CHT A282: ETHICAL HACKING AND NETWORK DEFENSE

Item	Value
Curriculum Committee Approval Date	10/20/2021
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	72 Total Hours (Lecture Hours 45; Lab Hours 27)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Students will learn how hackers attack computers and networks, and how to protect Windows and Linux systems. Legal restrictions and ethical guidelines will be taught and enforced. Students will perform many hands-on labs; attacking and defending, using port scans, footprinting, buffer overflow exploits, SQL injection, privilege escalation, Trojans, and backdoors. ADVISORY: CHT A191, IT A191 or CIS A191; and CHT A261, IT A261 or CIS A261. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Demonstrate in project format the use of the differing technologies, protocols and tools to secure wired and wireless networks.
2. Design, implement, document, and explain in project format a solution to protect a real-world business network.

Course Objectives

- 1. Explain what an ethical hacker can and can not do legally, and explain the credentials and roles of penetration testers.
- 2. Define the types of malicious software found in modern networks.
- 3. Explain the threats and countermeasures for physical security and social engineering.
- 4. Perform footprinting to learn about a company and its network.
- 5. Perform port scans to locate potential entry points to servers and networks.
- 6. Perform enumeration (finding resources, accounts, and passwords) on Microsoft, Netware, and Unix/Linux targets.
- 7. Perform very simple programming in C, HTML, and Perl, specifically oriented towards the needs of network security professionals.
- 8. Identify Microsoft Windows vulnerabilities and to harden systems.
- 9. Identify Linux vulnerabilities and to protect servers.
- 10. Describe how to take control of Web Servers, and how to protect them.
- 11. Locate and hack into wireless networks, and protect them.
- 12. Explain how cryptography and hashing work, and perform attacks against them such as password cracking and man-in-the-middle attacks.
- 13. Describe and deploy security devices, including routers, firewalls, Intrusion Detection Systems, and honeypots.

Lecture Content

1. Network and Computer Attacks Malicious Software (Malware) Protecting Against Malware Attacks Intruder Attacks on Networks and Computers Addressing Physical Security 2. Footprinting and Social Engineeering Using Web Tools for Footprinting Conducting Competitive Intelligence Using Domain Name Service (DNS) Zone Transfers Social Engineering 3. Port Programming for Security Types of Port Scanning Using Port Scanning Tools Conducting Ping Sweeps Understanding Shell Scripting for Security 4. Enumeration Enumerating Microsoft Operating Systems Enumerating the Unix/Linux Operating Systems 5. Microsoft Operating System Vulnerabilities Tools to Identify Vulnerabilities on Microsoft Systems Microsoft Operating System Vulnerabilities Vulnerabilities in Microsoft Services Best Practices for Hardening Microsoft Systems 6. Linux Operating System Linux Operating System Vulnerabilities Remote Access Attacks on Linux Systems Countermeasures Against Linux Remote Attacks 7. Hacking Web Understanding Web Applications and Vulerabilities Tools of Web Attackers and Security Testers 8. Hacking Wireless Understanding Wireless Network Standards Understanding Authentication Understanding Wardriving Understanding Wireless hacking Cracking WEP Encryption Man-in-the-Middle Attacks 9. Cryptography Cryptography Basics Symmetric and Asymmetric Algorithms Public Key Infrastructure (PKI) Understanding Cryptography Attacks 10. Protecting Networks with Security Understanding Network Security Devices Understanding Firewalls Understanding Intrusion Detection Systems (IDSs) Understanding Honeypots

Lab Content

Project 1: Preparing Windows 7 Target and Kali Linux Virtual Machine Project 2: Taking Control of a Windows Machine with Armitage Project 3: Port Scans and Firewalls Project 4: Analyzing Types of Port Scans Project 5: Creating Infectious Media with Metasploit Project 6: TCP Handshake with Scapy Project 7: Cookie Replay Project 8: Cracking Linux Password Hashes with Hashcat Project 9: Programming in C on Linux Project 10: HTTP Basic Authentication Project 11: PicoCTF Project 12: Attacking Apache with the OWASP HTTTP DoS Tool Project 13: Attacking Apache with the OWASP HTTTP Dos Tool Project 14: yesman Honeypot with Scapy Project 15: Cracking Windows Passwords with Cain and Abel Project 16:SQL Injection Challenges Project 17: Hijacking HTTPS Sessions with SSLstrip

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

Lecture and application of ideas Students will be presented material from several different sources, including, but not limited to study guides, “Web-based” curriculum, in-class demonstrations of systems integration and personal experiences of industry professionals.Individual and paired exercises During the lab portion of the class, students will be required to perform many of the tasks of a network administrator. In order to complete several projects, students will need to work together in teams to build working local area networks.Interactive computer-based assignments Using computer and “Web-based” training tools, students will be working on simulated networks in order to solve problems.

Reading Assignments

Minimum of 3 hours per week (45 hours) reading from textbook material.

Writing Assignments

Program and configure a set of routers to create a simulated Wide Area Network (WAN) infrastructure.Given a minimum set of requirements, the student will design a recommended solution accommodating routing technologies using some combination of hardware and software. After the solution is designed, the student will create a presentation describing the results. Minimum of 3 hours per week creating and editing class and software projects.

Out-of-class Assignments

45 hours (3hrs/wk). Student performance on quizzes, tests, including short essays, and laboratory assignments will be used to determine proficiency

Demonstration of Critical Thinking

Reading and writing assignments Web-based research Term or other paper(s) Laboratory reports Problem solving demonstrations Exams Homework problems Skill demonstrations Performance exams Case study presentations Objective examinations, including Multiple-choice True/false Completion

Required Writing, Problem Solving, Skills Demonstration

Program and configure a set of routers to create a simulated Wide Area Network (WAN) infrastructure. Given a minimum set of requirements, the student will design a recommended solution accommodating routing technologies using some combination of hardware and software. After the solution is designed, the student will create a presentation describing the results.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Simpson, Michael T. . Hands-On Ethical Hacking and Network Defense, 3rd ed. Boston: Cengage Learning, 2017 Rationale: -