CIS 064: INTRO TO ETHICAL HACKING

Originator

fmarhuenda

Co-Contributor(s)

Name(s)
Flores, Martin

Justification / Rationale

Exchange one lecture unit for one lab unit. The contact hours are simply not enough to deliver the content. We taught this course for the first time this past academic year.
It's part of the process of improvement.

Effective Term

Spring 2023

Credit Status

Credit - Degree Applicable

Subject

CIS - Computer Information Systems

Course Number

064

Full Course Title

Intro to Ethical Hacking

Short Title

ETHICAL HACKING

Discipline

Disciplines List
Computer Information Systems (Computer network installation, microcomputer technology, computer applications)

Modality

Face-to-Face
100% Online
Hybrid

Catalog Description

This course introduces the network security specialist working in a red team environment to the various methodologies for attacking a network and gaining access to networks, applications, databases, and other critical data on a secured system. Students will be introduced to the concepts, principles, and the latest hacking techniques, supplemented by hands-on exercises, for attacking and disabling a network within the context of properly securing a network, along with the most advanced hacking tools and exploits, the appropriate defenses, and countermeasures. Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to a virtual environment. Students will experience a hands-on practical approach to penetration testing measures and ethical hacking.

Schedule Description

This course introduces the network security specialist to the various methodologies for attacking a network, various attack vectors, and preventative measures. It will teach the students how a hacker thinks and acts so that they will be better positioned to set up their security infrastructure and defend against future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident. The students will have a hands-on environment and systematic process across every ethical hacking domain and methodology, giving the student the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker.

Prerequisite: CIS 060 or equivalent

Lecture Units
2
Lecture Semester Hours
36

Lab Units
1
Lab Semester Hours
54

In-class Hours
90

Out-of-class Hours
72

Total Course Units
3
Total Semester Hours
162

Prerequisite Course(s)
CIS 060 or equivalent

Required Text and Other Instructional Materials

Resource Type
Web/Other
Open Educational Resource
No

Year
2021

Description
TestOut Ethical Hacker Pro
https://w3.testout.com/courses/ethical-hacker-pro

Class Size Maximum
35

Entrance Skills
Information Systems Security.

Requisite Course Objectives
CIS 060-Describe the fundamental principles of information systems security.

Entrance Skills
Malware and Social Engineering Attacks.

Requisite Course Objectives
CIS 060-Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.

Entrance Skills
Application and Network Attacks.

Requisite Course Objectives

CIS 060-Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
CIS 060-Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/ controls.

Entrance Skills

Vulnerability Assessment and Mitigating Attacks.

Requisite Course Objectives

CIS 060-Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
CIS 060-Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/ controls.

Entrance Skills

Host, Application, and Data Security.

Requisite Course Objectives

CIS 060-Determine appropriate strategies to assure confidentiality, integrity, and availability of information.

Entrance Skills

Network Security and its administration

Requisite Course Objectives

CIS 060-Create and maintain a comprehensive security model.
CIS 060-Design and guide the development of an organization’s security policy.

Entrance Skills

Wireless Network Security.

Requisite Course Objectives

CIS 060-Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
CIS 060-Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/ controls.

Entrance Skills

Access Control Fundamentals.

Requisite Course Objectives

CIS 060-Evaluate the need for the careful design of a secure organizational information infrastructure.

Entrance Skills

Authentication and Account Management.

Requisite Course Objectives

CIS 060-Evaluate the need for the careful design of a secure organizational information infrastructure.
CIS 060-Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/ controls.

Entrance Skills

Risk Mitigation

Requisite Course Objectives

CIS 060-Perform risk analysis and risk management.

Course Content

1.0 Introduction to Ethical Hacking
- Introductions

2.0 Introduction to Penetration Testing
- Penetration Testing Process and Types
- Threat Actors
- Target Selection
- Assessment Types
- Legal and Ethical Compliance

3.0 Social Engineering and Physical Security
- Social Engineering
- Physical Security
- Countermeasures and Prevention

4.0 Reconnaissance
- Reconnaissance Overview
- Reconnaissance Countermeasures

5.0 Scanning
- Scanning Overview
- Banner Grabbing

6.0 Enumeration
- Enumeration Overview
- Enumeration Counter Measures

7.0 Analyze Vulnerabilities
- Vulnerability Assessment
- Vulnerability Management Life Cycle
- Vulnerability Assessment Tools

8.0 System Hacking
- System Hacking
- Privilege Escalation
- Maintain Access
- Cover Your Tracks

9.0 Malware
- Malware
- Combat Malware

10.0 Sniffers, Session Hijacking and Denial of Service
- Sniffing
- Session Hijacking
- Denial of Service

11.0 Intrusion Detection Systems (IDS), Firewalls, and Honeypots
- Intrusion Detection Systems (IDS)
- Firewalls
- Honeypots

12.0 Web Servers, Web Applications, and Structured Query Language (SQL) Injections
- Web Servers
- Web Applications
- SQL Injections

13.0 Wi-Fi, Bluetooth, and Mobile Devices
- Wi-Fi
- Bluetooth
- Mobile Devices

14.0 Cloud Computing and Internet of Things (IoT)

- Cloud Computing
- Internet of Things (IoT)

15.0 Cryptography
- Cryptography
- Public Key Infrastructure (PKI)
- Cryptanalysis and Cryptographic Attack Countermeasures

Lab Content
- Identify Social Engineering
- Implement Physical Security Measures
- Perform Reconnaissance with Nmap
- Disable Windows Services
- Manage Linux Services
- Enable and Disable Linus Services
- Hide the IIS Banner Broadcast
- Perform an Internal Scan
- Perform an External Scan Using Zenmap
- Perform enumeration with Nmap
- Perform enumeration with Metasploit
- Perform Enumeration of MSSQL (Microsoft Structure Query Language) with Metasploit
- Prevent Zone Transfer
- Scan for Vulnerabilities on a Windows Workstation
- Scan for Vulnerabilities on a Domain Controller
- Scan for Vulnerabilities on a Security Appliance
- Scan for Vulnerabilities on a WAP (Wireless Access Point)
- Analyze a USB (Universal Serial Bus) Keylogger Attack
- Analyze a USB Keylogger Attack 2
- Crack a Password with Rainbow Tables
- Crack a Password with John the Ripper
- Configure Account Password Policies
- Crack the SAM (Secure Account Manager) Database with John the Ripper
- Enforce User Account Control
- Create a Backdoor with Metasploit
- Create a backdoor with Netcat
- Clear Windows Loge Files on Server 2016
- Clear Audit Policies
- Hide Files with OpenStego
- Detect Open Ports with Nmap
- View Open Ports with Netstat
- Scan for Open Ports from a Remote Computer
- Counter Malware with Windows Defender
- Spoof MAC (Media Access Control) Addresses with SMAC
- Poison ARP (Address Resolution Protocol) and Analyze with Wireshark
- Poison DNS (Domain Name System)
- Filter and Analyze Traffic with Wireshark
- Analyze Email Traffic for Sensitive Data
- Analyze Email Traffic for Sensitive Data 2
- Perform a DHCP (Dynamis Host Configuration Protocol) Spoofing Man-in-the-Middle (MITM) Attack
- Perform a MITM from a remote Computer
- Capture HTTP (Hypertext Transfer Protocol) POST Packets with Wireshark
- Hijack a Web Session
- Perform and Analyze an SYN (Synchronize) Flood Attack
- Analyze ICMP (Internet Control Message Protocol) Traffic in Wireshark
- Perform a DoS (Denial of Service) Attack
- Analyze a DDoS (Distributed Denial of Service) Attack

- Implement Intrusion Detection
- Configure a Perimeter Firewall
- Perform a Decoy Scan
- Perform a Decoy Scan with Zenmap
- Bypass Windows Firewall with Metasploit
- Create a Honeypot with Pentbox
- Extract Web Server Information with Nmap
- Crack FTP (File Transfer Protocol) Credentials with Wireshark
- Perform a SQL (Structured Query language) Injection Attack
- Discover a Hidden Network
- Discover a Rogue DHCP (Dynamic Host Configuration Protocol) Server
- Locate a Rogue Wireless Access Point (WAP)
- Discover Bluetooth Devices
- Secure a Mobile Device
- Scan for IoT (Internet of Things) Devices
- Compare an MD5 Hash
- Encrypt a Hard Drive

Course Objectives

	Objectives
Objective 1	Identify footprinting techniques and tools
Objective 2	Recognize the characteristics of the enumeration phase of an attack and effective countermeasures
Objective 3	Determine the techniques and tools used in system hacking
Objective 4	Describe the characteristics of trojans, worms, and malware
Objective 5	Differentiate between ARP (Address Resolution Protocol) attack tools and countermeasures
Objective 6	Sequence the steps you would perform to complete a penetration test on your web servers
Objective 7	Determine what you test for at which stage of web application penetration
Objective 8	Determine how to counter wireless network hacking techniques
Objective 9	Identify tools and techniques used to evade IDS (Intrusion Detection System), firewalls, and honeypots
Objective 10	Determine ways to assess the effectiveness of security policies and procedures
Objective 11	Determine the type of penetration test to perform in a given situation
Objective 12	Evaluate various techniques and tools used in network scanning
Objective 13	Identify social engineering techniques and countermeasures
Objective 14	Determine countermeasures to denial-of-service (DoS) and session hijacking attacks
Objective 15	Describe best practices for keeping Android, iOS (iPhone Operating System), and Windows OS (Operating Service) devices secure

Student Learning Outcomes

	Upon satisfactory completion of this course, students will be able to:
Outcome 1	Apply the same tools and methods a "hacker" uses to break into a computer or network.
Outcome 2	Plan a vulnerability assessment and penetration test for a network
Outcome 3	Identify legal and ethical issues related to vulnerabilities and penetration testing

Methods of Instruction

Method	Please provide a description or examples of how each instructional method will be used in this course.
Collaborative/Team	Students will work in groups to determine network vulnerabilities.
Activity	Attempt to bypass COD network security.
Technology-based instruction	Utilize simulations and other IT equipment.
Participation	Students will be engaged with daily classroom or online forum participation.

Observation	Watch instructor setup man-in-the-middle type of attacks in a predetermined network.
Lecture	Attend instructor-led lectures.
Laboratory	Continuing work throughout the course using hands-on (classroom) and virtual computing devices and software.
Discussion	Weekly discussion topics on hacking case analysis.

Methods of Evaluation

Method	Please provide a description or examples of how each evaluation method will be used in this course.	Type of Assignment
Written homework	Written on-line assignments with topics relevant to the curriculum.	In and Out of Class
Student participation/contribution	Students will describe to the class steps taken to troubleshoot issues.	In and Out of Class
Tests/Quizzes/Examinations	Testing of each learning module.	In and Out of Class
Group activity participation/observation	Class and individual projects such as securing a local network.	In and Out of Class
Presentations/student demonstration observations	Hands-on-projects and a combination of examinations, presentations, discussions, or problem-solving assignments. Presentations of projects within specific modules.	In and Out of Class
Computational/problem-solving evaluations	Diagnose security flaws connections using appropriate software.	In and Out of Class
Laboratory projects	Laboratory projects/performance within a locally hosted network simulator.	In and Out of Class
Mid-term and final evaluations	Final examination/skills assessment in industry recognized security certification	In and Out of Class

Assignments

Other In-class Assignments

- Passive and active reconnaissance
- Linux/OSX exploits
- Vulnerability assessment reports
- Windows exploits
- Social Engineering and Advanced Persistent Threats (APT)
- Evasive Maneuvers and Post Exploitation
- Utilize Google Hacking Database (GHDB) and Other Google Hacking tools
- Present an overview of network scanning and the most commonly used tools
- Use of simulation software to develop networks that students can hack into. All these activities can be performed virtually.

Other Out-of-class Assignments

- Hands-on projects (hardening computer and server security)
- Problem-solving assignments such as hackthissite.org - realistic missions.
- Students will be assigned case-based assignments involving reading, computer manuals, and general textbook reading that cover network communications and possible exploits.
- Various assignments for this course involve the hacking of dummy networks. These activities will be performed by students on an individual basis outside of class time.
- Case studies will be assigned requiring outside research and readings like the following. Setup Man-in-the-Middle type of attacks on your personal home network.

Grade Methods

Letter Grade Only

Distance Education Checklist

Include the percentage of online and on-campus instruction you anticipate.

Online %
100
On-campus %
100

What will you be doing in the face-to-face sections of your course that necessitates a hybrid delivery vs a fully online delivery?
We will be using materials provided by the publisher and others that professionals use in the industry. We will maintain proper vigilance to ensure our materials are relevant, cost effective, and appropriate for online instruction.

Lab Courses

How will the lab component of your course be differentiated from the lecture component of the course?
Labs will be hands-on training using specific applications, software, and equipment to complete a certain task

From the COR list, what activities are specified as lab, and how will those be monitored by the instructor?
The labs are monitored by the instructor using a scoring system and annotated in the grade book

How will you assess the online delivery of lab activities?
The labs are online in the TestOut servers

Instructional Materials and Resources

If you use any other technologies in addition to the college LMS, what other technologies will you use and how are you ensuring student data security?
We rely on our partners to provide such security to their systems to protect our students' data. Our data, on the other hand, is secured through Canvas.

If used, explain how specific materials and resources outside the LMS will be used to enhance student learning.
Labs and courseware are fully online except for the some labs preformed in a face to face class

Effective Student/Faculty Contact

Which of the following methods of regular, timely, and effective student/faculty contact will be used in this course?

Within Course Management System:
Chat room/instant messaging
Discussion forums with substantive instructor participation
Online quizzes and examinations
Private messages
Regular virtual office hours
Timely feedback and return of student work as specified in the syllabus
Weekly announcements

External to Course Management System:
Posted audio/video (including YouTube, 3cmediasolutions, etc.)
Synchronous audio/video
Teleconferencing
Telephone contact/voicemail

Briefly discuss how the selected strategies above will be used to maintain Regular Effective Contact in the course.
There will be weekly discussions regarding topics related to the course with appropriate instructor participation.
Students will create logs describing the process to diagnose an issue. These logs are uploaded to the LMS and receive appropriate instructor feedback.

If interacting with students outside the LMS, explain how additional interactions with students outside the LMS will enhance student learning.
We have researched various approaches to teaching this course and have compiled them into this course. We have strongly considered the fact that this course may have to be taught online primarily considering the current situation.

Other Information

Comparable Transfer Course Information

University System
CSU

Campus
CSU San Bernardino

Course Number
2610

Course Title
Cybersecurity

Catalog Year
2021

MIS Course Data

CIP Code
11.0101 - Computer and Information Sciences, General.

TOP Code
070100 - Information Technology, General

SAM Code
C - Clearly Occupational

Basic Skills Status
Not Basic Skills

Prior College Level
Not applicable

Cooperative Work Experience
Not a Coop Course

Course Classification Status
Credit Course

Approved Special Class
Not special class

Noncredit Category
Not Applicable, Credit Course

Funding Agency Category
Not Applicable

Program Status
Program Applicable

Transfer Status
Transferable to CSU only

General Education Status
Y = Not applicable

Support Course Status
N = Course is not a support course

C-ID
ITIS 164

Allow Audit
No

Repeatability
No

Materials Fee
No

Additional Fees?
No

Approvals

Curriculum Committee Approval Date
04/05/2022

Academic Senate Approval Date
04/28/2022

Board of Trustees Approval Date
06/16/2022

Chancellor's Office Approval Date
06/18/2022

Course Control Number
CCC000632407

Programs referencing this course
Liberal Arts: Business and Technology AA Degree (http://catalog.collegeofthedesert.eduundefined/?key=27)
Computer Information Systems Associate of Science (http://catalog.collegeofthedesert.eduundefined/?key=323)
Computer Information Systems AS Degree for Employment Preparation (http://catalog.collegeofthedesert.eduundefined/?key=61)