Cerro Coso College

Course Outline of Record Report

10/12/2021

CSCIC190 : Introduction to Cybersecurity: Ethical Hacking

General Information

Author:	-
Course Code (CB01) :	CSCIC190
Course Title (CB02) :	Introduction to Cybersecurity: Ethical Hacking
Department:	Business Information Technolog
Proposal Start:	Fall 2013
TOP Code (CB03) :	(0708.10) Computer Networking
SAM Code (CB09) :	Clearly Occupational
Distance Education Approved:	Yes
Course Control Number (CB00) :	CCC000574155
Curriculum Committee Approval Date:	04/01/2016
Board of Trustees Approval Date:	05/05/2016
External Review Approval Date:	06/10/2016
Course Description:	This course introduces the network security specialist to the various methodologies for attacking a network. Students are 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 emphasizes network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students receive course content information through a variety of methods: lecture and demonstration of hacking tools are used in addition to a virtual environment. Students experience a hands-on practical approach to penetration testing measures and ethical hacking.
Submission Type:	New Course
Author:	No value

Faculty Minimum Qualifications

Master Discipline Preferred:	• Computer Science • Engineering Technology
Alternate Master Discipline Preferred:	No value
Bachelors or Associates Discipline Preferred:	• Computer Information Systems (Computer network installation, microcomputer technology, computer applications)
Additional Bachelors or Associates Discipline Preferred:	No value

Course Development Options

Basic Skills Status (CB08)

Course is not a basic skills course.

Course Special Class Status (CB13)

Course is not a special class.

Grade Options

- Letter Grade Methods

□ Allow Students to Gain Credit by Exam/Challenge

Rationale For Credit By Exam/Challenge

No value

Course Support Course Status (CB26)

No value

Allowed Number of Retakes

0

Retake Policy Description

Type:|Non-Repeatable Credit

Course Prior To College Level (CB21)

Not applicable.

☑ Allow Students To Audit Course

Associated Programs

☑ Course is part of a program (CB24)

Associated Program	Award Type	Active
Cyber Security Technology	A.S. Degree Major	Spring 2018
Cyber Security Technician	Certificate of Achievement	Spring 2018

Transferability & Gen. Ed. Options

Course General Education Status (CB25)

No value

Transferability

Transferable to CSU only

Transferability Status

Approved

Units and Hours:

Summary

Minimum Credit Units (CB07)	3
Maximum Credit Units (CB06)	3
Total Course In-Class (Contact) Hours	72
Total Course Out-of-Class Hours	90
Total Student Learning Hours	162
Faculty Load	0

Credit / Non-Credit Options

Course Credit Status (CB04)

Credit - Degree Applicable

Course Non Credit Category (CB22)

Credit Course.

Non-Credit Characteristic

No Value

Course Classification Status (CB11)

Credit Course.

□ Variable Credit Course

Funding Agency Category (CB23)

Not Applicable.

□ Cooperative Work Experience Education Status (CB10)

Weekly Student Hours

	In Class	Out of Classs
Lecture Hours	2.5	5
Laboratory Hours	1.5	0
Activity Hours	0	0

Course Student Hours

Course Duration (Weeks)	18
Hours per unit divisor	0
Course In-Class (Contact) Hours	
Lecture	0
Laboratory	0
Activity	0
Total	72
Course Out-of-Class Hours	
Lecture	0
Laboratory	0
Activity	0
Total	90

Time Commitment Notes for Students

No value

Faculty Load

Extra Duties: 0

Faculty Load: 0

Units and Hours: - Weekly Specialty Hours

Activity Name	Type	In Class	Out of Class
No Value	No Value	No Value	No Value

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

Prerequisite

CSCIC146 - Introduction to Information Systems Security

Students need an understanding of network security and risk management including processes, communications and the application of policies and procedures for securing computers and networks. This material is covered in the CSCI C146 course.

AND

Advisory

CSCIC143 - Computer Network Fundamentals

Students need a basic understanding of networking terminology, network structure to transfer that knowledge to network security. This material is covered in the CSCI C143 course.

AND

Advisory

CSCIC101 - Introduction to Computer Information Systems

Students need to be able to identify hardware components of a computer system, understand the basics of operating systems and application software, install software, understand what memory is, how to zip and unzip files, how to save and find files and understand the basics of network topology. This material is covered in the CSCI C101 course.

Entrance Skills

Entrance Skills	Description
No value	No value

Limitations on Enrollment

Limitations on Enrollment	Description
No value	No value

Specifications

Methods of Instruction

Methods of Instruction	Outside reading
Rationale	Textbook and Electronic Readings
Methods of Instruction	Audiovisual
Rationale	Pre-recorded Training Videos
Methods of Instruction	Skills Development and Performance
Rationale	No value
Methods of Instruction	Project-based learning
Rationale	No value
Methods of Instruction	Instruction through examination or quizzing
Rationale	No value
Methods of Instruction	Laboratory
Rationale	No value
Methods of Instruction	Lecture
Rationale	No value
Methods of Instruction	Guest Lecturers
Rationale	No value
Methods of Instruction	Discussion
Rationale	No value
Methods of Instruction	Demonstration
Rationale	No value
Methods of Instruction	Discussion

Rationale	Discussions

Methods of Instruction	Other
Rationale	Simulation Scenarios. Lab Based Scenarios.

Assignments

A. Chapter reading (Example: Reading the assigned chapters from the textbook based on the topics for the week).
B. Research and analysis projects (Example: Analyze a real world scenario and develop a plan for conducting a penetration test on the target systems).
C. Weekly step-by-step security tool assignments (Example: Follow instructions to evaluate computer system vulnerabilities using a vulnerability scanner and document findings).
D. Simulation and lab assignments (Example: Use industry standard utilities to identify and exploit weaknesses in target systems. Demonstrate an ability to then mitigate the discovered risks).

Methods of Evaluation	Rationale
Final Exam	Comprehensive Exam: A comprehensive exam will evaluate the student's preparedness for the Certified Ethical Hacker (CEH) certification exam.
Participation	In class discussions. These discussions will introduce students to concepts associated with ethical hacking and provide elaboration on topics from the text. For example, discussing what actions that must be taken to ensure that the security professio
Tests	Objective Exams. These exams will evaluate the student's comprehension of text material and prepare them for the Certified Ethical Hacker (CEH) certification exam.
Project	Hands-on projects. These projects will require the use of industry standard utilities for a wide array of activities such as fingerprinting a remote system and then exploiting identified weaknesses in the system to gain access.

Equipment

No Value

Textbooks

Author	Title	Publisher	Date	ISBN
	Simpson, M. T., Backman, K. & Corley, J. . (2012) Hands-On Ethical Hacking and Network Defense, 2, Cengage			

Other Instructional Materials

No Value

Materials Fee

No

Learning Outcomes and Objectives

Course Objectives

No value

CSLOs

Describe and categorize the tools and methods a "hacker" uses to break into a computer or network.

Expected SLO Performance: 70.0

Defend a computer and a Local Area Network (LAN) against a variety of different types of security attacks using a number of hands-on techniques.

Expected SLO Performance: 70.0

Evaluate and demonstrate safe techniques on the world wide web.

Expected SLO Performance: 70.0

Outline

Course Outline

1) Ethical Hacking Overview
a) Threats and Vulnerabilities
b) Network and Computer Attacks
c) Approaches to Ethical Hacking
2) Transmission Control Protocol/Internet Protocol (TCP/IP)Concepts Review
3) Footprinting
a) Footprinting Overview
b) Footprinting Tools
c) Public Footprinting Utilities
4) Social Engineering
5) Port Scanning
a) Scanning Overview
b) Scanning Tools
6) Enumeration
a) Enumeration Overview
b) Enumeration Tools and Techniques
7) Programming for Security Professionals
8) Embedded Operating Systems
9) Linux Operating System Vulnerabilities
10) System Hacking
a) Password Attacks and Countermeasures
b) Privilege Escalation
c) Keylogging
d) Spyware
e) Rootkits
11) Hacking Web Servers
12) Hacking Wireless Networks
13) Avoiding Detection
a) Audit and Event Log
b) Steganography
14) Cryptography
15) Protecting Networks with Security Devices

Lab Outline

Infiltrating wireless networksDiscovering targets on a networkExploiting common operating systemsExposing common results of poor security practices using a browser.

Delivery Methods and Distance Education

Delivery Method: Please list all that apply -Face to face -Online (purely online no face-to-face contact) -Online with some required face-to-face meetings (“Hybrid”) -Online course with on ground testing -iTV – Interactive video = Face to face course with significant required activities in a distance modality -Other

Face 2 Face
Online
Hybrid

Rigor Statement: Assignments and evaluations should be of the same rigor as those used in the on-ground course. If they are not the same as those noted in the COR on the Methods of Evaluation and out-of-class assignments pages, indicate what the differences are and why they are being used. For instance, if labs, field trips, or site visits are required in the face to face section of this course, how will these requirements be met with the same rigor in the Distance Education section?

All assignments in distance education courses (online, hybrid and iTV) of CSCI C190 are of the same rigor as those in the on-ground course, except that students in purely online sections will submit all of their assignments virtually. Use of industry stan

Effective Student-Instructor Contact: Good practice requires both asynchronous and synchronous contact for effective contact. List the methods expected of all instructors teaching the course. -Learning Management System -Discussion Forums -Moodle Message -Other Contact -Chat/Instant Messaging -E-mail -Face-to-face meeting(s) -Newsgroup/Discussion Board -Proctored Exam -Telephone -iTV - Interactive Video -Other (specify)

contact_moodle_forums
contact_email
contact_face2face
contact_discussion
contact_itv

Software and Equipment: What additional software or hardware, if any, is required for this course purely because of its delivery mode? How is technical support to be provided?

A 3 node server cluster running VMWare ESXi or Hyper-V which can be used to host virtual environments. Network equipment to establish a private network to provide connectivity to the class servers. Modern workstations with wired and wireless network car

Accessibility: Section 508 of the Rehabilitation Act requires access to the Federal government's electronic and information technology. The law covers all types of electronic and information technology in the Federal sector and is not limited to assistive technologies used by people with disabilities. It applies to all Federal agencies when they develop, procure, maintain, or use such technology. Federal agencies must ensure that this technology is accessible to employees and the public to the extent it does not pose an "undue burden". I am using -iTV—Interactive Video only -Learning management system -Publisher course with learning management system interface.

s508_itv
s508_moodle
s508_publisher

Class Size: Good practice is that section size should be no greater in distance ed modes than in regular face-to-face versions of the course. Will the recommended section size be lower than in on-ground sections? If so, explain why.

No Value