

Cyber Security: Fundamentals of Network Security

Length: 2 Days

Summary: This course is designed to introduce students to the fundamentals of network security in preparation for advanced courses. It will give students a solid foundation for understanding different security technologies and how they function. Students will also be able to design a basic network with the proper network security structures in place. This course is designed as an entry-level information assurance class, but it is highly recommended that students have a background in computer and network administration. After taking this course, students should be prepared to take the CompTIA Security+ exam. A good understanding of the Windows and Linux operating system, and TCP/IP protocol, or an extensive background in network administration is highly recommended

COURSE CONTENT

INTRODUCTION TO INFORMATION SECURITY

- The History of Information Security
- Information Security Defined
 - Key Information Technology Concepts
 - Information Assurance
- Critical Characteristics of Information
 - Availability, Accuracy, Authentication, Confidentiality, Integrity,
- Non-repudiation, Utility, and Possession
- NSTISSC Security Model
- Components of an Information System
- Securing the Components
- Balancing Security and Access
- Top-Down Approach to Security Implementation
- The System Development Life Cycle
- The Security System Development Life Cycle
- Security Professionals and The Organization
 - Senior Management
 - Information Security Project Team
 - Data Responsibilities
- Communities of Interest
- Information Security: Is It an Art or a Science?

ATTACKS AND THREATS

- Malware and Social Engineering Attacks
- Attacks Using Malware
- Social Engineering Attacks

- Psychological Approaches
- Physical Procedures
- Key Terms
- Application and Network Attacks
- Application Attacks
 - Web Application Attacks
 - Client-Side Attacks
 - Buffer Overflow Attacks
 - Network Attacks
 - Denial of Service (DoS)
 - Interception
 - Poisoning
 - Attacks on Access Rights

BLUEPRINT (PLANNING) FOR SECURITY

- Information Security Policy, Standards and Practices
 - Enterprise Information Security Policy (EISP)
 - Issue Specific Security Policy (ISSP)
 - System Specific Policy (SysSP)
- Information Classification
- Systems design
- Information Security Blueprints
- ISO 1779/BS 7799
- NIST Security Models and Security Principles
 - NIST Special Publications
 - NSTISSP 11

- Organizational Information Assurance
 - VISA International Security Model
 - Hybrid Framework for a Blueprint of an Information Security System
 - Security Education, Training, and Awareness Program
 - Design of Security Architecture
 - Spheres of Security
 - Levels of Control
 - Defense in Depth
 - Security Perimeter and Zone Controls
 - DoDD 85000.1 Policies
 - National **Policy for Safeguarding and control of COMSEC materials**
 - (CNSS Policy No.1)
 - Organizational COMSEC Policy
 - COMSEC Procedures
 - Anti-criminal Activity Preparedness Planning

LEGAL, ETHICAL AND PROFESSIONAL ISSUES IN INFORMATION SECURITY

- Organizational Accountability and the need for IS Policy
- Law and Ethics in Information Security
- Types of Law
- Relevant U.S. Laws
- International Laws and Legal Bodies
- Policy Versus Law
- Ethical Concepts in Information Security
- Codes of Ethics, Certifications, and Professional Organizations
- Organizational Liability and the Need for Counsel

VULNERABILITY ASSESSMENT AND MITIGATING ATTACKS

- Vulnerability Assessment
 - Assessment Techniques
 - Assessment Tools
- Vulnerability Scanning vs. Penetration Testing
 - Vulnerability Scanning?
 - Penetration Testing
- Mitigating and Deterring Attacks
 - Creating a Security Posture
 - Configuring Controls
 - Hardening
 - Reporting

HOST, APPLICATION, AND DATA SECURITY

- Securing the Host
 - Securing Devices
 - Physical Security
 - Hardware Security
 - Mobile Device Security
- Securing the Operating System Software
- Securing with Anti-Malware Software
- Monitoring System Logs
- Use of Fax Systems, Fax Security and Procedures
- Application Security
 - . Application Development Security
- Securing Data
 - Interception of Data
 - TEMPEST, Emanations and COMSEC Controls
 - Different States of Information
- Database Collection, Warehouse and Database Mining
- Database Vulnerabilities and Threats
 - Inference and Inference Attacks
 - Object Reuse and Polyinstantiation
- Database Operation and Protection

IMPLEMENTING INFORMATION SECURITY

- Information Security Project Management
 - Developing the Project Plan
 - Scope Considerations
 - The Need for Project Management
- Technical Aspects of Implementation
 - Conversion Strategies
 - Technology Governance and Change Control
- Nontechnical Aspects of Implementation
 - The Culture of Change Management
 - Considerations for Organizational Change
- Information Systems Security Certification, Accreditation, and Assessment
 - Information Systems Assessment as Basis for Certification
- Information Technology Maintenance
 - Security Change/Configuration Management Models and Controls
 - Security Management Maintenance Models
 - Monitoring Various Environments (External, Internal etc)

- Vendor Support and Cooperation
- Planning, Risk Assessment and Remediation

NETWORK SECURITY AND DEFENSE

- Security Through Network Devices
- Security Through Network Technologies
 - Network Address Translation (NAT)
 - Network Access Control (NAC)
- Security Through Network Design Elements
 - Demilitarized Zone (DMZ)
 - Subnetting
 - Virtual LANs (VLANs)
 - Remote Access

ADMINISTERING A SECURE NETWORK

- Common Network Protocols
 - Internet Control Message Protocol (ICMP)
 - Simple Network Management Protocol (SNMP)
 - Domain Name System (DNS)
 - File Transfer Protocols
 - IPv6
- Network Administration Principles
 - Device Security
 - Network Design Management
 - Port Security
- Securing Network Applications
 - Virtualization
 - IP Telephony
 - Cloud Computing

WIRELESS NETWORK SECURITY

- Wireless Attacks
 - Attacks on Bluetooth Devices
 - Wireless LAN Attacks
- Vulnerabilities of IEEE 802.11 Security
 - MAC Address Filtering
 - SSID Broadcast
 - Wired Equivalent Privacy (WEP)
- Wireless Security Solutions
 - Wi-Fi Protected Access (WPA)
 - Wi-Fi Protected Access 2 (WPA2)
 - Other Wireless Security Steps

ACCESS CONTROL FUNDAMENTALS

- What Is Access Control?
 - Access Control Terminology
 - Access Control Models
 - Best Practices for Access Control
- Implementing Access Control
 - Access Control Lists (ACLs)
 - Group Policies
 - Account Restrictions
 - Access control software management and Procedures
- Authentication Services
 - RADIUS
 - Kerberos
 - Terminal Access Control Access Control System (TACACS)
- Lightweight Directory Access Protocol (LDAP)

AUTHENTICATION AND ACCOUNT MANAGEMENT

- Authentication Credentials
 - What You Know: Passwords
 - What You Have: Tokens and Cards
 - What You Are: Biometrics
 - Password Attacks and Password Defenses
- Single Sign-On
 - Windows Live ID
 - OpenID
 - Open Authorization (OAuth)
- Account Management
- Trusted Operating Systems

RISK MANAGEMENT: IDENTIFYING AND ASSESSING RISK

- Mitigating Risk
- Risk Management
 - Risk Identification
 - Risk Assessment
 - Risk Control Strategies and Categories of Risk
- Risk Mitigation Strategy Selection
- Reducing Risks Through Policies
- Designing Security Policy
 - Types of Security Policies
- Awareness and Training
- Feasibility Studies and Cost Benefit Analysis (CBA)
- Documenting Results
- Benchmarking and Recommended Practices in Controlling Risk

CRYPTOGRAPHY

- Defining Cryptography
- Cryptographic Algorithms
 - Hash Algorithms
 - Symmetric Cryptographic Algorithms
 - Asymmetric Cryptographic Algorithms
- Using Cryptography
 - Encryption Through Software
 - Hardware Encryption
- Digital Certificates
- Public Key Infrastructure (PKI)
 - What Is Public Key Infrastructure (PKI)?
 - Public-Key Cryptographic Standards (PKCS)
 - Hierarchical Trust Models
 - Distributed Trust Models
 - Bridge Trust Models
 - Managing PKI
- Key Management
 - Key Storage, Usage, and Key-Handling Procedures
- Transport Encryption Algorithms
 - Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
 - Secure Shell (SSH)
 - Hypertext Transport Protocol over Secure Sockets Layer (HTTPS)
 - IP Security (IPsec)

BUSINESS CONTINUITY

- Business Continuity Strategies
 - Business Impact Analysis
 - Incident Response Planning
 - Disaster Recovery Planning
 - Business Continuity Planning
 - Model for a Consolidated Contingency Plan
 - Law Enforcement Involvement
- Disaster Recovery
 - Disaster Recovery Plan
 - Redundancy and Fault Tolerance
 - Data Backups
- Environmental Controls
 - Fire Suppression
 - Electromagnetic Interference (EMI) Shielding
 - EMSEC/TEMPEST Policy and Controls
 - HVAC
- Incident Response Procedures
 - . Forensics Defined

ADDITIONAL TOPICS DISCUSSED FROM SUPPLEMENTAL TEXT CHAPTERS

- OPSEC Process C6.2
- OPSEC Surveys/OPSEC Planning C6.2
- Unclassified Indicators C6.2
- Application Guidance C5.5
- Emanations Security C9.1
- HUMINT C6.4
- Telecommunications Systems, Telecommunications C3.0 & 3.1
- NSTISSAM COMPUSEC/1-99, Advisory Memorandum on the Transition from Trusted Computer System Evaluation Criteria to the International Common Criteria
- Vulnerabilities, Threats, Counter Measures
- Security Policies, Guidance, Contacts, and Roles C14.3
- Security Policies ▯ Budgeting, Valuation, and Training C1.0 & 1.4
- Systems Life Cycle Processes, Certification and Accreditation C11.6 &
- Contents of National Computer Security Center - TG-005 Publication
- Media Processes ▯ Attribution, Destruction, Classification, C6
- Sanitization, Transportation, Inventory, Incident Reporting C6.3
- National Threats, Vulnerabilities, Counter Measures, C1.0
- Risk Management, and other facets of NSTISS
- Security and Personnel
- Information Operation (IO)
- Testing
- Marking Data - C.F.R. 32 Section 2003, National Security Information -
- Standard Forms