Lassen Community College Course Outline

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.

Prerequisites:

Transfer Status: Not Transferrable
Number of total hours by instructional method. 51 hours lecture,102 hours out-of-class, 153 Total hours
Scheduled: Fall
CID ITIS 164

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 footprinting.
7. Describe various footprinting 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 web server attack tools.
15. Describe what ethical hackers can and cannot legally do.

IV. Course Content

A. Outline of Topics

1. Ethical hacking overview
2. TCP/IP concepts review
3. Network and computer attacks
4. Footprinting 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

Various Industry Articles and Reports

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.
3. 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

C. Expected Outside Assignments

Students will be required to complete two hours of outside-of-class homework for each hour of lecture.

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

D. Specific Assignments that Demonstrate Critical Thinking

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.

VI. Methods of Evaluation

1. Exams/Tests
2. Lab Projects
3. Written Assignments
4. Mid-term and final examinations

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 ☐ Web-enhance course

☐ Correspondence Delivery ☐ Hybrid Delivery ☐ **X** Online Delivery

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. Discipline/s Assignment

Computer Information Systems

X. Course Status

Current Status: Active
Original Approval Date: 10/18/2022
Course Originator: Melinda Duerksen
Board Approval Date:11/08/2022
Chancellor's Office Approval Date: 12/7/2022
Revised By:
Curriculum/Academic Standards Committee Revision Date: