GAVILAN COLLEGE
5055 Santa Teresa Blvd
Gilroy, CA 95023

Course Outline

COURSE: CSIS 186 DIVISION: 50 ALSO LISTED AS:

TERM EFFECTIVE: Spring 2022 CURRICULUM APPROVAL DATE: 05/11/2021

SHORT TITLE: CYBERSEC: ETHICAL HACKING

LONG TITLE: Cybersecurity: Ethical Hacking

Units	Number of Weeks	Type	Contact Hours/Week	Total Contact Hours
3	18	Lecture:	3	54
		Lab:	0	0
		Other:	0	0
		Total:	3	54
		Total Learning Hrs:	162	

COURSE DESCRIPTION:

This course emphasizes network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Topics will be presented in the context of legal restrictions and ethical guidelines. This course along with CSIS 179, 184, and 187; prepares students to take the professional industry option of a letter grade or pass/no pass. ADVISORY: CSIS 179.

PREREQUISITES:

COREQUISITES:

CREDIT STATUS: D - Credit - Degree Applicable

GRADING MODES
- L - Standard Letter Grade
- P - Pass/No Pass

REPEATABILITY: N - Course may not be repeated

SCHEDULE TYPES:
- 02 - Lecture and/or discussion
- 05 - Hybrid
- 71 - Dist. Ed Internet Simultaneous
- 72 - Dist. Ed Internet Delayed

STUDENT LEARNING OUTCOMES:

By the end of this course, a student should:

1. Describe the tools and methods a hacker uses to break into a computer network.

2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

3. Practice and utilize safe techniques on the World Wide Web.

CONTENT, STUDENT PERFORMANCE OBJECTIVES, OUT-OF-CLASS ASSIGNMENTS

Curriculum Approval Date: 05/11/2021

4 Hours

Content: Ethical Hacking Overview

Student Performance Objectives: Describe the role of an ethical hacker. Describe what you can do legally as an ethical hacker. Describe what you can't do as an ethical hacker.

4 Hours

Content: TCP/IP Concepts Review

Student Performance Objectives: Explain the TCP/IP protocol stack. Explain the basic concepts of IP addressing. Explain the binary, octal, and hexadecimal numbering systems.

4 Hours

Content: Network and Computer Attacks

Student Performance Objectives: Describe the different types of malicious software and what damage they can do. Describe the methods of protecting against malware attacks. Describe the types of network attacks. Identify physical security attacks and vulnerabilities.

4 Hours

Content: Footprinting and Social Engineering

Student Performance Objectives: Use Web tools for footprinting. Conduct competitive intelligence. Describe DNS zone transfers. Identify the types of social engineering.

4 Hours

Content: Port Scanning

Student Performance Objectives: Describe port scanning and types of port scans. Describe port-scanning tools. Explain what ping sweeps are used for. Explain how shell scripting is used to automate security tasks.

4 Hours

Content: Enumeration

Student Performance Objectives: Describe the enumeration step of security testing. Enumerate Windows OS targets, NetWare OS targets, and *nix OS targets.

4 Hours

Content: Programming for Security Professionals

Student Performance Objectives: Explain basic programming concepts. Write a simple C program. Explain how Web pages are created with HTML. Describe and create basic Perl programs. Explain basic object-oriented programming concepts.

4 Hours

Content: Linux Operating System Vulnerabilities

Student Performance Objectives: Describe vulnerabilities of the Windows and Linux operating systems. Identify specific vulnerabilities and explain ways to fix them. Explain techniques to harden systems against Windows and Linux vulnerabilities.

4 Hours

Content: Embedded Operating Systems

Student Performance Objectives: Explain what embedded operating systems are and where they're used. Describe Windows and other embedded operating systems. Identify vulnerabilities of embedded operating systems and best practices for protecting them.

4 Hours

Content: Hacking Web Servers

Student Performance Objectives: Describe Web applications. Explain Web application vulnerabilities. Describe the tools used to attack Web servers.

4 Hours

Content: Hacking Wireless Networks

Student Performance Objectives: Explain wireless technology. Describe wireless networking standards. Describe the process of authentication. Describe wardriving. Describe wireless hacking and tools used by hackers and security professionals.

4 Hours

Content: Cryptography

Student Performance Objectives: Summarize the history and principles of cryptography. Describe symmetric and asymmetric encryption algorithms. Explain public key infrastructure (PKI). Describe possible attacks on cryptosystems.

4 Hours

Content: Protecting Networks with Security Devices

Student Performance Objectives: Explain how routers are used as network protection systems. Describe firewall technology and tools for configuring firewalls and routers. Describe intrusion detection and prevention systems and Web-filtering technology. Explain the purpose of honeypots.

2 Hours

Final

METHODS OF INSTRUCTION:

Lecture, Computer Demonstrations, Projects, Presentations

OUT OF CLASS ASSIGNMENTS:

Required Outside Hours: 54

Assignment Description:

Homework: Complete hands-on presentations, projects, case studies, and/or problem solving assignments.

Examples: (1) Use the Telnet command to access port 25 on your mail server, log on, and send an e-mail message to a recipient. (2) Determine Web server information by using HTTP methods. (3) Demonstrate how to create, save, and run an executable script. (4) Demonstrate how to use Windows network mapping and enumeration tools. (5) Use OpenVAS to discover vulnerabilities on a Linux computer. (6) Use ASP to create dynamic Web pages and be able to recognize ASP Web pages. (7) Investigate what attackers can do with the results of an MD5 collision. (8) Examine and demonstrate how to use a network-based IDS. (9) After conducting a thorough security test on the Alexander Rocco network, you have identified several intrusion attempts from sources over the Internet. The hackers haven't gained access to the internal network yet, but you're concerned that it's only a matter of time before the attempts become successful. Based on this information, write a one-page report describing what can be done to attract intruders and keep them connected to the network long enough to trace them. The report should discuss the pros and cons of using this strategy and mention any legal issues the company might face.

Required Outside Hours: 27

Assignment Description:

Read textbook and answer end of chapter/section review questions.

Required Outside Hours: 27

Assignment Description:

Review chapters and study for exams.

METHODS OF EVALUATION:

Problem-solving assignments

Percent of total grade: 40.00 %

Percent range of total grade: 25% to 40% Homework, Presentation, Project, Case Study

Skill demonstrations

Percent of total grade: 40.00 %

Percent range of total grade: 30% to 50% Hands-On Exercises

Objective examinations

Percent of total grade: 20.00 %

Percent range of total grade: 20% to 30% Multiple Choice, True/False, Matching Items, Completion

REPRESENTATIVE TEXTBOOKS:

Simpson, Michael T. and Antill, Nicholas. Hands-On Ethical Hacking and Network Defense, 4th Edition. Boston, MA: Cengage Learning,2022.

ISBN: 978-0-357-50975-3

Reading Level of Text, Grade: 12th + Verified by: MS Word

ARTICULATION and CERTIFICATE INFORMATION

Associate Degree:
CSU GE:
IGETC:
CSU TRANSFER:
Transferable CSU, effective 202230
UC TRANSFER:
Not Transferable

SUPPLEMENTAL DATA:

Basic Skills: N
Classification: Y
Noncredit Category: Y
Cooperative Education: N
Program Status: 1 Program Applicable
Special Class Status: N
CAN:
CAN Sequence:
CSU Crosswalk Course Department:
CSU Crosswalk Course Number:
Prior to College Level: Y
Non Credit Enhanced Funding: N
Funding Agency Code: Y
In-Service: N
Occupational Course: C
Maximum Hours:
Minimum Hours:
Course Control Number: CCC000624734
Sports/Physical Education Course: N
Taxonomy of Program: 070810