CSIS-164: CYBERSECURITY: ETHICAL HACKING

Effective Term
Fall 2025

BOT Approval Date
01/16/2025

Discipline
CSIS - Computer Sci/Info Systems
Course Number
164

Course Title
Cybersecurity: Ethical Hacking

Short Title
Cybersecurity: Ethical Hacking

Credit Status (CB 04)
D - Credit - Degree applicable

Units

Lecture Units
3.00

Total Units
3.00

Hours

Lecture Contact Hours
48-54
Out of Class Hours Lecture
96-108

Total Contact Hours
48 - 54

Total Out of Class Hours
96 - 108

Total Student Learning Hours
144 - 162

Distance Education
Yes

Distance Education

Distance Education Type
Both Fully Online and Hybrid Online

Fully Online Delivery Requirements:
a. Students must be notified via the college schedule of classes and the syllabus for the class if proctored tests are required for this course
b. Any planned face-to-face meetings, such as an orientation or study session, must be optional

c. The MSJC curriculum committee requires the use of accessible, asynchronous discussion as a component of every fully online course

Are you using publisher content?

No

Regular Substantive Interaction

Instructor-to-student, student-to-student, and student-to-content contact shall be distributed in a manner that will ensure regular substantive interaction (RSI) is maintained not only weekly but also for the duration of the course. Instructor interactions should be equivalent in time, quality and consistency to the engagement students would receive in a face-to-face course—for example, through announcements, discussion participation, personalized feedback, video messages, or other instructional communications. Instructors are expected to be responsive to student inquiries within a 24-72 hour time frame excluding holidays. RSI will be maintained through a variety of methods: • Orientation - Students must be oriented to the online and face-to-face portions at the start of the course. • Announcements - Announcements using the course management system must be posted at least weekly to keep students current on course events, due dates, materials, etc. • Discussion Forums - Content-related discussion forums within the designated CMS will include appropriate instructor participation and will be initiated and maintained, with timely feedback provided. Instructors are required to monitor the discussions and related activities to provide guidance and direction. Open-ended discussion boards may be used to further learning and interaction. • MSJC Communication – Instructor will use MSJC-administered communication tools (such as email or the designated CMS communication tools) to regularly communicate with and provide ease of access to students. • Timely Feedback - Timely feedback on student work will be provided by the instructor, which may include comments and/or rubrics, within the Grades area of the designated CMS. • Scheduled Meetings – Hybrid and synchronous courses will meet at regularly scheduled times. ADA Compliance - All course interactions and content must be designed with accessibility in mind and meet ADA requirements.

Catalog Description

This course is a survey of the ethical and legal issues pertaining to security testing. It demonstrates how to use tools that can be used to gain information about a computer network, how to recognize that the tools are being used, and how to defend a network against those attacks.

Codes

TOP Code (CB 03)

0708.10* - *Computer Networking

CIP Code

43.0116 - Cyber/Computer Forensics and Counterterrorism.

Repeatability Code

No

Grading Option

Letter grade OR P/NP

Learning Objectives

Learning Objectives

Learning Objective
1. Describe the role of an ethical hacker.
2. Test a data communications network for security vulnerabilities.
3. Compose a certifiable security report.
4. Compare port scanning tools for viability.
5. Enumerate Windows OS targets and services.
6. Develop custom software applications for security testing purposes.
7. Analyze authentication processes for security vulnerabilities.
8. Compare symmetric and asymmetric encryption algorithms.
9. Describe intrusion detection and prevention systems and Web-filtering technologies.

10. Analyze the impact of "black hat" and "white hat" terminology in cybersecurity, propose inclusive alternatives, and strategize ways to foster diversity and nuanced understanding within the field.

Learning Outcome Information

Course Learning Outcomes

Learning Outcome
1. The student will demonstrate the ability to install, configure, and fine tune various tools that can be used to test and defend a computer network, a server, or a PC from inside or outside attacks.
2. Given an insecure network, the student will analyze and test it for vulnerabilities.
3. The student will explain how tools can be used to attack the system.

Program Learning Outcomes

Learning Outcome
Research and apply industry reference models and best practices in order to improve process designs. Apply systems concepts in the investigation, evaluation, and resolution of information technology problems.

Institutional Learning Outcomes

Information and Technology Literacy: The student will access, interpret, evaluate, and apply relevant information sources and digital media effectively, and in an ethical and legal manner.
Scientific Awareness: The student will apply the scientific method of inquiry to assess potential solutions for real-life challenges by employing science-based knowledge and methodologies in daily life.

Content

Course Lecture Content

1. Ethical Hacking
    a. Overview
    b. Introduction to Ethical Hacking
    c. The Role of Security and Penetration Testers
    d. Penetration-Testing Methodologies
    e. Certification Programs for Network Security Personnel
    f. What You Can Do Legally
    g. Laws of the Land
        i. Is Port Scanning Legal?
    h. Federal Laws
    i. What You Cannot Do Legally
    j. Get It in Writing
    k. Ethical Hacking in a Nutshell
2. TCP/IP Concepts Review
    a. Overview of TCP/IP
    b. The Application Layer
    c. The Transport Layer
    d. The Internet Layer
3. IP Addressing
    a. CIDR Notation
    b. Planning IP Address Assignments
    c. IPv6 Addressing
4. Overview of Numbering Systems
    a. Reviewing the Binary Numbering System
    b. Reviewing the Octal Numbering System
    c. Reviewing the Hexadecimal Numbering System
    d. Reviewing the Base-64 Numbering System
5. Network and Computer Attacks

   a. Malicious Software (Malware)
   b. Viruses
   c. Macro Viruses
   d. Worms
   e. Trojan
6. Programs
   a. Spyware
   b. Adware
   c. Protecting Against Malware
7. Intruder Attacks on Networks and Computers
   a. Denial-of-Service Attacks
   b. Distributed Denial-of-Service Attacks
   c. Buffer Overflow Attacks
   d. Eavesdropping
   e. Man-in-the-Middle
   f. Network Session Hijacking
8. Addressing Physical Security
   a. a.Keyloggers
   b. b.Behind Locked Doors
   c. c.Footprinting and Social Engineering
   d. d.Using Web Tools for Footprinting
   e. e.Conducting Competitive Intelligence
   f. f.Analyzing a Company's WebSite
   g. g.Using Other Footprinting Tools
   h. h.Using E-mail Addresses
9. Using HTTP Basics
10. a.Other Methods of Gathering Information
11. b.Using Domain Name
12. c.System Zone Transfers
13. 10. Introduction to Social Engineering
14. a.The Art of Shoulder Surfing
15. b.The Art of Dumpster
16. c.The Art of Piggybacking
17. d.Phishing
18. 11. Port Scanning
19. a.Introduction to Port Scanning
20. b.Types of Port Scans
21. c.Using Port-Scanning Tools
22. d.Nmap
23. f.Nessus and Open VAS (or Greenbone Security Assistant)
24. g.Conducting Ping Sweeps
25. h.Fping
26. i.Hping
27. j.Crafting
28. k.IP Packets
29. l.Understanding Scripting
30. m.Scripting Basic Enumeration
31. n.Introduction to Enumeration
32. o.Enumerating
33. 12. Windows Operating Systems
34. a.NetBIOS Basics
35. b.NetBIOS
36. c.Null Sessions
37. d.NetBIOS Enumeration Tools

38. e.Additional Enumeration Tools
39. f.Enumerating *nix
40. g.Operating System
41. h.*nix Enumeration
42. 13. Programming for Security Professionals
43. a.Introduction to Computer Programming
44. b.Programming Fundamentals
45. c.Learning the C Language
46. d.Anatomy of a C Program
47. e.Understanding HTML Basics
48. f.Creating a Web Page with HTML
49. g.Understanding Perl
50. h.Background on Perl
51. i.Understanding the Basics of Perl
52. j.Understanding the BLT of Perl
53. k.Understanding Object-Oriented Programming Concepts
54. l.Components of Object-Oriented Programming
55. m.An Overview of Ruby Desktop and Server OS
56. 14. Vulnerabilities
57. a.Windows OS Vulnerabilities
58. b.Windows File Systems
59. c.Remote Procedure Call
60. d.NetBIOS
61. f.Server Message Block
62. g.Common Internet File System
63. h.Null Sessions
64. i.Web Services
65. j.SQL
66. k.Server Buffer Overflows
67. l.Passwords and Authentication Tools for Identifying Vulnerabilities in Windows
68. m.Built-in Windows Tools
69. n.Best Practices for Hardening Windows Systems
70. o.Patching Systems Antivirus
71. p.Solutions
72. q.Enable Logging and Review Logs Regularly
73. r.Disable Unused Services and Filtering Ports
74. s.Other Security Best Practices
75. t.Linux OS Vulnerabilities
76. u.Samba Tools for Identifying Linux Vulnerabilities
77. v.More Countermeasures Against Linux Attacks
78. w.Embedded Operating Systems: The Hidden Threat
79. 15. Introduction to Embedded Operating Systems
80. a.Windows and Other Embedded Operating Systems
81. b.Other Proprietary
82. c.Embedded Oss
83. d.*Nix
84. e.Embedded Oss
85. f.Vulnerabilities of Embedded Oss
86. g.Embedded OSs Are Everywhere
87. h.Embedded Oss Are Networked
88. i.Embedded OSs Are Difficult to Patch
89. j.Embedded Oss Are in Networking Devices
90. k.Embedded Oss Are in Network Peripherals
91. 16. Supervisory Control and Data Acquisition Systems

92. a.Cell Phones, Smartphones, and PDAs Rootkits
93. b.Best Practices for Protecting Embedded Oss
94. c.Hacking Web Servers
95. d.Understanding Web Applications
96. 17. Web Application Components
97. a.Using Scripting Languages
98. b.Connecting to Databases
99. c.Understanding Web Application Vulnerabilities
100. d.Application Vulnerabilities and Countermeasures
101. e.Web Application Test Execution Tools for Web Attackers and Security Testers
102. f.Web Tools
103. 18. Hacking Wireless
104. a.Networks
105. b.Understanding Wireless Technology
106. c.Components of a Wireless Network
107. d.Understanding Wireless Network Standards
108. e.The 802.11 Standard
109. f.An Overview of Wireless Technologies
110. g.Additional IEEE 802.11 Projects Understanding Authentication
111. h.802.1X Standard
112. i.Understanding War driving
113. j.Understanding Wireless Hacking
114. k.Tools of the Trade
115. l.Countermeasures for Wireless
116. 19. Attacks
117. a.Cryptography
118. b.Understanding Cryptography Basics
119. c.History of Cryptography
120. d.Understanding Symmetric and Asymmetric
121. e.Algorithms
122. f.Symmetric Algorithms
123. g.Asymmetric Algorithms
124. h.Digital Signatures
125. i.Sensitive Data
126. j.Encryption
127. k.Hashing Algorithms
128. l.Understanding Public Key Infrastructure
129. m.Components of PKI
130. n.Understanding Cryptography Attacks
131. o.Birthday Attack
132. p.Mathematical Attack
133. q.Brute-Force Attack
134. r.Man-in-the-Middle Attack
135. s.SSL/TLS Downgrade Attack
136. t.Dictionary Attack
137. u.Replay Attack
138. v.Understanding Password Cracking
139. w.Network Protection Systems
140. 20. Understanding Network Protection Systems
141. a.Understanding Routers
142. b.Understanding Basic Hardware
143. c.Routers
144. d.Understanding Access Control Lists
145. f.Understanding Firewalls

146. g.Understanding Firewall Technology
147. h.Implementing a Firewall
148. i.Understanding the Cisco Adaptive Security Appliance Firewall
149. j.Using Configuration and Risk Analysis Tools for Firewalls and Routers
150. k.Understanding Intrusion Detection and Prevention Systems
151. l.Network-Based and Host-Based IDSs and IPSs
152. m.Web Filtering
153. n.Security Operations Center
154. o.Understanding Honeypots
155. p.How Honeypots Work.
156. 21. Understanding the Problems with "White Hat" and "Black Hat" Terminology in Ethical Hacking
157. a.Explore the historical context contributing to the adoption of this racially-charged terminology.
158. b.Recognize its implications on diversity and inclusion within the ethical hacking community.
159. c.Evaluate the ethical considerations associated with its use.

Methods of Instruction

Method

Discussion

Integration

Weekly discussions will be conducted as a means to compare and contrast various security vulnerabilities, threat analysis plans, and intrusion event categories. Method: Observation and Demonstration. In these discussions, students will not only examine technical aspects but also explore the diversity of impacts these security issues have on different communities. By integrating Diversity, Equity, and Inclusion (DEI) principles, students will consider how factors like culture, socioeconomic status, and accessibility affect the perception and handling of security threats.

For example, when discussing web application attacks like XSS or SQL Injection from their formative assignment, students will observe and demonstrate how these vulnerabilities might disproportionately affect underserved communities or regions with limited cybersecurity infrastructure. This approach encourages students to share diverse perspectives and fosters an inclusive environment where all voices contribute to a deeper understanding of the material.

DE Adaptations for MOI

Discussions will be conducted using the discussion tool within the course management system (CMS), which has been developed to prioritize accessibility. It includes features like screen reader compatibility, adjustable text size, and keyboard navigation to facilitate active participation for all students.The course's online forums, including the "Student Lounge" and formal discussion boards, will be spaces where students can engage in dialogues that emphasize DEI. When discussing topics from their assignments—like threat analysis plans or intrusion event categories—students will be encouraged to consider and share how these issues impact different groups globally.

Observation and Demonstration methods will be used as students post their analyses and respond to peers, highlighting varied perspectives influenced by cultural, ethical, and societal factors. This interaction not only enhances understanding of the technical content but also promotes an appreciation for diversity and the importance of inclusive practices in cybersecurity.

Feedback on contributions to discussions will be given through the CMS within one week, ensuring prompt and accessible interaction for everyone.

Method

Lecture

Integration

Lecture, with supporting visual materials (presentation or multimedia) will introduce conceptual and practical skills such as assessing different access control models, rating the effectiveness of various data ciphers, and the appraisal of different Antimalware and Antivirus software tools.Discuss how different access control models can impact users from diverse backgrounds, considering factors like accessibility, cultural norms, and varying levels of technical proficiency. Explore case studies where access control either enabled or hindered equitable access to resources.Analyze how antimalware and antivirus software can be designed to address threats prevalent in different parts of the world, ensuring that protection is not biased toward certain regions or demographics. Discuss the role of language support and user interface design in making these tools more inclusive.students will not only gain

technical expertise but also understand the broader social implications of information security. This approach fosters a more inclusive mindset, preparing students to develop security solutions that serve a diverse and global user base.

DE Adaptations for MOI

Lectures will be delivered via the course management system (CMS) using video capture software that combines voice narration with PowerPoint slides. To support accessibility, all video content will include closed captions and transcripts. The CMS will also serve as the platform for distributing additional lecture notes and sample materials, ensuring that all resources are readily accessible to students, regardless of their individual needs or location.

Method

Lab Activities

Integration

Guided practice and demonstration will illustrate lecture principles and reading assignments, with a focus on Intrusion Analysis, security attacks, and threat analysis. Discuss how unconscious biases can influence threat analysis and the interpretation of security data. Encourage students to recognize and mitigate these biases to develop more accurate and fair security assessments that consider the needs and vulnerabilities of all user groups.Examine how cultural differences can impact the perception of security threats and the effectiveness of response strategies. Encourage students to consider language barriers, local regulations, and cultural norms when developing threat mitigation plans.

DE Adaptations for MOI

Guided practice and demonstrations will be delivered through the course management system (CMS), featuring accessible videos with closed captions, web-based tutorials, and interactive hands-on activities. The CMS will also host interactive software simulations, providing students with real-time engagement and practice opportunities. These resources will ensure accessibility and foster active learning for all students.

Methods of Evaluation

Method

Exams/Tests

Integration

A midterm and final exam will be given. The exams will be composed of short answer and multiple choice questions designed to evaluate the mastery of such topics as incident response teams, intrusion analysis, security attacks, and access control models. Exams will be evaluated based on the correct answer given. Inclusive Question Design: Ensure that exam questions are culturally sensitive and free from bias, avoiding language or scenarios that could disadvantage any group of students. Case studies and examples used in questions will represent a diverse range of organizations and contexts, reflecting global perspectives in information security.Accessibility Considerations: Provide exams in formats accessible to all students, including those with disabilities. This may involve offering alternative formats such as large print, screen reader-compatible documents, or extended time accommodations to ensure equitable assessment conditions for all learners.

DE Adaptations for MOE

The midterm exam will be conducted through the course management system (CMS) and will include a combination of multiple-choice, true/false, and short-answer questions. Students will submit their exams directly through the CMS. Immediate feedback will be provided for objective questions like multiple-choice and true/false, while feedback for short-answer questions will be delivered within 48 hours. This approach ensures timely reinforcement of learning and helps students identify areas for improvement.

Method

Homework

Integration

Weekly Packet Tracer simulation and security report assignments will be given that apply important concepts and skills to the student's experience outside the classroom. The focus might be on network security devices, access control models, or Antimalware and Antivirus software tools. Incorporate Diverse Scenarios: Assignments will feature case studies and simulation tasks that represent a wide range of organizations and user demographics. This includes businesses of different sizes, cultural backgrounds,

and varying levels of technological advancement. By engaging with diverse scenarios, students will learn to design security solutions that are effective and sensitive to the needs of all users.

Emphasize Inclusive Design Principles: Students will be encouraged to consider accessibility and user-friendliness in their security configurations. For example, when setting up access control models, they should account for users with disabilities or those who may have limited technical expertise. This fosters the development of security systems that are usable by a broader audience.Homework will be evaluated based on correctness, completeness, and how well directions were followed.

DE Adaptations for MOE

Homework assignments will be submitted via the course management system (CMS) using the integrated assignment submission tool. All instructions and materials will be provided in accessible formats, including compatibility with screen readers and adjustable text settings, to ensure inclusivity. After submission, students will receive feedback through the CMS grading tool, with instructors offering detailed comments on accuracy, completeness, and adherence to guidelines. Feedback will be provided within one week, ensuring timely responses that help students monitor their progress and make improvements.

Method

Quizzes

Integration

Weekly multiple choice / short answer quizzes will be given as a means to test the students knowledge of Intrusion event categories, threat analysis, cipher effectiveness, and security vulnerabilities. Carefully craft quiz questions to use language that is free from bias or stereotypes. This includes avoiding culturally specific references that may not be universally understood and ensuring that terminology is accessible to all students, regardless of their background.Quizzes will be evaluated based on the correct answer given.

DE Adaptations for MOE

Quizzes will be administered and submitted through the Quiz tool in the course management system (CMS). Upon submission, students will receive immediate feedback for automatically graded questions, such as multiple-choice and true/false. For short-answer or more detailed responses, feedback will be provided within 48 hours through the CMS, enabling students to promptly review their performance and identify areas for improvement.

Assignments

Assignment Type

Writing

In-class and/or outside of class

In-class
Outside of class

Formative or Summative

Formative

Assignment

Throughout this course, you will engage in review questions and a series of hands-on lab exercises focused on cybersecurity and ethical hacking. These exercises are designed to provide you with practical experience, enhance your understanding of key concepts, and refine the technical skills needed to address complex challenges in the field.

Example Lab Exercise:
In this exercise, you will take on the role of an ethical hacker tasked with performing a proactive security assessment for a fictional large organization. You will begin by consulting with senior management to define the scope of the assessment, which will include systems, networks, policies, procedures, and human resources. Following this, you will negotiate the rules of engagement (RoE), ensuring that all guidelines for conducting the assessment are clear, ethical, and effective. Once the scope and RoE are agreed upon, you will move on to the information-gathering phase, where you will initiate the footprinting process. By using various data collection techniques, you will build a comprehensive blueprint of the organization's security profile, identifying vulnerabilities and areas that may require attention.

Grading and Feedback: Evaluation will be based on the successful completion of the tasks outlined in the lab instructions, with a focus on technical correctness, accuracy, and optimization of commands and scripts. Students' efforts in troubleshooting and problem-solving will be recognized and valued, irrespective of the final outcome. Feedback will be impartially delivered, honoring the diverse cultural, racial, and gender backgrounds of all students. It will be constructive, emphasizing the task at hand rather than individual characteristics. Labs will be graded within a week to ensure timely feedback and facilitate continuous improvement.

How assignment will be adapted in online format

Lab exercises and review questions will be seamlessly integrated into the online learning environment, allowing students to access instructional materials, perform simulations, and submit assignments electronically. Instructors will leverage virtual communication tools to facilitate discussions, provide feedback, and offer guidance, ensuring that students receive the support they need to succeed in mastering cybersecurity and ethical hacking principles and practices.

Assignment Type

Writing

In-class and/or outside of class

In-class
Outside of class

Formative or Summative

Summative

Assignment

Complete a final project that demonstrates your understanding of cybersecurity ethical hacking concepts and your ability to apply these concepts in real-world scenarios. The final project will involve investigating the security of cryptographic systems by implementing various cryptography attacks to evade the system's security.

Example Final Project: Perform a comprehensive analysis of the security of a cryptographic system. This analysis should include identifying potential vulnerabilities in codes, ciphers, cryptographic protocols, or key management schemes. Implement various cryptography attacks, such as brute force attacks, chosen plaintext attacks, or man-in-the-middle attacks, to exploit these vulnerabilities and evade the system's security measures. Document the process, including the rationale behind attack choices, methodologies used, and the outcomes of the attacks.

Grading and Feedback: The final project will be assessed based on several criteria. Firstly, the technical completeness and correctness of the cryptography attacks implemented will be evaluated, considering the accuracy and effectiveness of the chosen methodologies. Additionally, the depth of the analysis in identifying vulnerabilities and exploiting them will be examined to gauge the thoroughness of the investigation. Furthermore, the quality of the project report will be assessed, ensuring it is comprehensive, well-structured, and meticulously documented, including the rationale behind attack choices and methodologies used. For projects that require a presentation, clarity, confidence, and the ability to articulate attack methodologies and outcomes will be considered. Feedback provided will be objective, unbiased, and tailored to recognize the diverse backgrounds and perspectives students bring to their projects. Ultimately, the final project will be graded by finals week, taking into account these aspects to provide a comprehensive evaluation of the students' understanding and application of cybersecurity ethical hacking concepts.

How assignment will be adapted in online format

The final project will be submitted through the course management system, along with any supporting documentation and files. Students will be encouraged to collaborate and discuss their projects with their peers via discussion boards and video conferencing tools. Instructors will provide feedback and guidance during the project development process, and students will receive a comprehensive evaluation of their final submission, including feedback on both technical and documentation aspects.

Assignment Type

Reading

In-class and/or outside of class

Outside of class

Formative or Summative

Formative

Assignment

Background: In the realm of cybersecurity, the terms "black hat" and "white hat" have become entrenched, a legacy borrowed from old Western films. While seemingly innocuous, these terms create a problematic narrative that hinders diversity and equity within the field. The color association is key here. Historically, Western movies used black hats to signify villains and white hats for heroes, often perpetuating racial stereotypes where dark skin equated to criminality and white skin symbolized righteousness.This translates poorly to cybersecurity. Black hat hackers, the malicious actors, can devastate individuals by stealing personal information or disrupting critical infrastructure. However, the term "black hat" unintentionally implies that the hacker themself is bad because of their skin color, not their actions. White hat hackers, the ethical defenders, work to prevent these attacks. Yet, "white hat" creates an unattainable standard, potentially discouraging diverse talent from entering a field already struggling with inclusion.Shifting to "ethical hacker" and "unethical hacker" dismantles these issues. The focus moves from the color of a metaphorical hat to the hacker's actions and their impact. This fosters a more inclusive environment that welcomes a wider range of skilled individuals, ultimately strengthening cybersecurity for everyone. It's a crucial step towards a more equitable digital landscape, one where the color of a hat doesn't overshadow the true fight against cybercrime.

1. Diversity and Terminology: The terms "black hat" and "white hat" have historically been used in cybersecurity to differentiate between malicious and ethical hackers. However, critics argue these terms have negative connotations. Consider the following:
How might the color association of "black hat" with negativity reinforce racial stereotypes?
Propose alternative terms for "black hat" and "white hat" that are more inclusive and focus on the hacker's actions rather than implied race.
How can these alternative terms create a more welcoming environment for underrepresented groups in cybersecurity?
2. DEI and Recruitment: Cybersecurity suffers from a lack of diversity, which can hinder creativity and lead to blind spots in security measures. The "black hat/white hat" terminology might contribute to this problem. Explain how the following factors could be discouraging diverse talent from entering cybersecurity:
The potential for racial bias associated with the terminology.
The "white hat" concept of a flawless hero, which can be intimidating for newcomers..
How can we reframe cybersecurity careers in a way that is more approachable and attracts a wider range of individuals?
3. Inclusive Solutions: "Black hat" and "white hat" hackers represent different ends of a spectrum in cybersecurity. However, focusing solely on color can overshadow the complexity of the issue.
Discuss how the "black hat/white hat" terminology might downplay the varying motivations of hackers (e.g., financial gain vs. social activism).
How can we move beyond this binary and have a more nuanced conversation about the different types of hackers and their impact on cybersecurity?
Propose solutions to create a more inclusive cybersecurity landscape that values diverse perspectives and skillsets.

Reading: "Toward anti-racist technical terminology" by Patricia Hswe et al.

Criteria for Evaluation: Grading and feedback by following criteria
1. Understanding of Diversity and Bias:
Does the response demonstrate an awareness of the potential for racial bias inherent in the "black hat/white hat" terminology?
Does it acknowledge the negative impact this terminology can have on underrepresented groups entering cybersecurity?
2. Creativity and Inclusivity:
Does the response propose alternative terms for "black hat" and "white hat" that are more inclusive and focus on the hacker's actions?
Does it outline solutions to create a more welcoming environment for diverse talent within cybersecurity?
Does the response discuss how to reframe cybersecurity careers in a way that is more approachable?
3. Nuanced Understanding of Hackers:
Does the response acknowledge the limitations of the "black hat/white hat" binary in representing the motivations of hackers?
Does it propose ways to have a more nuanced conversation about the different types of hackers and their impact?
Does the response consider motivations beyond just malicious intent (e.g., financial gain) and ethical good (social activism)?
Bonus Points:
Demonstrating knowledge of existing efforts to promote diversity and inclusion within cybersecurity.
Proposing additional solutions beyond alternative terminology to create a more inclusive cybersecurity landscape.

How assignment will be adapted in online format

This assignment will be conducted through an online discussion board. Students will access the provided reading material via the course management system (CMS). They will be required to engage in discussions on the CMS, sharing their analysis of the assigned reading and proposing alternative terminology. Feedback will be provided by grading the discussion board posts through the CMS.

Course Materials

Textbooks

CompTIA Pentest+ Guide To Penetration Testing
by Rob S. Wilson
1st Edition | Copyright 2024
ISBN-13: 9780357950654

Class Size Information

Class Size

35

Class Size Category

B - Facilitated learning 35

Diversity and Inclusion

Explain how diversity and inclusion(e.g., gender, culture/race, sexuality, etc.) is infused into the course.

Our Cybersecurity Ethical Hacker course fosters a diverse and inclusive learning environment. We recognize the importance of creating a welcoming and respectful space for students from all backgrounds, including gender, culture, race, and sexual orientation. We achieve this by strategically integrating diversity and inclusion throughout the curriculum. This approach ensures students not only develop their technical expertise but also gain a deep understanding of how to build inclusive and equitable cybersecurity systems and networks in their future careers. For example, Chetan Nayak has significantly contributed to ethical hacking through his pioneering research in vulnerability analysis and exploitation techniques.

Describe how assignments, instruction, evaluation, course content, and interactions are contextualized for diverse learners promoting an equitable course.

Representation in course materials: We'll build a curriculum that celebrates diversity! We'll include a variety of people and groups from different cultures, races, and economic backgrounds. Stories, examples, and pictures will showcase their accomplishments and viewpoints. This inclusive approach will create a welcoming classroom where everyone feels seen, valued, and connected to the material. It's all about belonging! For example the course content includes the following selections:
#Explore the historical context contributing to the adoption of racially-charged terminology.
#Recognize its implications on diversity and inclusion within the ethical hacking community.
#Evaluate the ethical considerations associated with its use.

Real-world scenarios: Get hands-on with real-world hacking scenarios that impact different communities. Through projects and assignments, you'll discover why ethical hacking needs to consider diverse perspectives to build stronger defenses for everyone.

Addressing bias and stereotypes: This Ethical Hacking course will delve into unconscious biases and stereotypes that can exist within cybersecurity. We'll explore how these biases can impact areas like system administration and network security. By bringing these issues to light, students will gain awareness of their own biases and work towards creating a more equitable and inclusive professional environment.

Encouraging diverse perspectives: Our Cybersecurity Ethical Hacking course will promote a culture of diversity and inclusion through group discussions, collaborative projects, and peer evaluations. These activities will encourage students to share their unique perspectives and experiences within cybersecurity. By fostering open-mindedness and empathy, this approach will help students understand the critical role diversity plays in effective security administration and network management.

Cultivating an inclusive learning environment: In my Cybersecurity Ethical Hacking course, we'll prioritize a safe and supportive learning environment where everyone feels comfortable sharing ideas freely. This means establishing clear expectations for respectful interaction, offering anonymous feedback channels, and maintaining a zero-tolerance policy for bias or discrimination. By fostering open communication and valuing diverse perspectives, we'll not only cultivate a positive learning experience but also gain a deeper understanding of the importance of inclusivity in effective cybersecurity practices.

Interactions

Explain how the course will incorporate student-to-student interaction.

a. Collaboration: Facilitate student-to-student interaction by encouraging students to engage in the "Student Lounge" forum or designated discussion areas on the CMS. Through the formative ethical hacking lab assignment, guide students to share their

progress, insights, and challenges, particularly in tasks such as defining assessment scope and negotiating rules of engagement. Encourage them to discuss methods and offer troubleshooting advice to foster a supportive learning community.
b. Interactive Classroom Activities: Organize virtual group discussions or small breakout sessions centered around specific tasks in the ethical hacking lab exercises. Instruct students to collaborate and compare approaches to different assessment techniques, such as footprinting. This promotes critical thinking and reinforces teamwork by allowing students to learn from their peers' methods.
c. Online Discussion Forums: Set up forums for discussions specific to each assignment. Guide students to use these spaces to share findings and methodologies, whether for ethical hacking tasks or cryptographic analysis. Encourage them to post about challenges and solutions, particularly in selecting and implementing cryptographic attacks, so they benefit from diverse perspectives and collaborative problem-solving.

Explain how the course will incorporate instructor-to-student interaction.

a. Course Introduction Package: Prepare a welcome package to introduce both the ethical hacking lab exercises and the cryptographic final project, outlining assessment criteria and available resources. Include an orientation video that explains how students can expect to receive support and guidance throughout these assignments.
b. Weekly Course Updates: Use the CMS to provide weekly announcements focused on the progress and requirements of both assignments. Share insights on troubleshooting techniques for lab exercises or tips for implementing cryptographic attacks, ensuring students stay on track with assignment milestones.
c. Unit Discussions & Support: Maintain discussion boards dedicated to each assignment, responding promptly to student queries about technical challenges or assignment instructions. Provide clarification and feedback on their approaches, especially related to identifying vulnerabilities in labs or selecting methodologies in the final project.
d. Multiple Support Options: Hold regular office hours to offer additional, one-on-one support for students working on lab tasks or the cryptography project. Encourage students to seek help with specific assignment challenges or to discuss their project strategies. Emphasize accessibility and support so students feel guided in applying course concepts.

Explain how the course will incorporate student-to-content interaction.

a. Engaging Lectures: Develop lecture content that aligns directly with the skills required for both assignments. Focus on providing practical examples relevant to ethical hacking and cryptographic methods, integrating embedded quizzes that allow students to gauge their understanding of material tied directly to these assignments.

b. Supplemental Video Library: Curate a video library with content relevant to the lab exercises and final project. Include videos that provide visual guidance on topics such as footprinting and cryptographic attacks, enabling students to deepen their understanding of key concepts required for assignment completion.

c. Assessment Support: Provide access to practice questions and resources that build foundational skills for both assignments. Incorporate automated feedback to help students reinforce core competencies, preparing them for the practical applications required in lab exercises and the cryptographic analysis project.

Explain how the course will incorporate student-to-self interaction (metacognitive).

a. Self-Reflection for Growth: Encourage students to complete reflection prompts following each lab exercise and upon submission of the cryptographic analysis project. Guide them to assess their understanding, pinpoint challenges, and reflect on their learning progress, promoting critical self-assessment.

b. Unlocking Creativity: Encourage students to explore diverse problem-solving approaches in both assignments. Prompt them to think creatively as they work through the ethical hacking tasks and choose methodologies in cryptographic analysis. Use reflection prompts to help them evaluate their choices and strategies, reinforcing adaptability and innovation in cybersecurity problem-solving.

Key: 1064