C)IHE: Certified Incident Handling Engineer

Course ID #: 7000-778-ZZ-Z

Hours: 35

Course Content

Course Description:

This course will cover understanding how to plan, create and utilize their systems. Prevent, detect and respond to attacks through the use of hands-on labs in our exclusive Cyber Range.

Course Objectives:

Upon successful completion of this course, students will:

- Have knowledge to perform network forensic examinations
- Be able to accurately report on their findings
- Be ready to sit for the C)NFE exam

Prerequisites:

- 12 months network technologies
- Sound knowledge of networking and TCP/IP
- Linux knowledge is essential

Target Audience:

- Penetration Testers
- Microsoft Administrator
- Security Administrators
- Active Directory Administrators
- Anyone looking to learn more about security

Topics:

Chapter 1: Incident Handling Explained

- Introduction
- What is an Incident?
- What is Incident Handling?
- Difference Between IH and IR
- The Incident Response Process
- Seven Reasons You Must Put Together an Incident Response Plan
- How to Build an Effective Incident Response Team
- Considerations for Creating an Incident Response Team
- Tips for Incident Response Team Members

Chapter 2: Incident Response Policy, Plan, and Procedure Creation

- Introduction
- Incident Response Policy
- Incident Response Plan
- Incident Response Procedures
- Sharing Information with Outside Parties

Chapter 3: Incident Response Team Structure

- Introduction Section 2 – Team Models
- Team Model Selection Section 4 – Incident Response Personnel
- Dependencies within Organizations

C)IHE: Certified Incident Handling Engineer

Course ID #: 7000-778-ZZ-Z

Hours: 35

Chapter 4: Incident Response Team Services
- Introduction
- Intrusion Detection
- Advisory Distribution
- Education and Awareness
- Information Sharing

Chapter 5: Incident Response Recommendations
- Introduction
- Establish a formal Incident Response Capability
- Establish Information Sharing Capabilities
- Building an Incident Response Team

Chapter 6: Preparation
- Introduction
- Tools and Toolkits
- Policy
- Procedures
- Preventing Incidents

Chapter 7: Detection and Analysis
- Attack Vectors
- Signs of an Incident
- Sources of Precursors and Indicators
- Incident Analysis
- Incident Documentation
- Incident Prioritization
- Incident Notification

Chapter 8: Containment, Eradication, and Recovery
- Selecting the Right Containment Strategy
- Gathering and Handling Evidence
- Identifying the Attacking Hosts
- Eradication and Recovery

Chapter 9: GRR Rapid Response
- Introduction
- What is GRR?
- Installing GRR Server
- Deploying GRR Clients
- Investigating with GRR

Chapter 10: Request Tracker for Incident Response
- Introduction
- Request Tracker
- Request Tracker for Incident Response

Chapter 11: Post-Incident Activity
- Introduction
- Lessons Learned
- Using Collected Incident Data
- Evidence Retention

Chapter 12: Incident Handling Checklist
- Introduction
- Building Checklists

Chapter 13: Incident Handling Recommendation
- Introduction
- Recommendations

Chapter 14: Coordination and Information Sharing
- Introduction
- Coordination
- Information Sharing Techniques
- Granular Information Sharing
- Sharing Recommendations

C)IHE: Certified Incident Handling Engineer

Course ID #: 7000-778-ZZ-Z

Hours: 35

Labs:

Lab 1: Identifying Incident Triggers
Lab 2: Drafting Incident Response Procedures
Lab 3: Planning for Dependencies
Lab 4: Testing Your Plan
Lab 5: Acceptable Use Policy
Lab 6: Practice Attack Vectors
Lab 7: Deploy GRR Client
Lab 8: Create Request Tracker Workflow
Lab 9: GRR Rapid Response
Lab 10: Create a Checklist
Lab 11: Drafting Response Improvement Recommendations
Lab 12: Sharing Agreements

C)IHE: Certified Incident Handling Engineer

Course ID #: 7000-778-ZZ-Z

Hours: 35

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