Cybersecurity Foundations (CyberFound)

Code: 9701
Length: 5 days
URL: View Online

In this cybersecurity course, you will gain a global perspective of the challenges of designing a secure system, touching on all the cyber roles needed to provide a cohesive security solution. Through lecture, labs, and breakout discussion groups, you will learn about current threat trends across the Internet and their impact on organizational security. You will review standard cybersecurity terminology and compliance requirements, examine sample exploits, and gain hands-on experience mitigating controls. In a contained lab environment, you will work with live viruses, including botnets, worms, and Trojans.

Skills Gained

- Current cyber threats and cybersecurity site references
- Government-mandated directives and compliance requirements
- Cyber roles required to successfully design secure systems
- The attack cycle perpetrated by malicious hackers
- Enterprise policy requirements
- Best strategies for securing the enterprise with layered defenses
- How security zones and detailed logging augment information assurance
- Forensic challenges and incident response planning
- Risk management process
- Goals achievable with auditing, scanning, and testing systems
- Industry recommendations for maintaining secure access control
- Standards-based cryptographic solutions for securing communications

Who Can Benefit

- Network professionals looking to advance their knowledge and explore cybersecurity as a career path.
- Executives and managers looking to increase their ability to communicate with security professionals and implement a robust security solution at the organizational level.
- Individuals wants to improve their understanding of cybersecurity fundamentals, including threats, mitigating controls, and organizational responsibilities.

Prerequisites

TCP/IP Networking or equivalent knowledge

Course Details

Lab 1: Lab Setup

- Access the Virtual Lab Environment
- Configure BackTrack and Redhat Security Spin
- Rebuild Your Physical Computer

Lab 2: Understanding TCP/IP

- Convert Binary to Decimal
- Convert Decimal to Binary
- Convert Hexadecimal to Decimal
- Analyze Wireshark Traffic

Lab 3: Vulnerability Assessment

- Use Nessus
- Identify Coding Issues

Lab 4: Cyber Awareness

- Identifying Social Engineering Attacks
- Detect Phishing Using Internet-Based Tools

Lab 5: Cyber Scanning

- Trace Domains and IP Addresses
- Map Web Site Content with Teleport Pro
- Use Cheops for Graphical Display of Network
- Use GFI LanGuard
- Scan Using Nmap
- Scan Using Zenmap
- Perform Banner Grabbing

Lab 6: Cyber Attacks and Passwords

- Crack Passwords via the GUI
- Crack Passwords via the CLI
- Hide Files with NTFS

Lab 7: Cyber Attacks and Backdoors

- Perform Netcat Banner Grabbing

- Perform Netcat Shoveling
- Use Netcat to Port Scan
- Create and Detect a Trojan

Lab 8: Risk Assessment

- Review Profile and Complete a Criticality Ranking
- Complete a Criticality Review
- Complete a Threat Profile
- Evaluate the Support Policy and Cost

Lab 9: Security Policies

- Review Security Policies
- Develop an Incident Response Policy

Lab 10: Host Security

- Use the RECUB Trojan
- Identify the RECUB Service
- Harden the System

Lab 11: Covert Communications

- Hide Messages Using S-Tools
- Use Spam Mimic

Lab 12: Authentication and Cryptography

- Use Ettercap
- Use Dsniff
- Explore Cain and Abel

Lab 13: Snort IDS

- Install Snort IDS
- Configure Eagle X IDS
- Configure Rule to Ignore Hosts in Snort

Lab 14: Forensic Analysis

- Examine an IIS Event Log and Identify Common
- Use CurrPorts to Identify Anomalies
- Use Jotti for Forensic Analysis

Lab 15: Business Continuity Plan

2015-12-09 14:30:28.833000000

16. Cyber Evolution

- Cyber Forces
- Cyber Terrorism
- Cyber Security: Crime, War, or Fear Mongering?
- Cyber Future 7 Compliance Initiatives
- Cyber Defense in Depth
- Education and Training

Lab 1: Lab Setup

- Access the Virtual Lab Environment
- Configure BackTrack and Redhat Security Spin
- Rebuild Your Physical Computer

Lab 2: Understanding TCP/IP

- Convert Binary to Decimal
- Convert Decimal to Binary
- Convert Hexadecimal to Decimal
- Analyze Wireshark Traffic

Lab 3: Vulnerability Assessment

- Use Nessus
- Identify Coding Issues

Lab 4: Cyber Awareness

- Identifying Social Engineering Attacks
- Detect Phishing Using Internet-Based Tools

Lab 5: Cyber Scanning

- Trace Domains and IP Addresses
- Map Web Site Content with Teleport Pro
- Use Cheops for Graphical Display of Network
- Use GFI LanGuard
- Scan Using Nmap
- Scan Using Zenmap
- Perform Banner Grabbing

Lab 6: Cyber Attacks and Passwords

- Crack Passwords via the GUI
- Crack Passwords via the CLI
- Hide Files with NTFS

Lab 7: Cyber Attacks and Backdoors

- Perform Netcat Banner Grabbing
- Perform Netcat Shoveling
- Use Netcat to Port Scan
- Create and Detect a Trojan

Lab 8: Risk Assessment

- Review Profile and Complete a Criticality Ranking
- Complete a Criticality Review
- Complete a Threat Profile
- Evaluate the Support Policy and Cost

Lab 9: Security Policies

- Review Security Policies
- Develop an Incident Response Policy

Lab 10: Host Security

- Use the RECUB Trojan
- Identify the RECUB Service
- Harden the System

Lab 11: Covert Communications

- Hide Messages Using S-Tools
- Use Spam Mimic

Lab 12: Authentication and Cryptography

- Use Ettercap
- Use Dsniff
- Explore Cain and Abel

Lab 13: Snort IDS

- Install Snort IDS

- Configure Eagle X IDS
- Configure Rule to Ignore Hosts in Snort

Lab 14: Forensic Analysis

- Examine an IIS Event Log and Identify Common
- Use CurrPorts to Identify Anomalies
- Use Jotti for Forensic Analysis

Lab 15: Business Continuity Plan

- Identify When a Disaster Has Occurred
- Determine Key Assets
- Identify Potential Controls

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy
Get Your Free Copy Now

ExitCertified® Corporation and iMVP® are registered trademarks of ExitCertified ULC and ExitCertified Corporation, respectively
Copyright ©2024 ExitCertified ULC & ExitCertified Corporation. All Rights Reserved.