



MERCER
COUNTY COMMUNITY COLLEGE

COURSE OUTLINE

Course Number NET 245	Course Title Ethical Hacking	Credits 3
Hours: Lecture/Lab/Other 2/2/0	Co-requisite NET102, NET104	Implementation Semester & Year Fall 2022

Catalog description:

Combines an ethical hacking methodology with the hands-on application of security tools to better help students secure their systems. Students are introduced to common countermeasures that effectively reduce and/or mitigate attacks, including penetration testing, reconnaissance/open source intelligence gathering, scanning, enumeration, exploitation, and post-exploitation. Hands-on activities reinforce certification exam objectives.

General Education Category:

Not GenEd

Course coordinator:

Winston H. Maddox, Professor Networking, Information Technology and Cybersecurity
609.570.3867, maddoxw@mccc.edu

Required texts & Other materials:

COMPTIA-TESTOut Web Material ISBN:(978-1-935080-69-5)

Course Student Learning Outcomes (SLO):

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

1. Utilize various information security tools given different target systems in different environments; **(ILG: 4; PLO: 1,3)**
2. Discuss how the tools interrelate with each other in an overall penetration testing process; **ILG: 2, 4, 11; PLO: 2, 5)**
3. Implement countermeasures for various types of attacks; **ILG: 4; PLO: 3, 4, 5)**
4. Apply a common ethical hacking methodology to carry out a penetration test; **(ILG: 11; PLO:2, 6, 7)**
5. Analyze how penetration testing and ethical hacking fit into a comprehensive enterprise information security program; **(ILG: 11; PLO: 2, 6)**
6. Demonstrate ethical behavior appropriate to security-related technologies); **(ILG: 9, 11; PLO: 1, 5, 7)**

Course-specific Institutional Learning Goals (ILG):

Institutional Learning Goal 2. Mathematics. Students will use appropriate mathematical and statistical concepts and operations to interpret data and to solve problems.

Institutional Learning Goal 4. Technology. Students will use computer systems or other appropriate forms of technology to achieve educational and personal goals...

Institutional Learning Goal 9. Ethical Reasoning and Action. Students will understand ethical frameworks, issues, and situations.

Institutional Learning Goal 11. Critical Thinking: Students will use critical thinking skills understand, analyze, or apply information or solve problems.

Program Learning Outcomes (PLO) for Information Technology – Cybersecurity Concentration (A.A.S.)

1. Describe the elements of information security, including possible threats and attack vectors as well as the motives, goals, and objectives of information security attacks;
2. Explain what steps can be taken to secure a system, and provide secure network management and reporting;
3. Secure routers and switches and their associated networks, including installing, troubleshooting, and monitoring network devices to maintain integrity, confidentiality, and availability of data and devices;
4. Prevent common security threats, including implementing firewall and VPN technologies and perimeter defenses, conducting vulnerability and penetration testing, and scanning networked systems;
5. Describe the security weaknesses inherent in wireless networks, and implement solutions to address them;
6. Use printed and online technical documentation, and demonstrate written and oral communication skills;
7. Work effectively individually and in workgroups to install and implement information security technology

Units of study in detail – Unit Student Learning Outcomes:

Unit I Introduction to Ethical Hacking [Supports Course SLO # 1]

Learning Objectives

Students will be able to:

- Understand the Hacker Mindset
- Gain an overview of Ethical Hacking
- Understand the Role of Ethical Hacking
- Learn common Hacking Methodologies

Unit II Introduction to Penetration Testing [Supports Course SLO # 2]

Learning Objectives

The student will be able to...

- Penetration Test Process and Types
- Threat Actors
- Target Selection
- Assessment Types
- Legal and Ethical Compliance

Unit III Social Engineering and Physical Security [Supports Course SLO # 6]

Learning Objectives

The student will be able to...

- Social Engineering
- Physical Security
- Countermeasures and Prevention

Unit IV Reconnaissance [Supports Course SLO # 1]

Learning Objectives

The student will be able to...

- Reconnaissance Overview
- Perform Reconnaissance with Harvester
- Implement Nmap
- Reconnaissance Countermeasures
- Countermeasures View of Windows
- Manage Linux

Unit V Scanning [Supports Course SLO # 2]

Learning Objectives

The student will be able to...

- *Configure and explain:*
 - Scanning overview process
 - Scanning tools
 - Internal and external scanning
 - Scanning utilizing Nmap Scripts
 - Banner grabbing methods

Unit VI Enumeration [Supports Course SLO # 3]

Learning Objectives

The student will be able to...

- Understand IPS, IDS, NIDS, HIDS
- Analyze Information Collected
- Enumeration overview
- Windows system enumeration
- NetBIOS Enumeration
- Review Ports and Services
- Enumeration Countermeasures

Unit VII Analyze Vulnerabilities [Supports Course SLO # 5]

Learning Objectives

The student will be able to...

- Develop and implement Vulnerability Assessments
- Manage vulnerability life cycles
- Implement Scoring systems
- Manage vulnerability assessment tools
- Windows assessment tools

Unit VIII SYSTEM Hacking & Malware [Supports Course SLO # 3]

Learning Objectives

The student will be able to...

- Identify System Hacking
- Manage Privilege Escalation
- Maintain Access
- Develop a firm knowledge of "Cover Your Tracks"
- Malware: Trojans and Backdoors
- Develop knowledge to Combat Malware

Unit IX Sniffer, Session Hacking & DOS [Supports Course SLO # 4]

Learning Objectives

The student will be able to...

- Explain Sniffers: Network Traffic with Wireshark
- Explain Spoof of Addresses
- Analyze and Analyze Traffic
- Filter and Analyze Email Traffic
- Explain Session Hacking
- Perform a Man-in-the-Middle DHCP Attack
- Explain Denial of Service
- Identify Dos Attack

Unit X IDS, FIREWALLS, AND HONEYPOTS [Supports Course SLO # 5]

Learning Objectives

The student will be able to...

Explain Intrusion Detection Systems

- Implement Intrusion Detection
- Explain Avoid IDS Detection
- Explain Firewalls
- Configure a Perimeter Firewall
- Perform a Decoy Scan
- Explain Honeypots and the use with Pentbox

Unit XI WEB SERVERS, WEB APPLICATIONS, AND SQL INJECTIONS [Supports Course SLO # 4]

Learning Objectives

The student will be able to...

- Understand explain: Web Serves in Hacking
- Mirror a Website with appropriate tools
- Extract Web Server Information
- Explain critical Hacking Issue with Web Applications
- Explain SQL
- Perform an SQL Injection Countermeasures

Unit XII WI-FI, CLOUD COMPUTING AND INTERNET OF THINGS [Supports Course SLO # 5]

Learning Objectives

The student will be able to...

- Explain the critical functions of WI-FI
- Discuss key points with Mobile Devices Hacking
- Discuss Bluetooth Hacking
- Explain Cloud Computing and Attacks Issues
- Discuss IOT Technologies and Protocols

Unit XII **CRYPTOGRAPHY [Supports Course SLO # 6]**

Learning Objectives

The student will be able to...

- Explain the critical aspects of Cryptography
- Develop a functional knowledge of:
 - Public Key Infrastructure
 - Cryptography Implementation
 - Cryptanalysis and Cryptographic Attack Countermeasures

Evaluation of student learning:

Evaluation of student learning: [Evaluates SLOs #1, 2, 3, 4, 5, 6]

Students' achievement of the course objectives evaluated with the following:

- CompTIA-TESTOut Lab assignments assessing students' comprehension skills related to the unit objectives.
- CompTIA-TESTOut Lab Chapter quizzes assessing students' comprehension of software computer concepts related to the unit objectives.
- Research and Final Research presentation assessing students' comprehension through the use of word, PowerPoint and graphics to demonstrate knowledge,
- Basic programming Labs and Quizzes assignments assessing students' basic comprehension of hardware functions and skills related to the unit objectives.
- Exams and Final Research Presentation assessing students' comprehension of computer concepts and applications related to the unit objectives.

Grade Criteria

Item	Percent	Description
TESTOut Labs	10%	Activity-based lab Assignment in Excel
TESTOut Quizzes	10%	15 Question quiz for each unit of Computer Concepts
Exams	35%	3 Assignment based on your IT Topics leading to the final project
Final Research Presentation	45%	Professional Presentation