ITNT-2370: NETWORK SECURITY FUNDAMENTALS

Cuyahoga Community College

Viewing: ITNT-2370 : Network Security Fundamentals

Board of Trustees:
May 2023

Academic Term:
Fall 2023

Subject Code
ITNT - Info Tech-Networking Software

Course Number:
2370

Title:
Network Security Fundamentals

Catalog Description:
A survey examination of network security fundamentals involved in creating and managing secure computer network environments. Both hardware and software topics are considered, including authentication methods, remote access, network security architectures and devices, cryptography, forensics, and disaster recovery plans. Serves as preparation basis for CompTIA Security+ exam.

Credit Hour(s):
3

Lecture Hour(s):
2
Lab Hour(s):
2

Requisites

Prerequisite and Corequisite
ITNT-2300 Networking Fundamentals.

Outcomes

Course Outcome(s):
Assess, design, implement, and maintain basic network security policies and practices to secure a network.

Objective(s):

a. Describe computer forensics approaches and select when to use them.
b. Explain various network security terms and concepts.
c. Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
d. Explain the security implications of embedded and specialized systems.
e. Define the need for network security and how to implement it.
f. Analyze and compare hardware and software used to implement network security.
g. Analyze potential indicators to determine the type of attack, when given a scenario.
h. Relate how to set-up and operate a secure network.
i. Diagram and differentiate common network security architectures.
j. Explain privacy and sensitive data concepts in relation to security.
k. Explain network security threats and countermeasures for the wired and wireless network environment including hardware, software, protocols and services.
l. Evaluate the need for security policies based on given scenarios.
m. Create and critique disaster recovery plans.
n. Explain the importance of policies to organizational security.

o. Explain the importance of security concepts in an enterprise environment.
p. Utilize appropriate data sources to support an investigation, when given an incident.

Methods of Evaluation:

a. Exams
b. Discussion
c. Research paper/report
d. Presentation
e. Activities/labs
f. Quizzes
g. Scenario evaluations

Course Content Outline:

a. Introduction to Security
    i. Challenges of Securing Information
        1. Today's Security Attacks
        2. Difficulties in Defending Against Attacks
    ii. What is Information Security
        1. Defining Information Security
        2. Information Security Terminology
    iii. Attacker Examples
        1. Cybercriminals, Script Kiddies, Brokers, Insiders, Cyberterrorists, Hacktivists, State-Sponsored, and other attackers
    iv. Attacks and Defenses
        1. Attack Steps
        2. Attack Defenses
b. Malware and Social Engineering Attacks
    i. Malware Attacks
        1. Circulation/Infection
        2. Concealment
        3. Payload Capabilities
    ii. Social Engineering Attacks
        1. Psychological Approaches
        2. Physical Procedures
c. Application and Networking-Based Attacks
    i. Application Attacks
        1. Server-side Web Application Attacks
        2. Client-side Application Attacks
        3. Impartial Overflow Attacks
    ii. Networking-Based Attacks
        1. Denial of Service (DoS)
        2. Interception
        3. Poisoning
        4. Attacks on Access Rights
d. Host, Application, and Data Security
    i. Securing the Host
        1. Devices
        2. Operating Systems
        3. Using Antimalware
    ii. Securing Static Environments
    iii. Application Security
        1. Application Development Security
        2. Application Hardening and Patch Management
    iv. Securing Data
e. Basic Cryptography
    i. Cryptography Defined
        1. Cryptography and Security
        2. Cryptography Defined

- ii. Cryptographic Algorithms
  1. Hash Algorithms
  2. Symmetric Cryptographic Algorithms
  3. Asymmetric Cryptographic Algorithms
  4. Other Algorithms
- iii. Using Cryptography
  1. Software Encryption
  2. Hardware Encryption

f. Advanced Cryptography
- i. Digital Certificates
  1. Digital Certificates Defined
  2. Digital Certificate Management
  3. Digital Certificate Types
- ii. Public Key Infrastructure (PKI)
  1. Public Key Infrastructure Defined
  2. Public Key Cryptography Standards
  3. Trust Models
  4. PKI Management
- iii. Key Management
  1. Key Storage
  2. Key Usage
  3. Key Handling Procedures
- iv. Cryptographic Transport Protocols
  1. Secure Sockets Layer (SSL)
  2. Transport Layer Security (TLS)
  3. Secure Shell (SSH)
  4. Hypertext Transport Protocol Secure (HTTPS)
  5. IP Security (IPsec)
  6. Other appropriate Protocols

g. Network Security Fundamentals
- i. Security Through Network Devices
  1. Standard Network Devices
  2. Network Security Hardware
- ii. Security Through Network Technologies
  1. Network Address Translation (NAT)
  2. Network Access Control (NAC)
  3. Other Appropriate Technologies
- iii. Security Through Network Design Elements
  1. Demilitarized Zone (DMZ)
  2. Subnetting
  3. Virtual LANs (VLANs)
  4. Remote Access

h. Administering a Secure Network
- i. Common Network Protocols
  1. Internet Control Message Protocol (ICMP)
  2. Simple Network Management Protocol (SNMP)
  3. Domain Name System (DNS)
  4. File Transfer Protocols
  5. Storage Protocols
  6. NetBIOS
  7. Telnet
  8. IPv6
  9. Other Appropriate Protocols
- ii. Network Administration Principles
  1. Device Security
  2. Monitoring and Analyzing Logs
  3. Network Design Management
  4. Port Security
- iii. Securing Network Applications and Platforms

1. IP Telephony
2. Virtualization
3. Cloud Computing

i. Wireless Network Security
   i. Wireless Attacks
      1. Bluetooth Attacks
      2. Near Field Communication (NFC) Attacks
      3. Wireless Local Area Network (WLAN) Attacks
   ii. Vulnerabilities of IEEE Wireless Security
      1. Wired Equivalent Privacy (WEP)
      2. Wi-FiProtected Setup (WPS)
      3. MAC Address Filtering
      4. Disabling SSID Broadcasts
      5. Other vulnerabilities as appropriate
   iii. Wireless Security Solutions
      1. Wi-Fi Protected Access (WPA)
      2. Wi-Fi Protected Access 2 (WPA2)
      3. Additional Wireless Security Protections
j. Mobile Device Security
   i. Types of Mobile Devices
   ii. Mobile Device Risks
      1. Limited Physical Security
      2. Connecting to Public Networks
      3. Location Tracking
      4. Installing Unsecured Applications
      5. Accessing Untrusted Content
      6. Bring Your Own Device (BYOD) Risks
   iii. Securing Mobile Devices
      1. Device Setup
      2. Device and App Management
      3. Device Loss or Theft
   iv. Mobile Device App Security
   v. BYOD Security
k. Access Control Fundamentals
   i. Access Control Defined
      1. Access Control Terminology
      2. Access Control Models
      3. Best Practices for Access Control
   ii. Implementing Access Control
      1. Access Control Lists (ACLs)
      2. Group Policies
      3. Account Restrictions
   iii. Authentication Services
      1. RADIUS
      2. Kerberos
      3. Terminal Access Control Access Control System (TACACS)
      4. Lightweight Directory Access Protocol (LDAP)
      5. Security Assertion Markup Language (SAML)
l. Authentication and Account Management
   i. Authentication Credentials
      1. What You Know
      2. What You Have
      3. What You Are
      4. What You Do
      5. Where You Are
   ii. Single Sign-On
      1. Appropriate Examples which may include; Microsoft Account, Open ID, Open Authorization (OAuth)
      2. Or Other Examples
   iii. Account Management

m. Business Continuity
    i. Business Continuity Defined
    ii. Disaster Recovery
        1. Disaster Recovery Plan (DRP)
        2. Redundancy and Fault Tolerance
        3. Data Backups
    iii. Environmental Controls
        1. Fire Suppression
        2. Electromagnetic Interference (EMI) Shielding
        3. HVAC
    iv. Incident Response
        1. Forensics
        2. Incident Response Procedures
n. Risk Mitigation
    i. Controlling Risk
        1. Privilege Management
        2. Change Management
        3. Incident Management
        4. Risk Calculation
    ii. Reducing Risk Through Policies
        1. Security Policy Defined
        2. Balancing Trust and Control
        3. Designing a Security Policy
        4. Security Policy Types
    iii. Awareness and Training
        1. Compliance
        2. User Practices
        3. Threat Awareness Training Techniques
o. Vulnerability Assessment
    i. Assessing Vulnerabilities
        1. Vulnerability Assessment Defined
        2. Assessment Techniques
        3. Assessment Tools
    ii. Vulnerability Scanning Vs. Penetration Testing
        1. Vulnerability Scanning
        2. Penetration Testing
    iii. Third-Party Integration
    iv. Mitigating and Deterring Attacks
        1. Security Posture
        2. Selecting Appropriate Controls
        3. Configuring Controls
        4. Hardening
        5. Reporting

Resources

Ciampa, Mark. *Security+ Guide to Networking Security Fundamentals*. 6th. ed. Boston, MA: Thomson Learning/Course Technology, 2017.

Kim, David and Micheal G. Solomon. *Fundamentals of Information Systems Security*. 4th ed. Sudbury, MA: Jones & Bartlett Learning, 2021.

Whitman, Michael and Herbert J. Mattord, Dave Mackey, Andrew Green. *Guide to Network Security.* 1st. Boston MA: Cengage Learning, 2013.

EC-Council. *Network Defense: Security and Vulnerability Assessment.* 1st Edition. Boston, MA: Cengage Learning, 2011.

Perez, Andre. *Network Security.* 1st Edition. Wiley ISTE, 2014.

Dulaney, Emmett and Chuck Esttomm. *CompTIA Security+ Study Guide: Exam SY0-601*. 8th Edition. Wiley / Sybex, 2021.

Delaney, Emmett. *CompTIA Security+ Certification Kit: Exam SY0-601*. 6th Edition. Wiley / Sybex, 2021.

Mark Ciampa. *CompTIA Security+ Guide to Network Security Fundamentals*. 7th Edition. Cengage Learning, 2020. December 16.

Resources Other
www.Microsoft.com (http://www.Microsoft.com)
www.CompTIA.com (http://www.CompTIA.com)
www.CERT.org (http://www.CERT.org)
www.SANS.org (http://www.SANS.org)
www.FBI.gov
www.DHS.gov

Instructional Services

CTAN Number:
Career Technical Assurance Guide CTIT015 and Industry-Recognized Transfer Assurance Guide ITITS015

Top of page
Key: 2572