CS/IS193 : Introduction to Cybersecurity: Ethical Hacking

General Information

Author:	• Vladimir Paransky
Course Code (CB01) :	CS/IS193
Course Title (CB02) :	Introduction to Cybersecurity: Ethical Hacking
Department:	CSIS
Proposal Start:	Fall 2024
TOP Code (CB03) :	(0708.00) Computer Infrastructure and Support
CIP Code:	(11.1003) Computer and Information Systems Security/Auditing/Information Assurance.
SAM Code (CB09) :	Possibly Occupational
Distance Education Approved:	No
Will this course be taught asynchronously?:	No
Course Control Number (CB00) :	CCC000571266
Curriculum Committee Approval Date:	10/25/2023
Board of Trustees Approval Date:	12/19/2023
Last Cyclical Review Date:	10/25/2023
Course Description and Course Note:	CS/IS 193 introduces students 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 emphasizes network attack methods with an emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students experience a hands-on practical approach to penetration testing measures and ethical hacking. This course includes labs to provide hands-on training.
Justification:	Mandatory Revision
Academic Career:	• Credit

Academic Senate Discipline

Primary Discipline:	• Computer Information Systems (Computer network installation, microcomputer technology, computer applications)
Alternate Discipline:	No value
Alternate Discipline:	No value

Course Development

Basic Skill Status (CB08)

Course is not a basic skills course.

Course Special Class Status (CB13)

Course is not a special class.

Grading Basis

- Grade with Pass / No-Pass Option

Pre-Collegiate Level (CB21)

Course Support Course Status (CB26)

☐ Allow Students to Gain Credit by Exam/Challenge	Not applicable.	Course is not a support course

Transferability & Gen. Ed. Options

General Education Status (CB25)

Not Applicable

Transferability

Transferable to CSU only

Transferability Status

Approved

C-ID	Area	Status	Approval Date	Comparable Course
ITIS	Information Technology and Information Systems	Approved	02/16/2016	ITIS 164 - Introduction to Cybersecurity: Ethical Hacking

Units and Hours

Summary

Minimum Credit Units (CB07)	3
Maximum Credit Units (CB06)	3
Total Course In-Class (Contact) Hours	90
Total Course Out-of-Class Hours	72
Total Student Learning Hours	162

Credit / Non-Credit Options

Course Type (CB04)

Credit - Degree Applicable

Noncredit Course Category (CB22)

Credit Course.

Noncredit Special Characteristics

No Value

Course Classification Code (CB11)

Credit Course.

Funding Agency Category (CB23)

Not Applicable.

☐ Cooperative Work Experience Education Status (CB10)

☐ Variable Credit Course

Weekly Student Hours

	In Class	Out of Class
Lecture Hours	2	4
Laboratory Hours	3	0

Course Student Hours

Course Duration (Weeks)	18
Hours per unit divisor	0
Course In-Class (Contact) Hours	
Lecture	36

Studio Hours	0	0	Laboratory	54
			Studio	0
			Total	90
			Course Out-of-Class Hours	
			Lecture	72
			Laboratory	0
			Studio	0
			Total	72

Time Commitment Notes for Students

No value

Pre-requisites, Co-requisites, Anti-requisites and Advisories

Advisory

CS/IS190 - Introduction to Computer Networks (in-development)

Objectives

- Use network testing tools to identify and correct common network issues.

AND

Advisory

CS/IS196 - Advanced Networking: Security (in-development)

Objectives

- Design and administer an organization's security policy.
- Use encryption methods to safeguard information.
- Test, evaluate, and implement network security.

Entry Standards

Entry Standards

No value

Specifications

Methods of Instruction

Methods of Instruction	Lecture

Methods of Instruction	Laboratory

Methods of Instruction	Discussion
Methods of Instruction	Multimedia
Methods of Instruction	Tutorial
Methods of Instruction	Collaborative Learning
Methods of Instruction	Demonstrations
Methods of Instruction	Guest Speakers
Methods of Instruction	Presentations

Out of Class Assignments

- Hands-on projects (e.g. hardening computer and server security)
- Problem solving assignment such as hackthissite.org - realistic missions

Methods of Evaluation	Rationale
Exam/Quiz/Test	Final Examination
Exam/Quiz/Test	Quizze(s)
Project/Portfolio	NetLab+ Projects
Project/Portfolio	Final Project(s)

Textbook Rationale

No Value

Textbooks

Author	Title	Publisher	Date	ISBN
Allen Harper	Gray Hat Hacking: The Ethical Hacker's Handbook	McGrawHill Education	2022	978-1-264-26894-8

Other Instructional Materials (i.e. OER, handouts)

No Value

Materials Fee

No value

Learning Outcomes and Objectives

Course Objectives

Describe ethical hacking and appropriate uses of hacking.

Defend a computer and a Local Area Network (LAN) against a variety of security attacks.

Determine security vulnerabilities of computer, server, network and embedded systems.

Protect computer-based networks with security devices.

Use of software tools to start or stop an exploratory attack.

SLOs

Explain the tools and methods a hacker uses to break into a computer or network. Expected Outcome Performance: 70.0

ILOs Core ILOs	Analyze and solve problems using critical, logical, and creative thinking; ask questions, pursue a line of inquiry, and derive conclusions; cultivate creativity that leads to innovative ideas.
	Communicate clearly, ethically, and creatively; listen actively and engage respectfully with others; consider situational, cultural, and personal contexts within or across multiple modes of communication.
CSIS Information Technology - A.S. Degree Major	Demonstrate an understanding of ethical concern associated with information technology including access, reliability, legal, ethical, and accuracy; identify types of computer crime; select, access, and use appropriate sources.
	Demonstrate installing, configuring, and maintaining computer and mobile devices, including diagnosing, resolving, and documenting common hardware and software.
	Demonstrate the proper server operation procedures, maintenance procedures and managing risks associated with real world networks.
CSIS Information Technology Certificate	Demonstrate an understanding of ethical concern associated with information technology including access, reliability, legal, ethical, and accuracy; identity types of computer crime; select, access, and use appropriate sources.
	Demonstrate installing, configuring and maintaining computer and mobile devices, including diagnosing, resolving and documenting common hardware and software.
	Demonstrate the proper server operation procedures, maintenance procedures and managing risk associated with real world networks.
CSIS Computer Science - A.S. Degree Major	Prepare a software project to implement a single scientific, mathematical, business, or technical function.

CSIS Computer Science - Certificate	Prepare a software project to implement a single scientific, mathematical, business, or technical function.
CSIS Computer Information Systems	analyze simple business or technical problems relevant to programming, and prepare solutions to them
	demonstrate an understanding of the operations and processes of a computer relevant to programming.
CSIS Computer Software Technician	demonstrate the ability to independently create, save, modify and print a document using a word processing program and appropriate assistive technology
CSIS Web Development - A.S. Degree Major	use industry standard tools and techniques to produce, publish and maintain Web sites and Web content.
CSIS Web Development - Certificate	use industry standard tools and techniques to produce, publish and maintain Web sites and Web content.

Discuss, explain, and demonstrate safe techniques on the World Wide Web. Expected Outcome Performance: 70.0

ILOs Core ILOs	Analyze and solve problems using critical, logical, and creative thinking; ask questions, pursue a line of inquiry, and derive conclusions; cultivate creativity that leads to innovative ideas.
	Communicate clearly, ethically, and creatively; listen actively and engage respectfully with others; consider situational, cultural, and personal contexts within or across multiple modes of communication.
	Demonstrate depth of knowledge in a course, discipline, or vocation by applying practical knowledge, skills, abilities, theories, or methodologies to solve unique problems.
CSIS Information Technology - A.S. Degree Major	Demonstrate an understanding of ethical concern associated with information technology including access, reliability, legal, ethical, and accuracy; identify types of computer crime; select, access, and use appropriate sources.
	Demonstrate installing, configuring, and maintaining computer and mobile devices, including diagnosing, resolving, and documenting common hardware and software.
	Demonstrate the proper server operation procedures, maintenance procedures and managing risks associated with real world networks.
CSIS Information Technology Certificate	Demonstrate an understanding of ethical concern associated with information technology including access, reliability, legal, ethical, and accuracy; identity types of computer crime; select, access, and use appropriate sources.
	Demonstrate installing, configuring and maintaining computer and mobile devices, including diagnosing, resolving and documenting common hardware and software.
	Demonstrate the proper server operation procedures, maintenance procedures and managing risk associated with real world networks.
CSIS Computer Science - A.S. Degree Major	Prepare a software project to implement a single scientific, mathematical, business, or technical function.
CSIS Computer Science - Certificate	Prepare a software project to implement a single scientific, mathematical, business, or technical function.
CSIS Computer Information Systems	analyze simple business or technical problems relevant to programming, and prepare solutions to them
	demonstrate an understanding of the operations and processes of a computer relevant to programming.
CSIS Computer Software Technician	demonstrate the ability to independently create, save, modify and print a document using a word processing program and appropriate assistive technology
CSIS Web Development - Certificate	use industry standard tools and techniques to produce, publish and maintain Web sites and Web content.

CSIS Web Development - A.S. Degree Major	use industry standard tools and techniques to produce, publish and maintain Web sites and Web content.

Apply knowledge of networking and security to lunch a penetration attack to test network security. Expected Outcome Performance: 70.0

ILOs Core ILOs	Analyze and solve problems using critical, logical, and creative thinking; ask questions, pursue a line of inquiry, and derive conclusions; cultivate creativity that leads to innovative ideas.
	Demonstrate depth of knowledge in a course, discipline, or vocation by applying practical knowledge, skills, abilities, theories, or methodologies to solve unique problems.

Additional SLO Information

Does this proposal include revisions that might improve student attainment of course learning outcomes?

No

Is this proposal submitted in response to learning outcomes assessment data?

No

If yes was selected in either of the above questions for learning outcomes, explain and attach evidence of discussions about learning outcomes.

No Value

SLO Evidence

No Value

Course Content

Lecture Content

Ethical Hacking Overview (3 hours)
- Getting Started
- Soft Skills
- Stay Legal

Transmission Control Protocol/Internet Protocol (TCP/IP) (3 hours)
- Concepts Review
- Application layer
- Transport layer
- Network layer
- Data link layer

Network and Computer Attacks (4 hours)
- Eavesdropping
- Data Modification
- IP Address Spoofing Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack
- Application-Layer Attack

Footprinting and Social Engineering (4 hours)
- Information-gathering methodology
- Competitive intelligence
- Whois and American Registry for Internet Numbers (ARIN) lookup
- Types of Domain Name System (DNS) records

- Email tracking
- Web spiders
- Dumpster diving
- Reverse social engineering

Port Scanning (2 hours)
Enumeration (2 hours)
- Methods to retrieve usernames and info on groups, shares, and services of networked computers (using Nmap and Nessus).

Programming for Security Professionals (2 hours)
Embedded Operating Systems (2 hours)
- Operating systems for digital watches, MP3 players, traffic lights and hybrid vehicles

Linux Operating System Vulnerabilities (2 hours)
- Stack Operations
- Buffer Overflows
- Exploit Development process

Hacking Web Servers (4 hours)
Hacking Wireless Networks (4 hours)
Cryptography (2 hours)
- Symmetric-key
- Public-key
- Cryptanalysis
- PrimitivesCryptosystems

Protecting Networks with Security Devices (2 hours)
- Create a Wireless Security Policy
- Secure the Wireless Local Area Network (WLAN)
- Protect Your Wired Network from Wireless Threats
- Protect Your Company from Outside Threats
- Get Employees Involved

Total Hours: 36

Laboratory/Studio Content

Ethical Hacking Overview (3 hours)
- Getting Started
- Soft Skills
- Stay Legal

Network and Computer Attacks (6 hours)
- Eavesdropping
- Data Modification
- IP Address Spoofing Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Compromised-Key Attack
- Sniffer Attack
- Application-Layer Attack

Footprinting and Social Engineering (6 hours)
- Information-gathering methodology
- Competitive intelligence
- Whois and American Registry for Internet Numbers (ARIN) lookup
- Types of Domain Name System (DNS) records
- Email tracking
- Web spiders
- Dumpster diving
- Reverse social engineering

Port Scanning (6 hours)

Enumeration (6 hours)
- Methods to retrieve usernames and info on groups, shares, and services of networked computers (using Nmap and Nessus).

Linux Operating System Vulnerabilities (6 hours)
- Stack Operations
- Buffer Overflows

- Exploit Development process

Hacking Web Servers (6 hours)
Hacking Wireless Networks (6 hours)
Cryptography (3 hours)

- Symmetric-key
- Public-key
- Cryptanalysis
- PrimitivesCryptosystems

Protecting Networks with Security Devices (6 hours)

- Create a Wireless Security Policy
- Secure the Wireless Local Area Network (WLAN)
- Protect Your Wired Network from Wireless Threats
- Protect Your Company from Outside Threats
- Get Employees Involved

Total Hours: 54