CONTINUING EDUCATION
Course Outline

Threat Analysis: Ethical Hacking Prep Certificate

Now, more than ever, organizations need to eliminate vulnerabilities and protect their customer and confidential data against security breaches. To accomplish this, many companies are turning to ethical hackers/pen-testers to evaluate the security of an IT infrastructure by safely exploiting vulnerabilities that may exist in operating systems, services, applications, network components etc., and recommend solutions to improve overall security posture.

In this online course, you'll gain the ethical hacking knowledge to conduct a threat assessment; secure a network across popular platforms and operating systems; work with various types of threats and intrusion detection systems; and establish auditing and monitoring systems for vulnerabilities and threats.

Who Should Take This Course

This course is designed for anyone who is concerned about or responsible for the integrity of the network infrastructure, including those studying to become security officers, auditors, security professionals and site administrators.

Course Objectives

- Introduction
- List and explain the attack phases
- Differentiate between threats and defense mechanisms
- Describe and differentiate the types of web application, data server, and network operating system threats
- Implement threats on web applications, data servers, and network operating systems
- Use countermeasure tools on web applications, data servers, and networks operating systems

Course Info

Hours:

Students will spend approximately 15-20 hours per week on this course

Prerequisites:

Good understanding of the Windows and Linux OS command line; solid understanding of networking devices and principles, such as the TCP/IP and OSI stack, routing and switching devices, wireless systems, firewalls and virtual machines; and exposure to information security concepts, such as confidentiality, integrity and authentication.

Instructional Methods:

- **Reading**: Students are expected to read the chapters as directed.
- **Quizzes/Tests**: The quizzes and exams will consist primarily of multiple-choice questions, although other question types may be used. Quizzes will test the student's comprehension of the course content.
    - **Videos**: Students are encouraged to watch videos relevant to weekly content using online media such as You Tube. Instructor will post relevant channels on the Learning Management System.

Course Content

Introduction

- Identify the importance of information security
- Distinguish the elements of security
- Identify the phases of the hacking cycle
- Differentiate types of hacker attacks
- Compare and contrast types of ethical hacking
- Use tools to research and fix security vulnerabilities
- List steps for conducting ethical hacking
- Distinguish between computer crimes and implications

List and explain the attack phases

Footprinting

- Define footprinting of the reconnaissance phase
- Research publicly accessible information from a company's website
- Identify passive and competitive intelligence gathering
- Complete a WHOIS query
- Demonstrate tracing Internet connections for safety and vulnerability issues

Scanning

- Define and name different types of scanning
- List the steps in scanning methodology
- Use scanning tools
- Define banner grabbing
- Describe Operating System fingerprinting
- Draw network diagrams of a vulnerable host
- Differentiate the types and uses of an anonymizer
- Identify scanning countermeasures

Enumeration

- Define enumeration
- Use enumeration techniques and tools
- Differentiate Simple Network Management Protocol (SNMP) enumeration and Management Information Bases (MIBs)
- Identify SNMP tools and enumeration countermeasures

System Hacking

- Identify how to crack passwords

- Use password cracking tools
- Implement countermeasures for password cracking
- Identify escalating privileges
- Execute applications remotely
- Explain keyloggers and keylogger tools
- Identify spyware and countermeasures

Penetration Testing

- Perform penetration testing (PT)
- Identify penetration-testing tools
- Use penetration-testing software
- Evaluate security assessments
- Calculate risk management
- Use manual and automated testing

Differentiate between threats and defense mechanisms

Trojans and Backdoors

- Define Trojans and backdoors
- Summarize the types of Trojans, functions, and indications of Trojan attacks
- Distinguish between overt and covert channels
- Use tools to test for Trojans
- Construct a Trojan horse using a construction kit
- List the steps to detect Trojans and Trojan countermeasures
- List various tools used for sending Trojans
- Identify various anti-Trojans

Viruses and Worms

- Define viruses
- Differentiate between a virus and worm
- Identify the basic symptoms of a virus attack
- Characterize and differentiate types of viruses and worms
- List the phases and life cycle of viruses
- Create a virus program
- Use tools and techniques to detect, diagnose, and combat viruses
- List the steps in a virus incident response

Sniffers

- Define sniffing
- Identify types of sniffing
- Identify protocols vulnerable to sniffing
- Differentiate types of sniffing attacks
- Describe the Switch Port Analyzer (SPAN)
- List tools for ARP spoofing
- Explain MAC flooding tools
- Define DNS poisoning
- Use tools to detect sniffing
- Implement countermeasures for sniffing

Social Engineering

- Define social engineering
- List the types of social engineering
- Classify social engineering threats and defenses
- Implement countermeasures for social engineering
- Develop policies and procedures
- Summarize incidents when using social media
- Define identity theft
- Implement countermeasures for identity theft

Phishing

- Define phishing
- Identify reasons for successful phishing
- Describe phishing methods and compromises
- Discuss phishing attacks and symptoms
- Use anti-phishing tools

Denial of Service

- Define a denial-of-service attack
- Identify the types and impact of denial-of-service attacks
- Explain a distributed denial-of-service attack
- Describe tools that facilitate a denial-of-service attack
- Define bots and their uses
- Identify the taxonomy of a distributed denial-of-service attack
- Define a reflected denial-of-service attack
- List tools that facilitate a distributed denial-of-service attack
- Use tools for detecting denial of service attacks
- Use countermeasures for a distributed denial-of-service attack

Buffer Overflows

- Define and distinguish the types and dangers of buffer overflows
- Explain the reasons for buffer overflow attacks
- Identify a buffer overflow exploit
- Use tools and techniques for buffer overflow countermeasures
- Perform code analysis to find buffer overflow vulnerabilities
- Discuss methods to prevent buffer overflow attacks

Describe/differentiate types of web application, data server, and network operating system threats

Session Hijacking

- Identify occurrences of session hijacks
- List the steps in conducting a session hijacking attack
- Characterize types of session hijacking
- Perform sequence number prediction
- Define TCP/IP hijacking
- Distinguish session hijacking tools
- Use countermeasures for session hijacking

Hijacking Web Servers

- Identify common Web server vulnerabilities
- Define the types of attacks used against Web servers
- Demonstrate tools used in attacking Web servers
- Define patch management
- Use vulnerability scanners
- Utilize tools for web server countermeasures and security

Web Application Vulnerabilities

- Define Web application hacking
- Summarize the steps of an anatomy of an attack
- Differentiate types of Web application threats
- Demonstrate tools for Web application threats
- Utilize tools for Web application countermeasures

Web-based Password-Cracking Techniques

- Discuss the methodology of an attacker using a password cracker
- List different password attacks
- Define a password cracker
- Identify the operation of a password cracker
- Test password-cracking tools
- Implement password-cracking countermeasures

Hacking Web Browsers

- Describe web browser hacking methods for Firefox, Internet Explorer, Opera, and Safari
- Identify Firefox, Internet Explorer, Opera, and Safari browsers' security
- Detect various other security and privacy features

Hacking Database Servers – SQL Injection

- Demonstrate ways to break into an Oracle database
- Identify an Oracle worm
- Define and explain SQL injections
- List the steps for performing SQL injection
- Describe SQL injection techniques and automated tools
- Use security tools to secure and take countermeasures against SQL injection

Implement threats on web applications, data servers, and network operating systems

Hacking Wireless Networks

- Describe Wired Equivalent Privacy (WEP), vulnerabilities, and solutions
- Explain Wi-Fi Protected Access (WPA) and its vulnerabilities
- Identify tools for WEP cracking
- Use tools to scan, sniff, deploy, secure, and troubleshoot wireless networks

Physical Security

- Define physical security
- Differentiate physical security countermeasures--physical, technical, and operational
- Explain and illustrate device locks
- Discuss the challenges in ensuring physical security
- Differentiate between various spyware technologies
- List physical security tools to prevent technology invasion.

Evading IDS, Firewalls, and Detecting Honeypots

- Describe the types intrusion detection systems (IDS)
- Specify methods to detect an IDS attack
- List tools to evade IDS attacks
- Install an intrusion prevention system (IPS)
- Define a firewall, and list the types of firewalls
- Explain methods to protect or bypass a firewall
- Define and describe Honeypots
- Clarify security policies to prevent attacks

Hacking Routers and Cable Modems

- Exploit vulnerabilities in Cisco IOS
- Discuss types of router attacks
- List the steps in cable modem hacking
- Explain types of network attacks
- Evaluate various pen-testing tools
- Discuss security policies to prevent breaches

Linux Hacking

- Describe Linux intrusion detection systems, security, and vulnerabilities
- Explain SARA
- Use tools in Linux
- List Linux countermeasure tools

MAC OS Hacking

- Identify vulnerabilities in the Macintosh OS
- Identify worms and viruses that can infect the Macintosh OS
- List Macintosh OS antivirus software
- Explain Macintosh OS security tools

Hacking Mobile Phones, PDAs, and Handheld Devices

- Explain mobile phone vulnerabilities
- Describe methods used to hack handheld devices
- Describe viruses and antivirus protection for handheld devices
- Use tools to defend handheld device attacks
- Provide mobile phone security tips

Hacking Portable Devices

- Differentiate the types of USB attacks
- List countermeasures to prevent USB virus/worm infections
- Explain Bluetooth security vulnerabilities
- List types of Bluetooth attacks
- Describe security measures of a Bluetooth network
- Name RFID risks
- Specify RFID security, vulnerabilities, and privacy threats
- Implement countermeasures against RFID attacks

Cryptography

- Define and describe types of public-key cryptography and encryptions
- Define Rivet Shamir Adleman (RSA)
- Explain types of algorithms and security
- List message digest functions
- Define Security Sockets Layer (SSL), and identify its uses
- Describe Secure Shell (SSH) protocols
- List code-breaking methodologies
- Distinguish types of cryptography attacks
- Use encryption-cracking tools
- Distinguish encryption countermeasure tools

Assessment/CEU Letter/Certificate of Completion

This course is not assigned a letter or numerical grade. However, there will be assignments, quizzes and tests. Students are expected to complete all assignments, quizzes and tests to receive a Certificate of Completion and/or a CEU letter at the end of the course.

Course Completion/Continuing Education Unit (CEU) Letter

If your company requires proof of course completion, or if you would like to have proof for your own records, you may request a Course Completion/Continuing Education Unit (CEU) letter **after the final session of your course**. You must attend 80 percent of the course (or 100 percent of a single-day course) to qualify for the letter. Attendance is verified through the Sign-in Sheet/Roster. It is your responsibility to sign-in at every session. You can request a Course Completion/CEU letter online.

*Attendance for CEU letters and certificate programs is verified via the sign-in sheets provided at each class session. It is your responsibility to sign-in.

Green River College is committed to providing access to all who visit, work and study on campus. The College will provide reasonable accommodations for individuals with disabilities, with advance notice of need. If you require accommodations, please contact Disability Support Services as soon as possible to determine eligibility and/or request accommodations. Accommodations are determined on a case-by-case basis. Please contact Disability Support by email at dss@greenriver.edu; by phone at 253-833-9111, ext. 2631; TTY 253-288-3359; or in person at the Student Affairs and Success Center, Room 210, to request accommodations. For additional information, please visit **www.greenriver.edu/dss**.

The accommodations authorized on your forms should be discussed with your instructor. All discussions will remain confidential. Accommodations are not provided retroactively, so it is essential to discuss your needs at the beginning of the quarter. Additionally, only accommodations approved by Disability Support Services will be provided. This syllabus is available in alternate formats upon request. Green River College is an equal opportunity educator and employer. Learn more at **www.greenriver.edu/accessibility**.