Course Description

CIS4204 |Ethical Hacking I | 4.00 credits

This upper division course introduces students to penetration testing techniques. The student will learn how to footprint, scan, and enumerate networks, how to hack web applications, wireless networks, and mobile platforms, and how to evade IDS, firewalls and honeypots. Other topics include denial of service attacks, social engineering, malware and relevant laws. Prerequisite: CIS3360.

Course Competencies:

Competency 1: The student will be able to demonstrate an understanding of the field of ethical hacking by:

1. Describing the role of an ethical hacker
2. Explaining the legal aspects of penetration testing
3. Describing penetration testing methodologies, including the flaw hypothesis methodology (white box, grey box, black box) and OSSTMM
4. Listing the steps in a typical cyberattack
5. Understanding families of attacks such as denial of service attacks, password attacks, social engineering, malware, etc

Competency 2: The student will be able to demonstrate an understanding of the foot printing step by:

1. Describing the foot printing step in penetration testing
2. Using search engines, social networking sites, websites, and domain name system zone transfers to perform foot printing
3. Explaining how to conduct competitive intelligence
4. Performing active and passive foot printing on an organization
5. Using tools to find the Internet footprint of an organization (IP addresses, host, subdomains)

Competency 3: The student will be able to demonstrate an understanding of social engineering by:

1. Defining social engineering
2. Identifying the behaviors vulnerable to attacks
3. Listing the types of social engineering
4. Defining identity theft

Competency 4: The student will be able to demonstrate an understanding of the network scanning step by:

1. Describing the scanning step in penetration testing
2. Explaining what ping sweeps are used for
3. Comparing the different types of port scans
4. Using port-scanning tools such as nmap and hping3

Competency 5: The student will be able to demonstrate an understanding of the enumeration step by:

1. Describing the enumeration step in penetration testing
2. Describing the NetBIOS system
3. Describing SNMP
4. Using windows enumeration tools
5. Using UNIX\Linux enumeration tools

Competency 6: The student will be able to demonstrate an understanding of vulnerability analysis by:

1. Defining vulnerability
2. Defining vulnerability research and vulnerability assessment
3. Defining attack surface
4. Performing threat modeling
5. Describing the vulnerability assessment lifecycle, including baseline creation, vulnerability mapping, risk

assessment, and remediation using effective mitigation strategies, verification, and monitoring

6. Explaining vulnerability scoring systems and identifiers (CVSS, CVE, NVD)
7. Explaining vulnerability assessment approaches
8. Using vulnerability and exploit databases
9. Understanding flaws that lead to vulnerabilities such as buffer overflow, SQL injection, cross-site scripting, and cross-site request forgery
10. Using tools to perform vulnerability assessment on a simple network
11. Explaining when vulnerabilities must be disclosed

Competency 7: The student will be able to demonstrate an understanding of the exploitation and obfuscation steps by:

1. Comparing methods to crack passwords
2. Using password cracking tools
3. Listing privilege escalation techniques
4. Explaining buffer overflow attacks, including stack smashing, heap overflow, and return-oriented programming
5. Using tools to execute applications remotely
6. Using tools such as keyloggers, steganography, spyware, and rootkits to hide files and cover tracks

Competency 8: The student will be able to demonstrate an understanding of malware by:

1. Comparing the different types of malwares
2. Listing the different ways malware can get into a system
3. Describing the components of malware
4. Distinguishing between overt and covert channels
5. Constructing and delivering malware using construction and exploit kits
6. Summarizing the history of viruses and worms
7. Identifying the basic symptoms of a virus attack
8. Describing the lifecycle of viruses
9. 9. Using tools and techniques to detect, diagnose, and combat viruses

Competency 9: The student will be able to demonstrate an understanding of sniffing by:

1. Differentiating types of sniffing attacks
2. Describing the switch port analyzer (SPAN)
3. Defining lawful intercept
4. Using tools for ARP spoofing
5. Using MAC flooding tools
6. Defining DNS poisoning
7. Using tools to detect sniffing

Competency 10: The student will be able to demonstrate an understanding of denial-of-service attacks by:

1. Defining denial-of-service attacks
2. Comparing the types of denial-of-service attacks and their impact
3. Explaining distributed denial-of-service techniques
4. Explaining reflected denial-of-service techniques
5. Define bots and their uses
6. Explaining DoS/DDoS mitigation strategies and countermeasures

Learning Outcomes

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