Course Description

CIS4378 | Ethical Hacking II | 4.00 credits

This upper division course is a continuation of Ethical Hacking I. Students will focus on how web applications, wireless networks, and mobile platforms can be hacked, and how intrusion detection systems (IDS), firewalls and honeypots can be evaded. Other topics include cloud computing security, Internet of Things (IoT) security, and cryptography. Prerequisite: CIS4204.

Course Competencies:

Competency 1: The student will be able to demonstrate an understanding of web server hacking by:

1. Describing the components of a web server
2. Listing popular web servers
3. Describing web server authentication and access control features
4. Identifying common web server vulnerabilities, including DNS Server hijacking, DDoS, directory traversal, man-in-the-middle, HTTP response splitting, web cache poisoning, and sniffing attacks
5. Identifying the vulnerabilities specific to IIS servers
6. Defining patch management and patch management tools
7. Demonstrating tools used to attack web servers

Competency 2: The student will be able to demonstrate an understanding of web applications hacking by:

1. Describing the architecture of web applications, web services, and service-oriented architecture
2. Describing web application technologies, including the HTTP protocol methods and codes, AJAX, XML, JSON, and various encoding schemes
3. Describing web authentication techniques and protocols, including cookie-based authentication, token-based authentication, Oauth, OpenID, and SAM
4. Describing web authorization techniques and protocols, including Oauth2 and SAML
5. Explaining common web server threats, such as injections, broken authentication, data exposure, XML External Entity (XXE), cross-site scripting (XSS), Cross-Site Request Forgery (CSRF), and Cookie/session Poisoning
6. Describing web browser hacking methods
7. Analyzing web applications to map the attack surface
8. Using vulnerability assessment tools to identify web servers' vulnerabilities
9. Using fuzzy testing to identify web application coding errors and security loopholes.
10. Performing documentation review and source code review to identify vulnerabilities in the code that traditional scanning tools, including application logic flaws, cannot identify
11. Describing recent attack threats

Competency 3: The student will be able to demonstrate an understanding of SQL injections by:

1. Defining and explaining SQL injections
2. Comparing various SQL injection types, including UNION SQL injections, Error-based SQL injections, blind and double-blind SQL injections
3. Explaining how SQL injections can be used to bypass authentication
4. Using SQL injection tools to find and exploit SQL injection vulnerabilities
5. Using fuzzy testing to detect SQL injection vulnerabilities
6. Using static and dynamic source code analysis to detect SQL injection vulnerabilities
7. Using intrusion detection systems (IDS) evasion techniques to perform SQL injections that bypass IDS

Competency 4: The student will be able to demonstrate an understanding of session hijacking by:

1. Describing session management and session hijacking
2. Explaining how session hijacking can be used to bypass authentication
3. Characterizing the application-level session hijacking attacks, including CSRF, session replay, man-in- the-browser, session fixation, proxy servers, and SSL/TLS-related attacks
4. Explaining network-level session hijacking attacks such as TCP/IP hijacking, Blind hijacking, man-in-the-middle, and RST hijacking
5. Performing sequence number prediction
6. Listing the steps in conducting a session hijacking attack
7. Using session hijacking tools
8. Describing approaches to prevent session hijacking

Competency 5: The student will be able to demonstrate an understanding of IDS, firewalls, and honeypots evasion by:

1. Describing the types of IDS and intrusion prevention systems (IPS)
2. Explaining the types of IDS evasion techniques
3. Using tools to evade IDS
4. Specify methods to detect IDS attacks
5. Explaining strategies to defend against IDS evasion
6. Comparing the types of firewalls
7. Explaining methods to identify and bypass a firewall
8. Describing honeypots and honeynets
9. Explaining methods to detect and defeat honeypots

Competency 6: The student will be able to demonstrate an understanding of wireless networks hacking by:

1. Defining and differentiating types of wireless technologies
2. Listing the advantages and disadvantages of a wireless network
3. Comparing and contrasting wireless standards
4. Identifying wireless access points
5. Listing wireless threats, including disassociation attacks, EAP-failure, beacon flood, rogue access point, evil twin, key reinstallation attack (KRACK), jamming, etc
6. Explaining Bluetooth threats
7. Describing Wired Equivalent Privacy (WEP) vulnerabilities
8. Describe Wi-Fi Protected Access (WPA) and its vulnerabilities
9. Describe Wi-Fi Protected Access 2 (WPA2) and its vulnerabilities
10. Using tools to scan, sniff, and attack wireless networks
11. Listing countermeasures to wireless attacks

Competency 7: The student will be able to demonstrate an understanding of mobile platform hacking by:

1. Describing the types of handheld devices and their operating systems
2. Describing mobile attack vectors and vulnerabilities, including jail-broken and rooted devices, app sandboxing vulnerabilities, mobile spam, SMS phishing attacks, etc
3. Describing methods used to hack handheld devices
4. Describing mobile device management policies and solutions
5. Using tools to defend against handheld devices attacks

Competency 8: The student will be able to demonstrate an understanding of Internet of Things (IoT) hacking by:

1. Defining and describing the IoT
2. Explaining the IoT architecture and IoT communication models

3. Listing IoT technologies and protocols
4. Explaining the vulnerabilities associated with the IoT
5. Describing the IoT attack surface
6. Explaining various IoT threats, including rolling code attacks, blue-borne attacks, firmware exploits, and Sybil attacks
7. Using tools and devices to hack IoT devices
8. Listing strategies and tools to defend against IoT attacks

Competency 9: The student will be able to demonstrate an understanding of cloud computing hacking by

1. Describing the characteristics of cloud computing, including on-demand self-service, rapid elasticity, resource pooling, and virtualization
2. Comparing various virtualization platforms
3. Comparing the types of cloud computing (IaaS, PaaS and SaaS)
4. Explaining the separation of responsibilities in the cloud
5. Describing the cloud deployment models (public, private, community, hybrid)
6. Describing the National Institute of Standards and Technology (NIST) Cloud Deployment Reference Architecture
7. Understanding shared storage options
8. Listing and explaining cloud computing threats, including VM-level attacks, lock-in, loss of governance, and loss of encryption keys
9. Describing cloud computing attacks
10. Describing cloud computing security considerations and the cloud security control layers
11. Using cloud security tools to test cloud-based systems

Competency 10: The student will be able to demonstrate an understanding of cryptographic attacks by:

1. Distinguishing secret-key cryptography from public-key cryptography
2. Explaining cryptographic hashing functions
3. Describing the RSA algorithm
4. Defining Secure Socket Layer (SSL) and identifying its uses
5. Describing the Secure Shell (SSH) protocol
6. Distinguishing types of cryptographic attacks
7. Using encryption-cracking tools

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Formulate strategies to locate, evaluate, and apply information
- Use computer and emerging technologies effectively