IT-2710: ADVANCED TOPICS IN NETWORK SECURITY

Cuyahoga Community College

Viewing: IT-2710 : Advanced Topics in Network Security

Board of Trustees:
June 2022

Academic Term:
Fall 2022

Subject Code
IT - Information Technology

Course Number:
2710

Title:
Advanced Topics in Network Security

Catalog Description:
Capstone course. Provides in-depth understanding of network security principles and the tools and configurations needed to secure a network.

Credit Hour(s):
3

Lecture Hour(s):
2

Lab Hour(s):
2

Requisites

Prerequisite and Corequisite
ITNT-2370 Network Security Fundamentals.

Outcomes

Course Outcome(s):
Apply knowledge of advanced network security principles to mitigate security threats to network by utilizing secure design, management, and reporting.

Objective(s):
1. Describe the security threats facing modern network infrastructures
2. Implement Authentication, Authorization, and Accounting (AAA).
3. Mitigate threats to networks using Access Controls.
4. Demonstrate methods used to Implement secure network design, management, and reporting.

Course Outcome(s):
Utilize the tools and understand the configurations necessary to secure a network.

Objective(s):
1. Implement Authentication, Authorization, and Accounting (AAA).
2. Mitigate threats to networks using Access Controls.
3. Demonstrate methods used to implement secure network design, management, and reporting.
4. Mitigate common attacks.
5. Explain the Incident Response Process.
6. Discuss organizational compliance and assessment related to security.

Methods of Evaluation:

Evaluation can include any combination of the following:

1. Assignments
2. Quizzes
3. Exams
4. Lab Assignments
5. Projects
6. Reports
7. Oral Evaluations

Course Content Outline:

1. Security threats facing modern network infrastructures
   a. Network security principles
   b. Types of threats and attacks
   c. Current tools and procedures to mitigate the effects of malware and common network attacks
   d. Vulnerability management
2. Secure Network Devices
   a. Configuration of secure administrative access
   b. Assignment of administrative roles
   c. Secure management and monitoring of network devices
3. Authentication, Authorization, and Accounting (AAA)
   a. AAA to secure a network
   b. Local AAA authentication
   c. Server-based AAA authentication
   d. Proactive threat hunting
   e. Automation concepts and technology
4. Mitigating threats to networks
   a. Use of Access Controls to mitigate threats to networks
   b. Use of firewall to mitigate network attacks
5. Secure network design, management, and reporting
   a. Principles of secure network design
   b. Implementation of a comprehensive security policy
   c. Techniques and tools used for network security testing
   d. Principles of business continuity planning and disaster recovery
   e. Comprehensive security policy
      i. Functions
      ii. Goals
      iii. Role
      iv. Structure
6. Incident response
   a. Communication plan
   b. Preparation
   c. Detection analysis
   d. Containment
   e. Eradication and recovery
   f. Post-incident activities
7. Compliance and assessment
   a. Data privacy and protection
   b. Risk mitigation
   c. Frameworks
   d. Policies and procedures
   e. Controls

Resources

Ciampa, M. (2022) *CompTIA CySA+ guide to cybersecurity analyst*, Boston: Cengage.

Stewart, J. & Kinsey, D. (2022) *Network security, firewalls, and VPNs*, Burlington, MA: Jones & Bartlett Learning.

Ciampa, M. (2022) *CompTIA Security+ guide to network security fundamentals*, Boston: Cengage.

Weaver, R. & Farwood, D. (2014) *Guide to network defense and countermeasures*, Boston: Cengage.

Top of page
Key: 2514