Lassen Community College Course Outline

Course-CIS 71 Introduction to Cybersecurity: Ethical Hacking 3.0 Units

I. Catalog Description

Introduction to the principles and techniques associated with the cyber security red team penetration testing or ethical hacking. The course covers planning, scoping, reconnaissance, scanning, exploitation, post-exploitation, and result reporting documentation. The student discovers how system vulnerabilities can be exploited and how to implement and secure systems to avoid problems. This course prepares students for the globally recognized CompTIA PenTest+ Certification test. This course has been approved for online and hybrid delivery

Diversity Statement

Our commitment to diversity requires that we strive to eliminate barriers to equity and that we act deliberately to create a safe and inclusive environment where individual and group differences are valued and leveraged for the growth and understanding as an educational community.

Additional Course Information

Transfer Status:

NT

Total Number of Hours by Instructional Method:

51 Hours Lecture 102 Out of Class Hours, 153 Total Hours of Instruction

Scheduled:

- Every Fall

II. Coding Information

Repeatability: Not Repeatable

Grading Option:

Graded only

Credit Type:

Credit - Degree Applicable

TOP Code:

0708.0

III. Course Objectives

A. Course Student Learning Outcomes

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

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques
2. Analyze the tools and methods a "hacker" uses to break into a computer or network
3. Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.

B. Course Objectives

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

1. Describe the tools and methods a “hacker uses to break into a computer or network.
2. Describe the roles of security and penetration testers.
3. Describe the layers of the TCP/IP protocol stack and important ports.
4. Define types of malicious software.
5. Describe types of network attacks, and physical security.
6. Use Web tools for foot printing.
7. Describe various foot printing and social engineering methods.
8. Explain the types of port scans and describe how to use port-scanning tools.
9. Describe steps and tools for enumerating operating systems.
10. Describe various methods for hacking systems.
11. Explain Web application vulnerabilities.
12. Explain strategies for evading network protection systems
13. Explain encryption algorithms and public key infrastructure components
14. Describe webserver attack tools
15. Describe what ethical hackers can and cannot legally do.

IV. Course Content

A. Outline of Topics

1. Introduction to Penetration Testing Concepts
3. Planning and Scoping Penetration Tests
4. Conducting Passive Reconnaissance
5. Conducting Non-Technical Tests
6. Conducting Active Reconnaissance
7. Analyzing Vulnerabilities
8. Penetrating Networks
9. Exploiting Host-Based Vulnerabilities
10. Testing Applications
11. Completing Post-Exploit Tasks

1. Ethical hacking overview
2. TCP/IP concepts review
3. Network and computer attacks
4. Foot printing and social engineering
5. Port scanning 6. Enumeration
6. Programming for security professionals
7. Embedded operating system
8. Linux operating system vulnerabilities
9. Hacking web servers
10. Hacking wireless networks
11. Cryptography
12. Protecting networks with security devices

V. Assignments

A. Appropriate Readings

1. Various Industry articles and weekly/daily news from security journals.

B. 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.

C. Expected Outside Assignments

1. Students will be required to complete two hours of outside-of-class homework for each hour of lecture which will include hands on assignments practicing various hacking and penetration methods using virtual machines and cloud based networks.

D. Specific Assignments that Demonstrate Critical Thinking

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

VI. Methods of Evaluation

List general evaluation methods (i.e., mixed format exams, participation, written essays, oral and listening exams)

Only include the appropriate evaluation modalities

Traditional Evaluation

Term paper (topic choice, thesis statement, outline, bibliography, rough draft, final draft), homework, classroom discussion, essay, journals, lab demonstrations and activities, multiple choice quizzes, and participation.

Hybrid Evaluation

Quizzes and exams could be administered in person and/ or online. Students will be expected to complete online assignments and activities equivalent to in class assignments and activities for the online portion of the course. Electronic communication, both synchronous and asynchronous (chat/forum) will be evaluated for participation and to maintain effective communication between instructor and students.

Online Evaluation

A variety of methods will be used, such as: research papers, asynchronous and synchronous (chat/forum) discussions, online quizzes and exams, posting to online website and email communications using the districts approved learning management system.

VII. Methods of Delivery

Check those delivery methods for which this course has been separately approved by the Curriculum/Academic Standards Committee.

X Traditional Classroom Delivery
☐ Correspondence Delivery
X Hybrid Delivery
X Online Delivery

Only include the appropriate delivery modalities

Traditional Classroom Delivery

Lecture, discussion, audio/visual aids, demonstration, group exercises, guest speakers, lab, individualized programs and other as needed.

Hybrid Delivery

A combination of traditional classroom and online instruction will be utilized. Each semester a minimum of 17 hours, or 1/3 of the instruction hours, will be taught face-to face by the instructor and the remaining hours will be instructed online through the technology platform adopted by the District. Traditional class instruction could consist of exercises/assignments, lectures, visual aids, practice exercises, exams and quizzes. Online delivery could consist of exercises/assignments, lecture posts, discussions, exams and quizzes, adding extra resources and other media sources as appropriate.

Online Delivery

A variety of methods will be used, such as: research papers, asynchronous and synchronous (chat/forum) discussions, online quizzes and exams, posting to

online website and email communications using the districts approved learning management system.

VIII. Representative Texts and Supplies

Cisco Network Academy Netacad learning management system. (www.netacad.com)

Santos, O., Taylor, R. (2018). CompTIA PenTest+ Cert Guide. *Pearson IT Certification, 1st*.

IX. Course Status

1. Current Status: Active
2. Original Approval Date: 10/18/22
3. Course Originator: Melinda Duerksen
4. Board Approval Date:
5. Chancellor's Office Approval Date: 12/07/2022
6. Revised By: Melinda Duerksen
7. Curriculum/Academic Standards Committee Revision Date: 09/03/2024