Virginia Western Community College
ITN 260
Network Security Basics

Prerequisites
TEL 150

Course Description
Provides instruction in the basics of network security in depth. Includes security objectives, security architecture, security models and security layers; risk management, network security policy, and security training. Includes the five security keys, confidentiality integrity, availability, accountability and auditability.

Semester Credits: 3 Lecture Hours: 3 Lab/Clinical/Internship Hours: 0

Required Materials

Textbook:
Security and Guide to Network Security Fundamentals; Mary Ciampa; 5th edition; ISBN: 978-1-305-09391-1

Other Required Materials:
none

Course Outcomes

At the completion of this course, the student should be able to:

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- List the basic steps of an attack
- Describe the five basic principles of defense
- Define malware
- List the different types of malware
- Identify payloads of malware
- Describe the types of social engineering psychological attacks
- Explain physical social engineering attacks
- List and explain the different types of server-side web application attacks
- Define client-side attacks
- Explain how overflow attacks work

- List different types of networking-based attacks
- List the steps for securing a host computer
- Define application security
- Explain how to secure data
- Define cryptography
- Describe hash, symmetric, and asymmetric cryptographic algorithms
- List the various ways in which cryptography is used
- Define digital certificates
- List the various types of digital certificates and how they are used
- Describe the components of Public Key Infrastructure (PKI)
- List the tasks associated with key management
- Describe the different transport encryption protocols
- List the different types of network security devices and how they can be used
- Explain how network technologies can enhance security
- Describe secure network design elements
- List and describe the functions of common network protocols
- Explain how network administration principles can be applied
- Define different network applications and how they can be secured
- Describe the different types of wireless network attacks
- List the vulnerabilities in IEEE 802.11 security
- Explain the solutions for securing a wireless network
- List and compare the different types of mobile devices
- Explain the risks associated with mobile devices
- List ways to secure a mobile device
- Explain how to apply mobile device app security
- Describe how to implement BYOD security
- Define access control and list the four access control models
- Describe how to implement access control
- Explain the different types of authentication services
- Describe the different types of authentication credentials
- Explain what single sign-on can do
- List the account management procedures for securing passwords
- Define business continuity
- List the features of a disaster recovery plan
- Explain different environmental controls
- Describe forensics and incident response procedures
- Explain how to control risk
- List the ways in which security policies can reduce risk
- Describe how awareness and training can provide increased security
- Define vulnerability assessment and explain why it is important
- Explain the differences between vulnerability scanning and penetration testing
- Describe the security implications of integration with third parties
- List techniques for mitigating and deterring attacks

Topical Description

- Chapter 01: Introduction to Security
  - Challenges of Securing Information
    - Today's Security Attacks
    - Difficulties in Defending Against Attacks
  - What Is Information Security?
    - Understanding Security
    - Defining Information Security
    - Information Security Terminology
    - Understanding the Importance of Information Security
  - Who Are the Attackers?
    - Cybercriminals
    - Script Kiddies
    - Brokers
    - Insiders
    - Cyberterrorists
    - Hactivists
    - State-Sponsored Attackers
  - Attacks and Defenses
    - Steps of an Attack
    - Defenses Against Attacks
- Chapter 02: Malware and Social Engineering Attacks
  - Attacks Using Malware
    - Circulation/Infection
    - Concealment
    - Payload Capabilities
  - Social Engineering Attacks
    - Psychological Approaches
    - Physical Procedures
- Chapter 03: Application and Networking-Based Attacks
  - Application Attacks
  - Server-Side Web Application Attacks
  - Client-Side Application
  - Impartial Overflow Attacks
- Networking-Based
  - Denial of Service (DoS)
  - Interception
  - Poisoning
  - Attacks on Access Rights
- Chapter 04: Host, Application, and Data Security
  - Securing the Host
    - Securing Devices
    - Securing the Operating System Software

        - Securing with Antimalware
    - Securing Static Environments
    - Application Security
        - Application Development Security
        - Application Hardening and Patch Management
    - Securing Data
- Chapter 05: Basic Cryptography
    - Defining Cryptography
        - What Is Cryptography?
        - Cryptography and Security
    - Cryptographic Algorithms
        - Hash Algorithms
        - Symmetric Cryptographic Algorithms
        - Asymmetric Cryptographic Algorithms
    - Using Cryptography
        - Encryption Through Software
        - Hardware Encryption
- Chapter 06: Advanced Cryptography
    - Digital Certificates
        - Defining Digital Certificates
        - Managing Digital Certificates
        - Types of Digital Certificates
    - Public Key Infrastructure(PKI)
        - What Is Public Key Infrastructure (PKI)?
        - Public Key Cryptography Standards (PKCS)
        - Trust Models
        - Managing PKI
    - Key Management
        - Key Storage
        - Key Usage
        - Key Handling Procedures
    - Cryptographic Transport Protocols
        - Secure Sockets Layer (SSL)
        - Transport Layer Security (TLS)
        - Secure Shell (SSH)
        - Hypertext Transport Protocol Secure (HTTPS)
        - IP Security (IPsec)
- Chapter 07: Network Security Fundamentals
    - Security Through Network Devices
        - Standard Network Devices
        - Network Security Hardware
    - 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
- Chapter 08: Administering a Secure Network
    - Common Network Protocols
        - Internet Control Message Protocol (ICMP)
        - Simple Network Management Protocol (SNMP)
        - Domain Name System (DNS)
        - File Transfer Protocols
        - Storage Protocols
        - NetBIOS
        - Telnet
        - IPv6
    - Network Administration Principles
        - Device Security
        - Monitoring and Analyzing Logs
        - Network Design Management
        - Port Security
    - Securing Network Applications and Platforms
        - IP Telephony
        - Virtualization
        - Cloud Computing
- Chapter 09: Wireless Network Security
    - Wireless Attacks
        - Bluetooth Attacks
        - Near Field Communication (NFC) Attacks
        - Wireless Local Area Network(WLAN) Attacks
    - Vulnerabilities of IEEE Wireless Security
        - Wired Equivalent Privacy (WEP)
        - Wi-Fi Protected Setup (WPS)
          MAC Address Filtering
        - Disabling SSID Broadcasts
    - Wireless Security Solutions
        - Wi-Fi Protected Access (WPA)
        - Wi-Fi Protected Access2 (WPA2)
        - Additional Wireless Security Protections
- Chapter 10: Mobile Device Security
    - Types of Mobile Devices
        - Portable Computers
        - Tablets
        - Smartphones
        - Wearable Technology
        - Legacy Devices
        - Mobile Device Removable Storage
    - Mobile Device Risks
        - Limited Physical Security

        - Connecting to Public Networks
        - Location Tracking
        - Installing Unsecured Applications
        - Accessing Untrusted Content
        - Bring Your Own Device (BYOD) Risks
    - Securing Mobile Devices
        - Device Setup
        - Device and App Management
        - Device Loss or Theft
    - Mobile Device App Security
    - BYOD Security
- Chapter 11: 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
    - Authentication Services
        - RADIUS
        - Kerberos
        - Terminal Access Control Access Control System(TACACS)
        - Lightweight Directory Access Protocol(LDAP)
        - Security Assertion Markup Language (SAML)
- Chapter 12: Authentication and Account Management
    - Authentication Credentials
        - What You Know: Passwords
        - What You Have: Tokens, Cards, and Cell Phones
        - What You Are: Biometrics
        - What You Do: Behavioral Biometrics
        - Where You Are: Geolocation
    - Single Sign-On
        - Microsoft Account
        - OpenID
        - Open Authorization (OAuth)
- Chapter 13: Business Continuity
    - What Is Business Continuity
    - Disaster Recovery
        - Disaster Recovery Plan (DRP)
        - Redundancy and Fault Tolerance
        - Data Backups
    - Environmental Controls
        - Fire Suppression
        - Electromagnetic Interference (EMI) Shielding

        - HVAC
    - Incident Response
        - Forensics
        - Incident Response Procedures
- Chapter 14: Risk Mitigation
    - Controlling Risk
        - Privilege Management
        - Change Management
        - Incident Management
        - Risk Calculation
    - Reducing Risk Through Policies
        - What Is a Security Policy?
        - Balancing Trust and Control
        - Designing a Security Policy
        - Types of Security Policies
    - Awareness and Training
        - Compliance
        - User Practices
        - Threat Awareness
        - Training Techniques
- Chapter 15: Vulnerability Assessment
    - Assessing Vulnerabilities
        - What Is Vulnerability Assessment?
        - Assessment Techniques
        - Assessment Tools
    - Vulnerability Scanning vs. Penetration Testing
        - Vulnerability Scanning
        - Penetration Testing
    - Third-Party Integration
    - Mitigating and Deterring Attacks
        - Creating a Security Posture
        - Selecting Appropriate Controls
        - Configuring Controls
        - Hardening
        - Reporting

Notes to Instructors

- none