Salem STATE | UNIVERSITY

Computer Science Department
cs.salemstate.edu

ITE335 Ethical Hacking and Penetration Testing 3 cr.

Catalog Description:

Ethical hacking and penetration testing are critical skills in today's cybersecurity landscape. This course provides an introduction to ethical hacking and penetration testing, focusing on the principles, methodologies, and tools used to secure computer systems and networks. Students will learn ethical hacking techniques, penetration methodologies, and the legal and ethical considerations associated with these practices. The course provides students with the knowledge and practical skills required to identify vulnerabilities, assess security measures, and protect computer systems and networks from cyber threats. Three lecture hours per week.

Prerequisite(s): ITE 315 or CSC 435

Course Narrative:

In an era defined by digital transformation, the discipline of cybersecurity plays a pivotal role in safeguarding our digital infrastructure. Within the realm of cybersecurity, the practice of ethical hacking and penetration testing stands as a critical discipline, ensuring the resilience and security of computer systems and networks. This course, "Ethical Hacking and Penetration Testing," offers a scholarly exploration of this domain, aimed at equipping students with the profound knowledge and analytical skills required to excel in this evolving field.

This course dives deep into the field of ethical hacking and penetration testing. The course provides a comprehensive understanding of the ethical and technical dimensions of cybersecurity. Through lectures, hands-on lab exercises, and homework, students will gain insight into the ethical hacker’s mindset and develop the capacity to systematically identify vulnerabilities, conduct security assessments, and devise effective protective measures.

Course Goals:

The purpose of this course is to develop students’ knowledge and understanding of ethical hacking and penetration testing. Specific goals are:

CG01: To demonstrate an understanding of the ethical and legal considerations that govern ethical hacking and penetration testing
CG02: To identify and exploit common security vulnerabilities and weaknesses in various systems
CG03: To become proficient in using industry-standard hacking tools and techniques
CG04: To develop the ability to create and implement effective security strategies to protect against cyber threats

CG05: To learn to assess network security, evaluate firewall rules, and identify weaknesses in network configurations and protocols

CG06: To adhere to ethical hacking best practices

Course Objectives:

Upon successful completion of the course, a student will have:

CO01: developed an understanding of the fundamental concepts of ethical hacking and penetration testing

CO02: gained hands-on experience with real-world scenarios and case studies

CO03: identified and assessed common vulnerabilities in computer systems and networks

CO04: conducted penetration tests using various tools and techniques

CO05: developed an understanding of legal and ethical guidelines while performing security assessments

Course topics:

- Introduction to Ethical Hacking and Penetration Testing
  - Role of Security and Penetration Testers
  - Penetration Testing Methodologies
- Legal and Ethical Framework for Hacking
  - What can you do legally
  - What you cannot do legally
- Information Gathering and Reconnaissance
  - Reconnaissance Types
  - Passive Reconnaissance Techniques
  - Active Reconnaissance Techniques
- Scanning and Enumeration
  - Introduction to Port Scanning
  - Using Port Scanning Tools
  - Conducting Ping Sweeps
  - Understanding Scripting
  - Introduction to Enumeration
  - Enumerating OS
- Exploitation and Post-Exploitation Techniques
  - Selecting Targets to Exploit
  - Exploit Frameworks
  - Common Exploits
  - Post Exploitation
  - Persistence

- Incident Response and Handling
    - Communicating in Real Time during a Pen Test
    - Communicating Findings and Recommending Remediation
    - Writing a Pen-Test Report
- Network, Web Application Security, and Social Engineering
    - Introduction to Wireless Networks and Web Application Security
    - Using Honeypots
    - Understanding Wardriving
    - Understanding Wireless Hacking
    - Tools for Web Attackers and Security Testers
    - Using Technology for Social Engineering
    - Physical Attacks
- Ethical Hacking Best Practices and Reporting
- Emerging Trends in Cybersecurity

Assignments and Examination:

The course consists of lectures, homework assignments, quizzes, hands-on lab assignments, and two exams – a midterm and a final. The course grade will be determined using the following approximate weights: final exam: 20%, midterm exam: 20%, written homework 20%, hands-on lab assignments 20%, and quizzes: 20%.

Course Objective / Assessment Mechanism matrix

	Homework	**Quizzes**	**Hands-on Lab**	**Midterm**	**Final**
CO01	✓	✓	✓	✓	✓
CO02	✓		✓		
CO03	✓	✓	✓	✓	✓
CO04	✓		✓	✓	✓
CO05	✓	✓	✓	✓	✓

Bibliography:

1. Rob S. Wilson, Michael T. Simpson, and Nicholas Antill. **Hands-On Ethical Hacking and Network Defense**. Cengage Publishers 4th edition 2023.
2. Rob S. Wilson. **CompTIA Pentest+ Guide To Penetration Testing.** Cengage Publishers. 1st edition 2024.
3. Michael Gregg and Omar Santos. **CEH Certified Ethical Hacker Cert. Guide**. Pearson IT Certification Publishing. 4th edition 2022.

4. Chuck Easttom. **CEH Certified Ethical Hacker.** Pearson IT Certification Publishing. 1st edition 2022.
5. EC-Council. **Ethical Hacking and Countermeasure: Web Applications and Data Servers.** Cengage Publishers. 2nd edition 2017.
6. Ric Messier. **CEH v11 Certified Ethical hacker Study Guide**. Wiley Publishers. 2021.
7. Sean-Philip Oriyano. **Penetration Testing Essentials.** Wiley Publishers. 2017.
8. Matt Walker. **CEH Certified Ethical Hacker Bundle.** McGraw Hill Publishers. 5th edition 2022.
9. Zaid Sabih. **Learn Ethical Hacking from Scratch.** Packt Publishing. 2018
10. Michael G. Solomon and Sean-Philip Oriyano. **Ethical hacking: Techniques, Tools, and Countermeasures**. Jones & Bartlett Learning. 4th edition 2022.
11. Ahmed Sheikh. **CEH Preparation Guide: Lesson-Based Review of Ethical hacking and Penetration Testing.** Apress Publihsers. 2021.