IT-2720: ETHICAL HACKING AND SYSTEMS DEFENSE

Cuyahoga Community College

Viewing: IT-2720 : Ethical Hacking and Systems Defense

Board of Trustees:

December 2023

Academic Term:

Fall 2024

Subject Code

IT - Information Technology

Course Number:

2720

Title:

Ethical Hacking and Systems Defense

Catalog Description:

Combines an ethical hacking methodology with the application of security tools to better help students secure systems. Includes an introduction to common countermeasures that effectively reduce and/or mitigate attacks.

Credit Hour(s):

3

Lecture Hour(s):

2

Lab Hour(s):

2

Requisites

Prerequisite and Corequisite

ITNT-2370 Network Security Fundamentals, and ITNT-2320 Network Administration I, and ITNT-2380 Linux Administration.

Outcomes

Course Outcome(s):

Utilize security tools in accordance with ethical hacking methodology to improve system security.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Explore the history and current state of hacking and penetration testing, including ethical and legal implications.
2. Identify methods that attackers use to obtain unauthorized access.
3. Describe methods that attackers use to alter systems and cover their tracks.
4. Identify basic equipment controls, physical area controls, and facility controls.
5. Identify common information-gathering tools and techniques.
6. Analyze how port scanning and fingerprinting are used by hackers.
7. Analyze how enumeration is used in conjunction with system hacking.
8. Analyze wireless network vulnerabilities exploited by hackers.
9. Identify common types of malware.
10. Identify Trojans, backdoors, and covert communication methods.
11. Perform network traffic analysis and sniffing by using appropriate tools.

Course Outcome(s):

Students are introduced to common countermeasures that effectively reduce and/or mitigate attacks.

Essential Learning Outcome Mapping:

Not Applicable: No Essential Learning Outcomes mapped. This course does not require application-level assignments that demonstrate mastery in any of the Essential Learning Outcomes.

Objective(s):

1. Perform incident handling by using appropriate methods.
2. Compare and contrast defensive technologies.
3. Describe methods that attackers use to alter systems and cover their tracks.
4. Identify common information-gathering tools and techniques.
5. Analyze wireless network vulnerabilities exploited by hackers.
6. Identify Trojans, backdoors, and covert communication methods.

Methods of Evaluation:

Evaluation can include any combination of the following:

1. Assignments
2. Quizzes
3. Exams
4. Lab Assignments
5. Projects
6. Reports
7. Oral Evaluation

Course Content Outline:

1. History and current state of hacking and penetration testing
    a. Profiles of hackers and cybercriminals
    b. History of computer hacking
    c. Common hacking methodologies
    d. Ethical hacking and penetration testing in relation to black-hat and white-hat activities
    e. Laws and ethical standards for penetration testers and ethical hackers
2. Basic equipment controls, physical area controls, and facility controls.
    a. The role of physical security
    b. Common physical controls
    c. Personal safety controls
    d. Physical access controls
    e. Avoiding common threats to physical security
    f. Defense in depth
3. Common information-gathering tools and techniques.
    a. Footprinting with the information-gathering process
    b. Exploiting insecure applications
    c. Using countermeasures
4. Hackers use of port scanning and fingerprinting are used by hackers
    a. Identification of target systems
    b. Port and vulnerability scanning techniques
    c. Network mapping tools
5. Use of enumeration is used in conjunction with system hacking
    a. Process of enumeration, system hacking, and password cracking
    b. Tools used to perform enumeration
    c. Privilege escalation
    d. Importance of covering tracks
6. Wireless network vulnerabilities exploited by hackers
    a. Wireless security
    b. Wireless technologies
    c. Threats and countermeasures
    d. Wireless network protection plan
7. Web and database attacks.

    a. Web server vulnerabilities, tools, and exploits
    b. Web application vulnerabilities, tools, and exploits
    c. Database attacks and attack tools

8. Common types of malware
    a. Types of malware
    b. Applicable laws
    c. Malware identification techniques, installation, tracking, and removal
9. Appropriate tools for network traffic analysis and sniffing
    a. Network sniffing and traffic analysis
    b. Session hijacking
    c. Denial of service (DoS)
    d. Botnets
10. Common social engineering attacks.
    a. Types of social engineering attacks
    b. Common social engineering scams
    c. Best practices and preventive measures
11. Appropriate methods for incident handling
    a. Basic concepts of incident response
    b. Best practices and procedures for incident reporting
    c. Investigative procedure
12. Defensive technologies.
    a. Intrusion detection/prevention systems
    b. Firewalls and other detection methods
13. Methods that attackers use to obtain unauthorized access to information systems.
    a. Weaknesses and vulnerabilities in targets
    b. Passive reconnaissance of targets
    c. Tools utilized for active reconnaissance
    d. The tools and techniques used in exploitation
    e. Attack vectors hackers pursue
14. Methods that attackers use to pillage their victims and to persist in their environment
    a. Accounts
    b. Processes
    c. Back doors and data exfiltration
    d. System alteration and cleanup

Resources

Ciampa, M. *CompTIA Security+ guide to network security fundamentals*. Seventh. Boston: Cengage, 2022.

Wilson, R., Simpson, M., & Antill, N. *Hands-on ethical hacking & network defense*. Fourth. Boston: Cengage, 2023.

Solomon, M. & Oriyano, S. *Ethical hacking: Techniques, tools, and countermeasures*. Fourth. Burlington, MA: Jones & Bartlett Learning, 2024.

Top of page
Key: 2515