Miami Dade College

Course Description

CNT3409C | Network Security | 4.00 credits

In this course, the student will be introduced to current and emerging threats to the security of computer networks, as well as tools and techniques for the prevention, detection and recovery from such attacks. Topics include firewalls, intrusion detection and intrusion prevention systems, virtual private networks, remote authentication and authorization systems, and security protocols. Prerequisite: CIS3360

Course Competencies:

Competency 1: The student will be able to demonstrate an understanding of the fundamentals of networking and network defense by:

1. Comparing the OSI and TCP/IP network models
2. Describing various network topologies
3. Describing various network components
4. Explaining various protocols in TCP/IP protocol stack
5. Discussing IP addressing
6. Describing the computer network defense process

Competency 2: The student will be able to demonstrate an understanding of network security threats, vulnerabilities, and attacks by:

1. Defining threat, attack, and vulnerability
2. Discussing the effect of network security breach on business continuity
3. Describing different types of network threats, vulnerabilities and attacks

Competency 3: The student will be able to demonstrate an understanding of network security controls, protocols, and devices by:

1. Describing various network access control mechanisms
2. Explaining different types of access controls
3. Describing network Authentication, Authorization and Auditing (AAA) mechanism
4. Explaining network data encryption mechanism
5. Describing Public Key Infrastructure (PKI)
6. Describing various network security protocols
7. Describing various network security devices

Competency 4: The student will be able to demonstrate an understanding of network security policy design and implementation by:

1. Describing the need for security policies
2. Describing the security policy hierarchy
3. Describing the characteristics of a good security policy
4. Describing the typical content of security policy
5. Designing a network security policy

Competency 5: The student will be able to demonstrate an understanding of physical security by:

1. Discussing the need for physical security
2. Describing the factors affecting physical security
3. Explaining Fire Fighting Systems
4. Describing various physical security controls

5. Describing various access control authentication techniques
6. Explaining workplace security
7. Explaining personnel security
8. Describing environmental controls
9. Discussing the importance of physical security awareness and training

Competency 6: The student will be able to demonstrate an understanding of host security by:

1. Discuss the need for securing individual hosts
2. Describing threats specific to hosts
3. Identifying paths to host threats
4. Describing host security baselining
5. Describing OS security baselining
6. Describing security requirements for different types of servers
7. Describe security requirements for hardening routers
8. Describe security requirements for hardening switches
9. Explaining data security at rest, in motion, and use
10. Describing virtualization security

Competency 7: The student will be able to demonstrate an understanding of secure firewall configuration and management by:

1. Describing various firewall technologies
2. Describing firewall topologies. Selecting appropriate firewall topologies
3. Designing and configuring a firewall ruleset
4. Implementing firewall policies
5. Explaining the deployment and implementation of firewalls
6. Discussing factors to consider before purchasing a firewall solution
7. Describing the configuring, testing and deploying of firewalls
8. Describing the managing, maintaining, and administrating firewall implementation
9. Explaining firewall logging
10. Implementing measures for avoiding firewall evasion
11. Describing firewall security best practices

Competency 8: The student will be able to demonstrate an understanding of secure ids configuration and management by:

1. Explaining different types of intrusions and their indications
2. Explaining IDPS.
3. Describing role of IDPS in network defense
4. Describing functions, components, and working of IDPS
5. Explaining various types of IDS implementation
6. Describing staged deployment of NIDS and HIDS
7. Describing fine-tuning of IDS by minimizing false positive and false negative rate
8. Discussing common IDS implementation mistakes and their remedies
9. Explaining various types of IPS implementation
10. Discussing requirements for selecting appropriate IDSP product
11. Describing technologies complementing IDS functionality

Competency 9: The student will be able to demonstrate an understanding of secure VPN configuration and management by:

1. Explaining Virtual Private Network (VPN)

2. Importance of establishing VPNs
3. Describing various VPN components
4. Describing the implementation of VPN concentrators and their functions
5. Explaining different types of VPN technologies
6. Discussing components for selecting appropriate VPN technology
7. Explaining core functions of VPN
8. Explaining various topologies for implementation of VPN
9. Discussing various VPN security concerns
10. Discussing various security implications to ensure VPN security and performance

Competency 10: The student will be able to demonstrate an understanding of wireless network defense by:

1. Discussing various wireless standards
2. Describing various wireless network topologies
3. Describing possible use of wireless networks
4. Explaining various wireless network components
5. Explaining wireless encryption (WEP, WPA, WPA2) technologies
6. Describing various authentication methods for wireless networks
7. Discussing various types of threats on wireless networks
8. Creating of inventory for wireless network components
9. Discussing the appropriate placement of wireless AP
10. Discuss the appropriate placement of the wireless antenna
11. Monitoring of wireless network traffic
12. Detecting and locating rogue access points
13. Discussing RF interference
14. Describing various security implications for wireless networks

Competency 11: The student will be able to demonstrate an understanding of network traffic monitoring and Analysis by:

1. Discussing the importance of network traffic monitoring
2. Discuss techniques used for network monitoring and analysis
3. Discuss appropriate positions for network monitoring
4. Explaining how to perform a network monitoring system using a managed switch
5. Defining network traffic signatures
6. Baselining for regular traffic
7. Discuss the various categories of suspicious traffic signatures
8. Listing various techniques for attack signature analysis
9. Explaining Wireshark components, working, and features
10. Demonstrating the use of various Wireshark filters
11. Demonstrating the monitoring of LAN traffic against policy violations
12. Demonstrating the security monitoring of network traffic
13. Demonstrating the detection of various attacks using Wireshark
14. Discuss network bandwidth monitoring and performance improvement

Competency 12: The student will be able to demonstrate an understanding of network risk and vulnerability management by:

1. Defining risk and risk management
2. Describing various risk management frameworks
3. Explaining vulnerability management
4. Describing the phases involved in vulnerability management

5. Explaining vulnerability assessment and its importance
6. Discussing internal and external vulnerability assessment
7. Selecting appropriate vulnerability assessment tools
8. Describing vulnerability reporting, mitigation, remediation, and verification

Competency 13: The student will be able to demonstrate an understanding of data backup and recovery by:

1. Describing data backup
2. Determining the appropriate backup medium for data backup
3. Understanding RAID backup technology and its advantages
4. Describing RAID architecture
5. Describing various RAID levels and their use
6. Describing Storage Area Network (SAN) backup technology and its advantages
7. Describing various types of NAS implementation

Competency 14: The student will be able to demonstrate an understanding of network incident response and management by:

1. Defining Incident Handling and Response (IH&R)
2. Describe the Incident Response Team (IRT) roles and responsibilities
3. Describing the Incident Handling and Response (IH&R) process
4. Explaining the goals of forensic investigation
5. Describing the forensics investigation methodology