PENETRATION TEST PROFESSIONAL CERTIFICATE OF ACHIEVEMENT

This certificate provides graduates with best practices penetration testing skills to safeguard enterprises against modern cyber-attacks. Students receive extensive hands-on experience and develop the knowledge and abilities necessary to apply the tools and methods used by cyber criminals to the protection of an organization's data and operations. Upon completion of the program, students will develop penetration testing skills based on real-world training scenarios.

Required Courses:		Units
CSC 116	Information and Communication Technology Essentials	4
CSC 117	Computer Network Fundamentals	3
CSC 118	Introduction to Information Systems Security	3
CSC 152	Network OS and Administration	3
CSC 158	Introduction to Cybersecurity: Ethical Hacking	3
CSC 159	Fundamentals of Penetration Testing	4
CSC 161	Cloud Infrastructure and Security	3
CSC 221	Programming and Algorithms I	3
Plus 3 additional units selected from the following:		**Units**
BUS 107	Customer Service	3
BUS 134	Human Relations in Business	3
BUS 170	Business Communication Skills for Managers	3

Total units required for Certificate   **29**

Program Level Student Learning Outcomes:
1. Define best practices for penetration testing.
2. Define the requirements for proper planning, implementation, and documentation of penetration tests.
3. Implement penetration testing across a wide range of scenarios including internal/external/perimeter network penetration testing, web application penetration testing, and cloud penetration testing.

Career Opportunities in COMPUTER SCIENCE

This program prepares students for careers in the Cybersecurity field. Some common job titles and careers for this certificate include ethical hackers, penetration testers, network server administrators, firewall administrators, security testers, system administrators and risk assessment professionals, information security analyst, and network security penetration tester.