CNIT R146: CYBERSECURITY: FUNDAMENTALS OF ETHICAL HACKING

Originator
ptrujillo

Co-Contributor(s)

Name(s)
Lynch , Alex (alynch)

College
Oxnard College

Discipline (CB01A)
CNIT - Computer Networking/IT

Course Number (CB01B)
R146

Course Title (CB02)
Cybersecurity: Fundamentals of Ethical Hacking

Banner/Short Title
Cybersecurity: Ethical Hacking

Credit Type
Credit

Start Term
Fall 2023

Catalog Course Description
This course helps to prepare students for a lucrative career in cybersecurity. Students will learn the methods to perform a vulnerability scan and subsequently a penetration test on host-based and network-based systems. Students will learn how to interpret the results, write detailed summary reports, and recommend mitigation strategies. This course prepares students for the TestOut Ethical Hacker Pro and the EC-Council Certified Ethical Hacker Certification Exams.

Taxonomy of Programs (TOP) Code (CB03)
0708.10 - *Computer Networking

Course Credit Status (CB04)
D (Credit - Degree Applicable)

Course Transfer Status (CB05) (select one only)
B (Transferable to CSU only)

Course Basic Skills Status (CB08)
N - The Course is Not a Basic Skills Course

SAM Priority Code (CB09)
C - Clearly Occupational

Course Cooperative Work Experience Education Status (CB10)
N - Is Not Part of a Cooperative Work Experience Education Program

Course Classification Status (CB11)
Y - Credit Course

Educational Assistance Class Instruction (Approved Special Class) (CB13)
N - The Course is Not an Approved Special Class

Course Prior to Transfer Level (CB21)
Y - Not Applicable

Course Noncredit Category (CB22)
Y - Credit Course

Funding Agency Category (CB23)
Y - Not Applicable (Funding Not Used)

Course Program Status (CB24)
1 - Program Applicable

General Education Status (CB25)
Y - Not Applicable

Support Course Status (CB26)
N - Course is not a support course

Field trips
May be required

Faculty notes on field trips; include possible destinations or other pertinent information
Possible destinations would be an IT shop, IT managed service provider, or a cybersecurity special event in Ventura County.

Grading method
(L) Letter Graded

Alternate grading methods
(E) Credit by exam, license, etc.

Does this course require an instructional materials fee?
No

Repeatable for Credit
No

Is this course part of a family?
No

Units and Hours

Carnegie Unit Override
No

In-Class

Lecture
Minimum Contact/In-Class Lecture Hours
43.75
Maximum Contact/In-Class Lecture Hours
43.75

Activity

Laboratory
Minimum Contact/In-Class Laboratory Hours
26.25

Maximum Contact/In-Class Laboratory Hours
26.25

Total in-Class

Total in-Class
Total Minimum Contact/In-Class Hours
70
Total Maximum Contact/In-Class Hours
70

Outside-of-Class

Internship/Cooperative Work Experience

Paid

Unpaid

Total Outside-of-Class

Total Outside-of-Class
Minimum Outside-of-Class Hours
87.5
Maximum Outside-of-Class Hours
87.5

Total Student Learning

Total Student Learning
Total Minimum Student Learning Hours
157.5
Total Maximum Student Learning Hours
157.5

Minimum Units (CB07)
3
Maximum Units (CB06)
3

Advisories on Recommended Preparation
CNIT R145

Entrance Skills

Entrance Skills
It is important that students have a solid understanding of cybersecurity fundamentals prior to taking this standalone course in the specialized cybersecurity area of penetration testing.

Prerequisite Course Objectives
CNIT R145-Differentiate and explain access control models
CNIT R145-Compare and contrast various authentication methods
CNIT R145-Identify non-essential protocols that pose a security risk
CNIT R145-Recognize attack methods and actions to take to mitigate risk
CNIT R145-Identify malicious code and appropriate actions to reduce vulnerability
CNIT R145-Understand the concept of social engineering and the risk it poses
CNIT R145-Log and record data
CNIT R145-Identify and define various remote access technologies
CNIT R145-Understand the administration of email security concepts
CNIT R145-Compare and contrast Internet security concepts
CNIT R145-Differentiate and explain wireless security protocols

CNIT R145-Evaluate security concerns on hardware devices
CNIT R145-Identify security concerns of different networking media
CNIT R145-Analyze types of intrusion detection systems
CNIT R145-Compare cryptography algorithms and summarize strength of each type of algorithm
CNIT R145-List the steps that are necessary to deal with a cybersecurity incident
CNIT R145-Differentiate between the different cloud coputing models

Requisite Justification

Requisite Type
Advisory

Requisite
CNIT R145

Requisite Description
Course in a sequence

Level of Scrutiny/Justification
Content review

Student Learning Outcomes (CSLOs)

	Upon satisfactory completion of the course, students will be able to:
1	Explain the key aspects of compliance-based assessments.
2	Describe the steps used to engage in a penetration test.
3	Summarize the legal issues related to performing penetration testing.

Course Objectives

	Upon satisfactory completion of the course, students will be able to:
1	Describe the tools and methods a "hacker" uses to break into a computer or 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 use safe techniques on the World Wide Web.
4	Perform a vulnerability scan using popular vulnerability scanning tools.
5	Perform an exploitation based on the results of a vulnerability scan.
6	Communicate recommended strategies to improve the overall state of IT security.
7	Mitigate host and network based vulnerabilities once identified.
8	Write a report of penetration test findings and remediation.

Course Content

Lecture/Course Content

1. Planning for an engagement
   a. Understanding the target audience
   b. Rules of engagement
   c. Communication escalation path
   d. Resources and requirements
   e. Budget
   f. Impact analysis and remediation timelines
   g. Disclaimers
   h. Technical constraints
   i. Support resources
2. Key legal concepts

   a. Ethical hacking
   b. Contracts
   c. Environmental differences
   d. Written authorization
3. Scoping an engagement properly
   a. Types of assessment
   b. Special scoping considerations
   c. Target selection
   d. Strategy
   e. Risk acceptance
   f. Tolerance to impact
   g. Scope creep
   h. Threat actors
4. Compliance-based assessments
   a. Compliance-based assessments, limitations and caveats
   b. Clearly defined objectives based on regulations
5. Information Gathering
   a. Port Scanning
   b. Enumeration
   c. Footprinting
   d. Packet crafting
   e. Packet inspection
   f. Fingerprinting
   g. Cryptography
   h. Eavesdropping
   i. Social Enginnering
   j. Decompilation
   k. Debugging
   l. Open Source Intelligence Gathering
6. Vulnerability Scan
   a. Credentialed vs. non-credentialed
   b. Types of scans
   c. Container security
   d. Application scan
   e. Considerations of vulnerability scanning
7. Analyze vulnerability scan results
   a. Asset categorization
   b. Prioritization of vulnerabilities
   c. Common themes
8. Leveraging information to prepare for exploitation
   a. Map vulnerabilities to potential exploits
   b. Prioritize activities in preparation for penetration test
   c. Common techniques to complete attack
      i. Cross-compiling code
      ii. Exploit modification
      iii. Exploit chaining
      iv. Proof-of-concept development
      v. Social engineering
      vi. Credential brute forcing
      vii. Dictionary attacks
      viii. Rainbow tables
      ix. Deception
9. Weaknesses related to specialized systems.
   a. ICS
   b. SCADA
   c. Mobile
   d. IoT
   e. Linux OS vulnerabilities

   f. Embedded operating systems
   g. Point-of-sale system
   h. Biometrics
   i. Application containers
   j. RTOS
10. Attacks and Exploits
   a. Social engineering attacks
   b. Exploit network-based vulnerabilities
   c. Hacking wireless networks
   d. Exploit application-based vulnerabilities
   e. Exploit local host vulnerabilities
   f. Hacking web servers
   g. Physical security attacks
   h. Post-exploitation techniques
11. Penetration Testing Tools
   a. SYN scan (-sS) vs. full connect scan
   b. Port selection
   c. Service identification
   d. OS fingerprinting
   e. Disabling ping
   f. Target input file
   g. Timing
   h. Output parameters
12. Reporting and Communication
   a. Normalization of data
   b. Written report of findings and remediation
   c. Risk appetite
   d. Storage time for report
   e. Secure handling and disposition of reports
   f. Post-engagement cleanup
   g. Lessons learned
   h. Follow-up actions/retest
   i. Attestation of findings
13. Protecting Networks with Security Devices
   a. Hardware based security devices
   b. Software based security devices
   c. Cybersecurity companies and their offerings
      i. Cyberark
      ii. Fireeye
      iii. Cisco
      iv. Palo Alto Networks
      v. Check Point

Laboratory or Activity Content

1. Vulnerability Testing Labs
   a. Scanning
   b. Enumeration
   c. Packet crafting
   d. Packet inspection
   e. Fingerprinting services and OS
   f. Packet capture and analysis
2. Penetration Testing Labs
   a. Injections
   b. SMB exploits
   c. SNMP exploits
   d. SMTP exploits
   e. FTP exploits
   f. DNS cache poisoning

   g. Pass the hash
   h. Man-in-the-middle
   i. DoS/stress test
   j. VLAN hopping
3. Wireless Penetration Testing Labs
   a. Evil twin
   b. Deauthentication attacks
   c. Fragmentation attacks
   d. Credential harvesting
   e. WPS implementation weakness
   f. Bluejacking
4. Reporting and Communication
   a. Normalization of data
   b. Written report of findings and remediation
5. Kali Linux OS
   a. Download and installation
   b. Ethical hacking
   c. GUI vulnerability/pen testing software
   d. CLI vulnerability/pen testing software
6. Operating System Vulnerabilities and Exploits
   a. Windows 10
   b. Apple OS X
   c. Linux
   d. Cisco IOS
   e. Android
   f. iOS

Methods of Evaluation

Which of these methods will students use to demonstrate proficiency in the subject matter of this course? (Check all that apply):

Written expression
Problem solving exercises
Skills demonstrations

Methods of Evaluation may include, but are not limited to, the following typical classroom assessment techniques/required assignments (check as many as are deemed appropriate):

Computational homework
Group projects
Individual projects
Laboratory activities
Laboratory reports
Objective exams
Problem-solving exams
Quizzes
Research papers
Skills demonstrations
Essays
Projects
Problem-Solving Assignments

Instructional Methodology

Specify the methods of instruction that may be employed in this course

Class activities
Class discussions
Collaborative group work
Computer-aided presentations
Distance Education
Field trips
Group discussions
Guest speakers
Instructor-guided interpretation and analysis

Instructor-guided use of technology
Internet research
Laboratory activities
Lecture
Small group activities

Describe specific examples of the methods the instructor will use:

1. Instructor will use PowerPoints provided by the publisher to lecture on chapter penetration testing topics.
2. The instructor will provide a demonstration on how to perform white hat vulnerability scanning and penetration tests.
3. The instructor will summarize cybersecurity current events and ask students critical thinking questions.
4. The instructor will form small groups and have each group research a specific vulnerability scanning or pen testing software tool. The group will then create a short presentation to share with the other groups in the class that will include the name of the tool, its specific purpose, and in what situation the tool is most appropriate.

Representative Course Assignments

Writing Assignments

1. Students will be asked to compare and contrast different types of pen testing software and share their response in a written summary.
2. Students will need to write explanations which demonstrate comprehension in security mitigation techniques once a vulnerability has been discovered from an assessment.
3. Students will be required to write about difficulties they encountered during pen testing lab activities and actions they took to alleviate the problem.

Critical Thinking Assignments

1. Evaluation of a cybersecurity vulnerability for a specific OS configuration and recommended steps that should be taken to mitigate the risk.
2. Evaluation of a cybersecurity vulnerability for a specific intermediary device configuration and recommended steps that should be taken to mitigate the risk.
3. Students will research the type of activities that demonstrate when white hat hacking has ventured into gray hat or black hat hacking and communicate their viewpoint on when that has occurred.

Reading Assignments

1. Students are required to read and study the information in the assigned chapter of the textbook in between classes in order to be prepared for the lecture and classroom activities.
2. Students are required to perform reading from assigned cybersecurity support websites such as www.sans.org, www.cert.org, www.cisecurity.com, www.darkreading.com, and forums.kali.org.

Skills Demonstrations

1. Students will demonstrate they can use the appropriate software tools to discover vulnerabilities on a PC with a specific operating system that has been preconfigured with vulnerabilities.
2. Students will demonstrate they can use the appropriate software tools to discover vulnerabilities on a networking device such as a switch or router with a specific operating system that has been preconfigured with vulnerabilties.
3. Students will demonstrate they can use the appropriate pen testing software tools to exploit vulnerabilities on a PC with a specific operating system that has been preconfigured with vulnerabilties.
4. Students will demonstrate they can use the appropriate pen testing software tools to exploit vulnerabilities on a networking device such as a switch or router with a specific operating system that has been preconfigured with vulnerabilties.

Problem-Solving and Other Assignments (if applicable)

1. Students will be required to answer preparation questions for the TestOut Ethical Hacker Pro and EC-Council Certified Ethical Hacker certifications.
2. Students will be perform practice skills exams.

Outside Assignments

Representative Outside Assignments

1. Read the assigned TestOut Ethical Hacker Pro chapters.
2. Watch the embedded videos in the TestOut Ethical Hacker Pro courseware.
3. Complete the assigned embedded lab activities in the TestOut Ethical Hacker Pro courseware.

4. Read about cybersecurity current events related to pen testing and exploits at www.sans.org/newsbites. Students will need to summarize the article or be prepared to provide an oral summary of the current event to their fellow students.
5. Read Kali Linux security blogs online and answer discussion questions in the course portal as it relates to updates regarding vulnerability scanning and pen testing software.

Articulation

C-ID Descriptor Number
ITIS 164

Status
Approved

Comparable Courses within the VCCCD
CNSE M84 - Certified Ethical Hacker

Equivalent Courses at other CCCs

College	Course ID	Course Title	Units
Coastline Community College	CST 242	PenTest+	3

District General Education

A. Natural Sciences

B. Social and Behavioral Sciences

C. Humanities

D. Language and Rationality

E. Health and Physical Education/Kinesiology

F. Ethnic Studies/Gender Studies

CSU GE-Breadth

Area A: English Language Communication and Critical Thinking

Area B: Scientific Inquiry and Quantitative Reasoning

Area C: Arts and Humanities

Area D: Social Sciences

Area E: Lifelong Learning and Self-Development

Area F: Ethnic Studies

CSU Graduation Requirement in U.S. History, Constitution and American Ideals:

IGETC

Area 1: English Communication

Area 2A: Mathematical Concepts & Quantitative Reasoning

Area 3: Arts and Humanities

Area 4: Social and Behavioral Sciences

Area 5: Physical and Biological Sciences

Area 6: Languages Other than English (LOTE)

Textbooks and Lab Manuals

Resource Type
Other Instructional Materials

Description
Kali Linux Pen Testing Toolkit

Resource Type
Other Instructional Materials

Description
Vulnerability scanning software such as Nessus and Nmap..

Resource Type
Other Instructional Materials

Description
Wireshark Protocol Analyzer

Resource Type
Other Resource Type

Description
TestOut Certified Ethical Hacker Pro courseware, 2022 (The curriculum is continuously updated online)

Distance Education Addendum

Definitions

Distance Education Modalities
Hybrid (1%–50% online)
Hybrid (51%–99% online)
100% online

Faculty Certifications

Faculty assigned to teach Hybrid or Fully Online sections of this course will receive training in how to satisfy the Federal and state regulations governing regular effective/substantive contact for distance education. The training will include common elements in the district-supported learning management system (LMS), online teaching methods, regular effective/substantive contact, and best practices.
Yes

Faculty assigned to teach Hybrid or Fully Online sections of this course will meet with the EAC Alternate Media Specialist to ensure that the course content meets the required Federal and state accessibility standards for access by students with disabilities. Common areas for discussion include accessibility of PDF files, images, captioning of videos, Power Point presentations, math and scientific notation, and ensuring the use of style mark-up in Word documents.
Yes

Regular Effective/Substantive Contact

Hybrid (1%–50% online) Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity to provide commentary and feedback on fellow student responses.
E-mail	Email will be used for individual interaction between professor and student, to send group email reminders of deadlines, to inform of upcoming course content.
Face to Face (by student request; cannot be required)	Part of the course requires face to face time. Also, face to face with individuals will take place to discus specific questions, issues or concerns.
Video Conferencing	Zoom or comparable video conferencing software to lecture on course content, demonstrate lab assignments, answer student questions in real time, and provide student assistance on anything that is course related.
Other DE (e.g., recorded lectures)	Any real-time instruction will be recorded and available to students through the LMS.

Hybrid (51%–99% online) Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity to provide commentary and feedback on fellow student responses.

E-mail	Email will be used for individual interaction between professor and student, to send group email reminders of deadlines, to inform of upcoming course content.
Face to Face (by student request; cannot be required)	Part of the course requires face to face time. Also, face to face with individuals will take place to discus specific questions, issues or concerns.
Video Conferencing	Zoom or comparable video conferencing software to lecture on course content, demonstrate lab assignments, answer student questions in real time, and provide student assistance on anything that is course related.
Other DE (e.g., recorded lectures)	Any real-time instruction will be recorded and available to students through the LMS.

100% online Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity to provide commentary and feedback on fellow student responses.
E-mail	Email will be used for individual interaction between professor and student, to send group email reminders of deadlines, to inform of upcoming course content.
Video Conferencing	Zoom or comparable video conferencing software will be utilized to lecture on course content, demonstrate lab assignments, answer student questions in real time, and provide student assistance on anything that is course related.
Other DE (e.g., recorded lectures)	Any real-time instruction will be recorded and available to students through the LMS.

Examinations

Hybrid (1%–50% online) Modality

On campus
Online

Hybrid (51%–99% online) Modality

On campus
Online

Primary Minimum Qualification

COMPUTER INFORMATION SYS

Additional local certifications required

CompTIA PenTest+. This course is preparing students to take and pass the CompTIA PenTest+ certification so the instructor needs to hold this certification.

Review and Approval Dates

Department Chair

11/16/2022

Dean

11/16/2022

Technical Review

11/23/2022

Curriculum Committee

11/23/2022

Curriculum Committee

12/14/2022

Control Number
CCC000599227

DOE/accreditation approval date
MM/DD/YYYY