C)PTE: Penetration Testing Engineer

Course ID #: 7000-782-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course you will cover 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting. Plus, discover the latest vulnerabilities and the techniques malicious hackers are using to acquire and destroy data. Additionally, you will learn more about the business skills needed to identify protection opportunities, justify testing activities and optimize security controls appropriate to the business needs in order to reduce business risk.

Course Objectives:

Upon successful completion of this course, students will:

- Have solid knowledge of testing and reporting procedures which will prepare them for upper management roles within a cybersecurity system
- Be able to competently take the C)PTE exam

Prerequisites:

- C)PEH or equivalent knowledge
- 12 months of Networking Experience
- Sound Knowledge of TCP/IP
- Basic Knowledge of Linux
- Microsoft Security experience

Target Audience:

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Topics:

Module 1 – Business and Technical Logistics of Pen Testing

- What is Penetration Testing?
- Today's Threats
- Staying up to Date
- Pen Testing Methodology
- Pre-Engagement Activities

C)PTE: Penetration Testing Engineer

Course ID #: 7000-782-ZZ-Z

Hours: 35

Module 2 – Information Gathering Reconnaissance- Passive (External Only)

- What are we looking for?
- Keeping Track of what we find!
- Where/How do we find this Information?
- Are there tools to help?
- Countermeasures

Module 3 – Detecting Live Systems – Reconnaissance (Active)

- What are we looking for?
- Reaching Out!
- Port Scanning
- Are there tools to help?
- Countermeasure

Module 4 – Banner Grabbing and Enumeration

- Banner Grabbing
- Enumeration

Module 5 – Automated Vulnerability Assessment

- What is a Vulnerability Assessment?
- Tools of the Trade
- Testing Internal/External Systems
- Dealing with the Results

Module 6 – Hacking Operating Systems

- Key Loggers
- Password Attacks
- Rootkits & Their Friends
- Clearing Tracks

Module 7 – Advanced Assessment and Exploitation Techniques

- Buffer Overflow
- Exploits
- Exploit Framework

Module 8 – Evasion Techniques

- Evading Firewall
- Evading Honeypots
- Evading IDS

Module 9 – Hacking with PowerShell

- PowerShell – A Few Interesting Items
- Finding Passwords with PowerShell

Module 10 – Networks and Sniffing

- Sniffing Techniques

Module 11 – Accessing and Hacking Web Techniques

- OWASP Top 10
- SQL Injection
- XSS

Module 12 – Mobile and IoT Hacking

- What devices are we talking about?
- What is the risk?
- Potential Avenues to Attack
- Hardening Mobile/IoT Devices

Module 13 – Report Writing Basics

- Report Components
- Report Results Matrix
- Recommendations

C)PTE: Penetration Testing Engineer

Course ID #: 7000-782-ZZ-Z

Hours: 35

Labs:

Lab 1 – Introduction to Pen Testing Setup
Lab 2 – Linux Fundamentals
Lab 3 – Using Tools for Reporting
Lab 4 – Information Gathering
Lab 5 – Detecting Live Systems
Lab 6 – Enumeration
Lab 7 – Vulnerability Assessments
Lab 8 – Software Goes Undercover
Lab 9 – System Hacking (Windows)
Lab 10 – System Hacking (Linux)
Lab 11 – Advanced Vulnerability and Exploitation Techniques
Lab 12 – Network Sniffing/IDS
Lab 13 – Attacking Databases
Lab 14 – Attacking Web Applications

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535