Course Outline

2026-2027 Catalog

CSCI 18 - Ethical Hacking

Catalog Description

Transfer Status: CSU

Prerequisite: CSCI 17 or Security+ Certification, or department approval

Unit(s): 3.00

Lecture: 34.00 Contact hours/68.00 Out of class hours/102.00 Total hours/2.00 Unit(s)
Lab: 51.00 Contact hours/0.00 Out of class hours/51.00 Total hours/1.00 Unit(s)
Total: 85.00 Contact hours/68.00 Out of class hours/153.00 Total hours/3.00 Unit(s)

Course Description: This course introduces the network security specialist to the various methodologies for attacking a network. Students will be introduced to the concepts, principles, and techniques, supplemented by hands-on exercises, for attacking and disabling a network within the context of properly securing a network. The course will emphasize network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to a virtual environment. Students will experience a hands-on practical approach to penetration testing measures and ethical hacking. (C-ID ITIS 164).

Objectives

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

1. Describe the tools and methodology a "hacker" uses to break into a computer or network.
2. Defend a computer and a Local Area Network (LAN) against a variety of different types of security attacks using several hands-on techniques.
3. Describe the legal and ethical aspects of hacking networked systems.

Course Content

Topic Titles / Suggested Time Topic

Lecture

Topics	Lec Hrs
Ethics and Legal Aspects for Cybersecurity Professionals	1.00
Ethical Hacking Overview	1.00
Information Security Frameworks	1.00
Transmission Control Protocol/Internet Protocol (TCP/IP) Concepts Review	1.00
Network and Computer Attacks	2.00
Passive Intelligence Gathering: Footprinting and Social Engineering	1.00
Network Reconnaissance	2.00
Port Scanning	2.00
Enumeration	1.00
Fundamentals of Exploitation	2.00
Denial of Service	2.00
Session Hijacking	2.00
Evading Intrusion Detection Systems (IDS), Firewalls, and Honeypots	2.00
Vulnerability Analysis	2.00
Linux Operating System Vulnerabilities	2.00
Internet of Things (IoT) Vulnerabilities and Hacking	1.00
Hacking Web Servers	1.50
Hacking Wireless Networks	1.00
Covering Tracks	1.00
Cryptography Fundamentals	1.00
Protecting Networks with Security Devices	1.50
Cloud Computing	1.00
Programming/Scripting for Security Professionals	1.00
Embedded Operating Systems	1.00
Total Hours:	**34.00**

Lab

Topics	Lab Hrs
Ethics and Legal Aspects for Cybersecurity Professionals	2.00
Information Security Frameworks	1.00
Ethical Hacking Overview	1.00
Transmission Control Protocol/Internet Protocol (TCP/IP) Concepts Review	1.00
Network and Computer Attacks	2.00
Passive Intelligence Gathering: Footprinting and Social Engineering	2.00
Network Reconnaissance	3.00
Port Scanning	2.00
Fundamentals of Exploitation	1.00
Enumeration	3.00
Denial of Service	3.00
Session Hijacking	3.00
Evading Intrusion Detection Systems (IDS), Firewalls, and Honeypots	4.00
Vulnerability Analysis	3.00
Linux Operating System Vulnerabilities	2.00
Internet of Things (IoT) Vulnerabilities and Hacking	2.00
Hacking Web Servers	2.00
Hacking Wireless Networks	2.00
Covering Tracks	2.00
Cryptography Fundamentals	2.00
Protecting Networks with Security Devices	2.00
Cloud Computing	2.00
Programming/Scripting for Security Professionals	2.00
Embedded Operating Systems	2.00
Total Hours:	**51.00**

Methods of Instruction

A. Demonstrations
B. Homework: Students are required to complete two hours of outside-of-class homework for each hour of lecture
C. Lecture
D. Multimedia Presentations

Methods of Evaluation

A. Exams/Tests
B. Lab Projects
C. Written Assignments
D. Practical Evaluations

Examples of Assignments

Reading Assignments

1. Read the Input Validation Testing section of the Open Web Application Security Project (OWASP) Testing Framework posted on Canvas. Be prepared to discuss SQL injection testing in class.
2. Read the document about Equation Groups provided. Be prepared to discuss it in class.

Writing Assignments

1. Using the provided scenario and the SANS Institute guidelines, write a 2-3 page business Statement of Work and Authorization for Pen Testing agreement to conduct a grey-box penetration test on an organization. It must include preparation and planning, specifics on scope, detection, analysis and cleanup.
2. Read the Threat intelligence report: How Quantum Computing Will Change Browser Encryption by F5 Labs. Write a two-page essay on your findings. Using the provided scenario and the SANS Institute guidelines, write a 2-3 page business Statement of Work and Authorization for Pen Testing agreement to conduct a grey-box penetration test on an organization. It must include preparation and planning, specifics on scope, detection, analysis and cleanup.

Out-of-Class Assignments

1. Watch the Defcon video link and answer the questions provided.
2. Using your home network: Write an authorization for pentesting for yourself, use Kali Linux to run a pen test on your home computing environment and document your vulnerabilities and remedies professionally.

Recommended Materials of Instruction

Santos, O., Taylor, R. (2018). CompTIA PenTest+ Cert Guide. *Pearson, 1st.* 9780789760357.
Simpson, M., et al. (2023). Hands-On Ethical Hacking and Network Defense. *Cengage, 4th.* 9798214028262.
Harper, A., et al. (2022). Gray Hat Hacking: The Ethical Hacker's Handbook. *McGraw-Hill, 6th.* 9781264268948.

Minimum Qualifications

Computer Information Systems
Computer Science (Masters Required)
Computer Service Technology

Created/Revised by: Fischer, Linda
Date: 11/17/2025