total number of units required for the certificate can be met.

Course	Title	Units
Required Core		
Students will complete all of the following:		
CST C191	CompTIA Linux+	3
CST C230	Introduction to Security	3
CST C232	Ethical Hacking	3
CST C242	PenTest+	3
Total Units		12