COURSE SYLLABUS

LAST REVIEW	Fall 2022
COURSE TITLE	Ethical Hacking & Penetration Testing
COURSE NUMBER	CIST 0135
DIVISION	Career and Technical Education
DEPARTMENT	CIST
CIP CODE	24.0101
CREDIT HOURS	3
CONTACT HOURS/WEEK	Class: 1 Lab: 4
PREREQUISITES	None

COURSE DESCRIPTION

This course provides students with valuable skills, knowledge and practice needed in ethical hacking and penetration testing. Students will understand the importance of vulnerability assessments and gain industry knowledge and skills in penetration testing. The course helps students learn how to attack and assess different types of systems and networks. Upon completing the course, students will learn how to secure information systems against attacks such as viruses, worms, and other system weaknesses that pose significant danger to organizational data.

PROGRAM ALIGNMENT

This course is part of a program aligned through the Kansas Board of Regents and Technical Education Authority. For more information, please visit: https://kansasregents.org/workforce_development/program-alignment

PROGRAM LEARNING OUTCOMES

1. Demonstrates the necessary skills to score at least a 70% in the Network 1 course.
2. Obtain the skills necessary to pass the Certification COMPTIA SEC+ certification.
3. Applies judicious and ethical offensive security techniques using knowledge gained through cyber security coursework.
4. Obtain the skills necessary to pass the NET+ certification.

TEXTBOOKS

http://kckccbookstore.com/

METHOD OF INSTRUCTION

A variety of instructional methods may be used depending on content area. These include but are not limited to lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE

I. Introduction to Ethical Hacking
   A. Information Security Overview
   B. Information Security Threats and Attack Vectors
   C. Hacking Concepts and Phases
   D. Types of Attacks

II. Cryptography
   A. Cryptography Concepts, attacks, and tools
   B. Encryption Algorithms
   C. Public Key Infrastructure (PKI)
   D. Email and Disk Encryption

III. Penetration Testing
   A. Pen Testing Concepts
   B. Types of Pen Testing
   C. Pen Testing Techniques, Phases and Roadmap
   D. Outsourcing Pen Testing Services

IV. Foot printing and Reconnaissance
   A. Foot printing Concepts
   B. Foot printing Threats
   C. Foot printing Methodology and Tools
   D. Foot printing Countermeasures and Penetration Testing

V. Scanning Networks
   A. Overview of Network Scanning
   B. CEH Scanning Methodology

VI. Enumeration
   A. Enumeration Concepts
   B. NetBIOS, SNMP, LDAP, NTP, SMTP and DNS Enumeration
   C. UNIX/Linux Enumeration
   D. Enumeration Countermeasures and Pen Testing

VII. System Hacking
   A. Information at Hand before System Hacking Stage
   B. System Hacking: Goals
   C. CEH Hacking Methodology
   D. CEH System Hacking Steps

VIII. Trojans and Backdoors
   A. Trojan Concepts
   B. Trojan Infection and Detection

  - C. Types of Trojans
  - D. Countermeasures
- IX. Viruses and Worms
  - A. Virus and Worms Concepts
  - B. Types of Viruses and Computer Worms
  - C. Malware Analysis
  - D. Countermeasures and Penetration Testing for Virus
- X. Sniffers
  - A. Sniffing Concepts and Tools
  - B. MAC, DHCP and Spoofing Attacks
  - C. ARP and DNS Poisoning
  - D. Sniffing Counter measures and Pen Testing
- XI. Social Engineering
  - A. Social Engineering Concepts and Techniques
  - B. Identity Theft
  - C. Social Engineering Countermeasures and Pen Testing.
- XII. Denial of Service
  - A. DoS/DDoS Concepts
  - B. DoS Attack Techniques and Tools
  - C. Botnet
  - D. DoS/DDoS Countermeasures and Protection Tools
- XIII. Session Hijacking
  - A. Session Hijacking Concepts
  - B. Network-level Session Hijacking
  - C. Session Hijacking Tools
  - D. Session Hijacking Countermeasures and Pen Testing
- XIV. Hacking Webservers
  - A. Webserver Concepts and Attacks
  - B. Webserver Attack Methodology and Tools
  - C. Patch Management and Webserver Security Tools
  - D. Webserver Countermeasures and Pen Testing.
- XV. Hacking Web Applications
  - A. Web App Concepts and Threats
  - B. Web App Hacking Methodology and Hacking Tools
  - C. Web App Countermeasures and Pen Testing
  - D. Web App Security Tools.
- XVI. Hacking Wireless Networks
  - A. Wireless Concepts, Encryption and Threats.
  - B. Wireless Hacking Methodology and Tools.
  - C. Wireless Security Tools.
  - D. Wireless Countermeasures and Pen Testing
- XVII. Evading IDS, Firewalls, and Honeypots
  - A. IDS, Firewall and Honeypot Concepts and Systems
  - B. Evading IDS and Firewalls

C. Detecting Honeypots
D. Firewall Evading Tools
E. Countermeasures and Penetration Testing.

XVIII. Buffer Overflow
A. Buffer Overflow Concepts and Methodology
B. Buffer Overflow Detection
C. Buffer Overflow Countermeasures and Penetration Testing
D. Buffer Overflow Security Tools

COURSE LEARNING OUTCOMES AND COMPETENCIES
Upon completion of the course, the student will:

A. Explain ethical hacking concepts.
1. Explain information security threats and attack vectors.
2. Explain hacking concepts, phases, and types of attacks.
3. Understand information security controls.

B. Explain the concept of cryptography.
4. Explain cryptography concepts, attacks, and tools.
5. Explain encryption algorithms.
6. Explain public key infrastructure.
7. Explain email and disk encryption.

C. Explain the importance of penetration testing.
8. Explain pen testing concepts and types of pen testing.
9. Explain pen testing techniques, phases, and roadmap.
10. Explain outsourcing pen testing services.

D. Explain foot printing and reconnaissance.
11. Understand the foot printing concepts.
12. Explain foot printing threats.
13. Explain foot printing methodology and tools.
14. Explain foot printing countermeasures and penetration testing.

E. Explain scanning networks process.
15. Explain network scanning process.
16. Define CEH scanning methodology.

F. Explain enumeration concepts.
17. Explain enumeration concepts.
18. Explain NetBIOS, SNMP, LDAP, NTP, SMTP and DNS enumeration concepts.
19. Understand UNIX/Linux enumeration.

G. Show knowledge of system hacking.
20. Understand system hacking goals.

21. Explain CEH hacking methodology.
22. Understand CEH system hacking steps.

H. Understand trojans, backdoors, viruses, worms, sniffers, and social engineering.
23. Understand trojan and worm's malware.
24. Understand backdoors techniques.
25. Understand viruses' malicious software.
26. Understand sniffers software concepts.
27. Explain social engineering concepts.

I. Understand denial of service concepts.
28. Explain DoS attack techniques and tools.
29. Explain DoS/DDoS protection tools.
30. Understand DoS attack penetration testing.

J. Explain session hijacking.
31. Understand network-level session hijacking.
32. Explain session hijacking tools.

K. Understand the process of hacking webservers, web applications and wireless networks.
33. Understand attack methodology and tools of webservers, web applications and wireless networks.
34. Explain security tools of webserver, web applications and wireless networks.
35. Countermeasures and pen testing for webserver, web applications and wireless networks.

L. Explain evading ids, firewalls, and honeypots.
36. Explain evading ids and firewalls.
37. Detect honeypots.

M. Explain buffer overflow.
38. Explain buffer overflow concepts and methodology.
39. Detect buffer overflow.

ASSESSMENT OF COURSE LEARNING OUTCOMES AND COMPETENCIES

Student progress is evaluated through both formative and summative assessment methods. Specific details may be found in the instructor's course information document.

COLLEGE POLICIES AND PROCEDURES

Student Handbook

https://www.kckcc.edu/files/docs/student-resources/student-handbook-and-code-of-conduct.pdf

College Catalog
https://www.kckcc.edu/academics/catalog/index.html

College Policies and Statements
https://www.kckcc.edu/about/policies-statements/index.html

Accessibility and Accommodations
https://www.kckcc.edu/academics/resources/student-accessibility-support-services/index.html.