ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

Introduction to Cybersecurity

Course Summary

Description

Investigate cybersecurity threats and master techniques needed to protect your network.
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.

Objectives
At the end of this course, students will be able to:

- Increase your awareness of security
- Interpret/analyze tool output for network mapping/footprinting
- Reduce attack surface of systems
- Review networking as it applies to security controls
- Explore different data protection principles
- Examine the role of PKI/certificates in building trusted relationships between devices in a network
- Implement login security and other identity management solutions
- Reduce attack surface of network devices
- Explore current malware threats and anti-malware solutions
- Explore social engineering threats, methods, and techniques
- Examine software vulnerabilities and security solutions for reducing the risk of exploitation
- Explain monitoring capabilities and requirements and how those may raise privacy concerns
- Identify physical security controls and the relationship between physical and IT security
- Explain incident response capabilities
- Identify legal considerations and investigative techniques when it comes to cybersecurity
- Research trends in cybersecurity

Topics

- Cybersecurity Awareness
- Network Discovery
- Systems Hardening
- Security Architecture
- Data Security
- Public Key Infrastructure
- Identity Management
- Network Hardening
- Malware
- Social Engineering
- Software Security
- Environment Monitoring
- Physical Security
- Incident Response
- Legal Considerations
- Trends in Cybersecurity
- Course Look Around

Introduction to Cybersecurity

Course Summary

Audience

This course is designed for network professionals looking to advance their knowledge and explore cybersecurity as a career path. It is also designed for executives and managers looking to increase their ability to communicate with security professionals and implement a robust security solution at the organizational level and individuals wants to improve their understanding of cybersecurity fundamentals, including threats, mitigating controls, and organizational responsibilities

Prerequisites

TCP/IP Networking or equivalent knowledge

Duration

Five days

ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

Introduction to Cybersecurity

Course Outline

I. Cybersecurity Awareness
- A. What is security?
- B. Confidentiality, integrity, and availability
- C. Security baselining
- D. Security concerns: Humans
- E. Types of threats
- F. Security controls
- G. What is hacking?
- H. Risk management
- I. Data in motion vs. data at rest
- J. Module review

II. Network Discovery
- A. Networking review
- B. Discovery, footprinting, and scanning
- C. Common vulnerabilities and exposures
- D. Security policies
- E. Vulnerabilities
- F. Module review

III. Systems Hardening
- A. What is hardening?
- B. Types of systems that can be hardened
- C. Security baselines
- D. How to harden systems
- E. Hardening systems by role
- F. Mobile devices
- G. Hardening on the network
- H. Analysis tools
- I. Authentication, authorization, and accounting
- J. Physical security
- K. Module review

IV. Security Architecture
- A. Security architecture
- B. Network devices
- C. Network zones
- D. Network segmentation
- E. Network Address Translation
- F. Network Access Control
- G. Module review

V. Data Security
- A. Cryptography
- B. Principles of permissions
- C. Steganography
- D. Module review

VI. Public Key Infrastructure
- A. Public key infrastructure
- B. Certification authorities
- C. Enabling trust
- D. Certificates
- E. CA management
- F. Module review

VII. Identity Management
- A. What is identity management?
- B. Personally identifiable information
- C. Authentication factors
- D. Directory services
- E. Kerberos
- F. Windows NT LAN Manager
- G. Password policies
- H. Cracking passwords
- I. Password assessment tools
- J. Password managers
- K. Group accounts
- L. Service accounts
- M. Federated identities
- N. Identity as a Service
- O. Module review

VIII. Network Hardening
- A. Limiting remote admin access
- B. AAA: Administrative access
- C. Simple Network Management Protocol
- D. Network segmentation
- E. Limiting physical access
- F. Establishing secure access
- G. Network devices
- H. Fundamental device protection summary
- I. Traffic filtering best practices
- J. Module review

Introduction to Cybersecurity

Course Outline (cont'd)

IX. Malware
- A. What is malware?
- B. Infection methods
- C. Types of malware
- D. Backdoors
- E. Countermeasures
- F. Protection tools
- G. Module review

X. Social Engineering
- A. What is social engineering?
- B. Social engineering targets
- C. Social engineering attacks
- D. Statistical data
- E. Information harvesting
- F. Preventing social engineering
- G. Cyber awareness: Policies and procedures
- H. Social media
- I. Module review

XI. Software Security
- A. Software engineering
- B. Security guidelines
- C. Software vulnerabilities
- D. Module review

XII. Environment Monitoring
- A. Monitoring
- B. Monitoring vs. logging
- C. Monitoring/logging benefits
- D. Logging
- E. Metrics
- F. Module review

XIII. Physical Security
- A. What is physical security?
- B. Defense in depth
- C. Types of physical security controls
- D. Device security
- E. Human security
- F. Security policies
- G. Equipment tracking
- H. Module review

XIV. Incident Response
- A. Disaster types
- B. Incident investigation tips
- C. Business continuity planning
- D. Disaster recovery plan
- E. Forensic incident response
- F. Module review

XV. Legal Considerations
- A. Regulatory compliance
- B. Cybercrime
- C. Module review

XVI. Trends in Cybersecurity
- A. Cybersecurity design constraints
- B. Cyber driving forces
- C. How connected are you?
- D. How reliant on connectivity are you?
- E. Identity management
- F. Cybersecurity standards
- G. Cybersecurity training

XVII. Course Look Around
- A. Looking back
- B. Looking forward
- C. Planning your journey

Classroom Live Labs
- Lab 1: Explore HR Security
- Lab 2: Interpret Scanning Results
- Lab 3: Harden Servers and Workstations Lab:4 Security Architecture
- Lab 5: Protect Data Lab 6: Configure a PKI
- Lab 7: Manage Passwords
- Lab 8: Explore Hardening Recommendations and Known Vulnerabilities Lab 9: Detect Malware
- Lab 10: Social Engineering Lab 11: Privilege Escalation Lab 12: Monitor a System
- Lab 13: Implement Physical Security Lab 14: Incident Response
- Lab 15: Review Legal Considerations