Lecture Contact Hours: 32-36; Homework Hours: 64-72; Total Student Learning Hours: 96-108
Laboratory Contact Hours: 48-54; Homework Hours: 0; Total Student Learning Hours: 48-54

CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

COMPUTER AND INFORMATION SCIENCE 264 - ETHICAL CYBERSECURITY HACKING

2 hours lecture, 3 hours laboratory, 3 units

Catalog Description
This course immerses IT Professionals in hands-on intensive environments, providing in-depth knowledge and experience with current essential security systems. Provides understanding of perimeter defenses and leads to scanning and attacking networks; no real networks are harmed. Students learn how intruders escalate privileges and the steps to be taken to secure a system. Also covers Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virtual Creation. Focus includes legal and regulatory requirements, ethical issues, basic methodology and technical tools used for ethical hacking and penetration tests. Students establish a pre-test agreement with the enterprise, discover and exploit vulnerabilities, participate as a member of a pen test team and prepare a penetration test report.

Prerequisite
"C" grade or higher or "Pass" in CIS 263 or CIS 209

Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) Identify major types of attack and malicious code.
2) Identify network security vulnerabilities.
3) Conduct a small security assessment, develop a security policy, and design a secure network topology.
4) Configure security software, protocols, encryption, remote access technologies, authentication and authorization services, intrusion detection services, and equipment.

Course Content
1) Footprinting and Reconnaissance
2) Scanning Networks
3) Enumeration
4) System Hacking
5) Trojans and Backdoors
6) Viruses and Worms
7) Sniffing
8) Social Engineering
9) Denial of Service
10) Session Hijacking
11) Hacking Webservers
12) Hacking Web Applications
13) SQL Injection
14) Hacking Wireless Networks
15) Hacking Mobile Platforms
16) Evading IDS, Firewall, and Honeypots
17) Buffer Overflow
18) Cryptography
19) Penetration Testing

Course Objectives
Students will be able to:
1) Evaluate the legal and regulatory requirements of ethical hacking and penetration tests.
2) Produce a penetration test authorization and rules of engagement document.
3) Contrast penetration testing methodologies.
4) Derive system reconnaissance and network scan to detect open ports and vulnerable systems.
5) Elaborate social engineering techniques for a penetration test.
6) Compile penetration test scanning results to exploit vulnerabilities.

Method of Evaluation
A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in the subject matter determined by multiple measurements for evaluation, one of which must be essay exams, skills demonstration or, where appropriate, the symbol system.
1) Essay Examinations
2) Objective Examinations and quizzes
3) Problem Solving Examination
4) Skill Demonstrations: securing a provided network
5) Classroom Discussion
6) Reports: students will be provided with specific scenarios relating to "real life" events that have taken place that relate to cyber security breaches and will be instructed to provide a limited written report relative to implementation of procedures and processes designed to combat future potential breaches. Instructor will evaluate the report based upon a rubric provided to students.

Special Materials Required of Student
Electronic storage media, reliable access to Internet

Minimum Instructional Facilities
Smart computer lab with whiteboards, Internet browser, Internet connectivity, software, printer; network connection not connected to school academic resources Virtual Machine (VM) environment for students to work (Netlab).

Method of Instruction
1) Lecture and demonstration in a traditional classroom or via electronic means
2) Hands-on practice in either a dedicated or a virtual lab environment
3) Topical discussion of current operating system trends and issues

Out-of-Class Assignments
1) Utilizing virtual machines configured with windows and windows server operating systems:
   a. Configure specific computer security functions and/or subsystems.
   b. Troubleshoot/analyze imposed security problems, investigate potential alternatives, and implement corrective action to achieve a determined result.
2) Read and analyze instructor assigned case studies; post analysis and comments to the class discussion board.
3) Respond to other students' analysis and comments on the class discussion board.

Texts and References
1) Required (representative example): Orivano, Sean-Philip. *Hacker Techniques, Tools, and Incident Handling.* 2nd Edition. Jones and Bartlett Learning, 2014.
2) Supplemental: None

Exit Skills

Students having successfully completed this course exit with the following skills, competencies and/or knowledge:

1) Evaluate the legal and regulatory requirements of ethical hacking and penetration tests.
2) Produce a penetration test authorization and rules of engagement document.
3) Contrast penetration testing methodologies.
4) Derive system reconnaissance and network scan to detect open ports and vulnerable systems.
5) Elaborate social engineering techniques for a penetration test.
6) Compile penetration test scanning results to exploit vulnerabilities.

Student Learning Outcomes

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

1) Describe the legal and regulatory requirements for ethical hacking and prepare documentation to reflect this skill and prepare the necessary documentation for authorization, performance, results and recommendations based on penetration testing.
2) Compare and contrast different penetration testing methodologies and describe the correct circumstance to apply those methodologies.
3) Perform system scan and reconnaissance to determine vulnerabilities, then create a report showing vulnerabilities and recommendations for rectifying the cited weaknesses.
4) Demonstrate social engineering techniques to discover system vulnerabilities.