SYLLABUS
PART I
EDISON STATE COMMUNITY COLLEGE
CYB 237S SYSTEMS VULNERABILITIES AND SECURITY
3 CREDIT HOURS

COURSE DESCRIPTION
In-depth exploration of ethical hacking techniques, allowing students to develop the skills needed to protect systems and networks from potential threats. Topics include penetration testing, reconnaissance, social engineering, system hacking, enumeration, vulnerability assessment, malware analysis, network sniffing, denial of service (DoS), session hijacking, web and mobile application security, cryptography, and cloud security. The course focuses on hands-on experience using tools and techniques used by ethical hackers, culminating in preparation for the EC-Council Certified Ethical Hacker (CEH) exam. By completing this course, students will be well-equipped to assess security vulnerabilities and implement countermeasures. Prerequisite: CYB 236S. Lab fee.

COURSE GOALS
The student will:

Bloom's Level		Program Outcomes
1	1. Recognize various cyber threat actors and ethical hacking principles.	1, 2
2	2. Describe the key phases of penetration testing and legal/ethical issues surrounding ethical hacking.	1, 2, 3
2	3. Identify social engineering and physical security vulnerabilities, and propose countermeasures.	3, 7
4	4. Analyze reconnaissance tools and techniques for gathering information on a target system.	3, 8
3	5. Perform scanning and enumeration to identify network vulnerabilities.	7, 8
5	6. Evaluate system hacking techniques, including password cracking and privilege escalation.	3, 7
3	7. Mitigate malware using anti-malware software and system defenses.	7, 8
5	8. Develop countermeasures for network security threats such as sniffing, session hijacking, and DoS attacks.	3, 7, 8
3	9. Implement security mechanisms such as firewalls, IDS, and honeypots for network defense.	7, 8
2	10. Explore cryptographic techniques to secure communications and protect data integrity.	4, 5
2	11. Summarize security risks related to cloud platforms, IoT devices, and mobile technologies.	5, 6
5	12. Create an ethical hacking report that includes findings, vulnerabilities, and recommended mitigation strategies.	1, 2, 8

CORE VALUES
The Core Values are a set of principles that guide in creating educational programs and environments at Edison State. They include communication, ethics, critical thinking, human diversity, inquiry/respect for learning, and interpersonal skills/teamwork. The goals, objectives, and activities in this course will introduce/reinforce these Core Values whenever appropriate.

TOPIC OUTLINE

1. Introduction to Ethical Hacking
2. Introduction to Penetration Testing
3. Penetration Testing Process and Threat Actors
4. Social Engineering and Physical Security
5. Reconnaissance Techniques and Tools
6. Scanning and Enumeration
7. Vulnerability Analysis and Assessment
8. System Hacking and Privilege Escalation
9. Malware Analysis and Countermeasures
10. Network Sniffing and Session Hijacking
11. Denial of Service (DoS) Attacks
12. IDS, Firewalls, and Honeypots
13. Web Application and SQL Injection Attacks
14. Wi-Fi, Bluetooth, and Mobile Device Security
15. Cloud Computing and Internet of Things IoT Vulnerabilities
16. Cryptography and Data Protection
17. Ethical Hacking Report and Documentation