COCONINO COMMUNITY COLLEGE
COURSE OUTLINE

Prepared by: D. Marshall, J. Jones, S. Rencher Date: Fall 2019
Status: Permanent
Effective Term: Fall 2020

A. **Identification:**

1. Subject Area: Computer Information Systems
2. Course Number: CIS 262
3. Course Title: Ethical Hacking for Cybersecurity
4. Credit Hours: 4
5. Catalog Description: Prerequisite: CIS 261. This course will prepare students for practical comprehension and awareness of network attack strategies and common countermeasures. Students will develop the knowledge and skills required to plan and scope an assessment, to explain legal and compliance requirements, perform vulnerability scanning and penetration testing, analyze data, and effectively report and communicate results. Four credits lecture.

B. **Course Goals:** To develop the skills required for students to assess, evaluate and report on security issues arising within the network of an organization. The student will be able to navigate that network to find vulnerabilities and security issues and suggest or implement the needed changes to combat these vulnerabilities. The student will also be able to develop a plan and present this plan to stakeholders explaining the problem(s) and the associated resolution(s).

C. **Course Outcomes:**

Upon successful completion of this course, students will be able to:

1. plan and scope an assessment;
2. explain legal and compliance requirements;
3. perform vulnerability scanning and penetration testing using appropriate tools and techniques;
4. analyze the results of testing;
5. produce a written report containing proposed remediation techniques providing practical recommendations;
6. communicate results.

D. **Course Outcomes Assessment**

Will include:

1. Exams;
2. Graded lab simulations.

E. **Course Content will include:**

1. planning for an engagement, understanding the audience and support resources
2. compliance based assessments
3. packet inspection, crafting, cryptography and open source intelligence gathering
4. mapping vulnerabilities and prioritizing activities in preparation for penetration test
5. social engineering attacks
6. exploiting network-based, wireless and application-based vulnerabilities
7. NMap and other penetration and reconnaissance tools
8. report writing of findings and remediation
9. communication paths, triggers and goal reprioritization