Miami Dade College

Course Competencies Template - Form 112

GENERAL INFORMATION	
Name: Nelly Delessy	Phone #: (305) 237-1485
Course Prefix/Number: CNT 3409C	Course Title: Network Security
Number of Credits: 4	
Degree Type	☐ B.A. ☒ B.S. ☐ B.A.S ☐ A.A. ☐ A.S. ☐ A.A.S. ☐ C.C.C. ☐ A.T.C. ☐ C.T.C.(V.C.C.)
Date Submitted/Revised: May 29, 2020	Effective Year/Term: Spring 2021
☐ New Course Competency ☒ Revised Course Competency	
Course to be designated as a General Education course (part of the 36 hours of A.A. Gen. Ed. coursework): ☐ Yes ☒ No	

Learning Outcomes Legend:

1.	Communication	4.	Information Literacy	8.	Computer / Technology Usage
2.	Numbers / Data	5.	Cultural / Global Perspective	9.	Aesthetics / Creativity Activities
3.	Critical Thinking	6.	Social Responsibility	10.	Environmental Responsibility
		7.	Ethical Issues		

Course Description (limit to 50 words or less, **must correspond with course description on Form 102**):

This upper division course introduces students 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: CIS 3360. (3 hr. lecture; 2 hr. lab).

Prerequisite(s): CIS3360	Co requisite(s):

Course Competencies: (for further instruction/guidelines go to: http://www.mdc.edu/asa/curriculum.asp)

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

a) Comparing the OSI and TCP/IP network models.	3, 8
b) Describing various network topologies.	3, 8
c) Describing various network components.	3, 8
d) Explaining various protocols in TCP/IP protocol stack.	3, 8
e) Discussing IP addressing.	3, 8
f) Describing the computer network defense process.	3, 8

Revision Date: **Spring 2020**

Approved By Academic Dean Date: _____ Reviewed By Director of Academic Programs Date: _____

Competency 2. The student will be able to demonstrate an understanding of network security threats, vulnerabilities, and attacks by:	
a) Defining threat, attack, and vulnerability.	3, 8
b) Discussing the effect of network security breach on business continuity.	3, 8
c) Describing different types of network threats, vulnerabilities and attacks.	3, 8

Competency 3. The student will be able to demonstrate an understanding of network security controls, protocols, and devices by:	
a) Describing various network access control mechanisms.	3, 8
b) Explaining different types of access controls.	3, 8
c) Describing network Authentication, Authorization and Auditing (AAA) mechanism.	3, 8
d) Explaining network data encryption mechanism.	3, 8
e) Describing Public Key Infrastructure (PKI).	3, 8
f) Describing various network security protocols	3, 8
g) Describing various network security devices	3, 8

Competency 4. The student will be able to demonstrate an understanding of network security policy design and implementation by:	
a) Describing the need for security policies.	3, 8
b) Describing the security policy hierarchy.	3, 8
c) Describing the characteristics of a good security policy.	3, 8
d) Describing the typical content of security policy.	3, 8
e) Designing a network security policy.	3, 8

Competency 5. The student will be able to demonstrate an understanding of physical security by:	
a) Discussing the need for physical security.	3, 8
b) Describing the factors affecting physical security.	3, 8
c) Describing various physical security controls.	3, 8
d) Explaining Fire Fighting Systems.	3, 8
e) Describing various access control authentication techniques.	3, 8
f) Explaining workplace security.	3, 8
g) Explaining personnel security.	3, 8
h) Describing environmental controls.	3, 8

Revision Date: **Spring 2020**

Approved By Academic Dean Date: _____ Reviewed By Director of Academic Programs Date: _____

i) Discussing the importance of physical security awareness and training.	3, 8

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

a) Discussing the need for securing individual hosts.	3, 8
b) Describing threats specific to hosts.	3, 8
c) Identifying paths to host threats.	3, 8
d) Describing host security baselining.	3, 8
e) Describing OS security baselining.	3, 8
f) Describing security requirements for different types of servers.	3, 8
g) Describing security requirements for hardening of routers.	3, 8
h) Describing security requirements for hardening of switches.	3, 8
i) Explaining data security at rest, in motion and in use.	3, 8
j) Describing virtualization security.	3, 8

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

a) Describing various firewall technologies.	3, 8
b) Describing firewall topologies.	3, 8
c) Selecting appropriate firewall topologies.	3, 8
d) Designing and configuring a firewall ruleset.	3, 8
e) Implementing firewall policies.	3, 8
f) Explaining the deployment and implementation of firewalls.	3, 8
g) Discussing factors to considers before purchasing a firewall solution.	3, 8
h) Describing the configuring, testing and deploying of firewalls.	3, 8
i) Describing the managing, maintaining, administrating firewall implementation.	3, 8
j) Explaining firewall logging.	3, 8
k) Implementing measures for avoiding firewall evasion.	3, 8
l) Describing firewall security best practices.	3, 8

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

a) Explaining different types of intrusions and their indications.	3, 8
b) Explaining IDPS.	3, 8

c) Describing role of IDPS in network defense.	3, 8
d) Describing functions, components, and working of IDPS.	3, 8
e) Explaining various types of IDS implementation.	3, 8
f) Describing staged deployment of NIDS and HIDS.	3, 8
g) Describing fine-tuning of IDS by minimizing false positive and false negative rate.	3, 8
h) Discussing common IDS implementation mistakes and their remedies.	3, 8
i) Explaining various types of IPS implementation.	3, 8
j) Discussing requirements for selecting appropriate IDSP product.	3, 8
k) Describing technologies complementing IDS functionality.	3, 8

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

a) Explaining Virtual Private Network (VPN).	3, 8
b) Importance of establishing VPNs.	3, 8
c) Describing various VPN components.	3, 8
d) Describing implementation of VPN concentrators and their functions.	3, 8
e) Explaining different types of VPN technologies.	3, 8
f) Discussing components for selecting appropriate VPN technology.	3, 8
g) Explaining core functions of VPN.	3, 8
h) Explaining various topologies for implementation of VPN.	3, 8
i) Discussing various VPN security concerns.	3, 8
j) Discussing various security implications for to ensure VPN security and performance	3, 8

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

a) Discussing various wireless standards.	3, 8
b) Describing various wireless network topologies.	3, 8
c) Describing possible use of wireless networks.	3, 8
d) Explaining various wireless network components.	3, 8
e) Explaining wireless encryption (WEP, WPA, WPA2) technologies.	3, 8
f) Describing various authentication methods for wireless networks.	3, 8
g) Discussing various types of threats on wireless networks.	3, 8
h) Creating of inventory for wireless network components.	3, 8
i) Discussing the appropriate placement of wireless AP.	3, 8
j) Discussing the appropriate placement of wireless antenna.	3, 8
k) Monitoring of wireless network traffic.	3, 8

Revision Date: **Spring 2020**

Approved By Academic Dean Date: _____ Reviewed By Director of Academic Programs Date: _____

l) Detecting and locating rogue access points.	3, 8
m) Discussing RF interference.	3, 8
n) Describing various security implications for wireless networks.	3, 8

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

a) Discussing the importance of network traffic monitoring.	3, 8
b) Discussing techniques used for network monitoring and analysis.	3, 8
c) Discussing appropriate position for network monitoring.	3, 8
d) Explaining how to perform network monitoring system using managed switch.	3, 8
e) Defining network traffic signatures.	3, 8
f) Baselining for normal traffic.	3, 8
g) Discussing the various categories of suspicious traffic signatures.	3, 8
h) Listing various techniques for attack signature analysis.	3, 8
i) Explaining Wireshark components, working and features.	3, 8
j) Demonstrating the use of various Wireshark filters.	3, 8
k) Demonstrating the monitoring LAN traffic against policy violation.	3, 8
l) Demonstrating the security monitoring of network traffic.	3, 8
m) Demonstrating the detection of various attacks using Wireshark.	3, 8
n) Discussing network bandwidth monitoring and performance improvement.	3, 8

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

a) Defining risk and risk management.	3, 8
b) Describing various risk management frameworks.	3, 8
c) Explaining vulnerability management.	3, 8
d) Describing the phases involved in vulnerability management.	3, 8
e) Explaining vulnerability assessment and its importance.	3, 8
f) Discussing internal and external vulnerability assessment.	3, 8
g) Selecting appropriate vulnerability assessment tools.	3, 8
h) Describing vulnerability reporting, mitigation, remediation and verification.	3, 8

Competency 13. The student will be able to demonstrate an understanding of data backup and recovery by:	
a) Describing data backup.	3, 8
b) Determining the appropriate backup medium for data backup.	3, 8
c) Understanding RAID backup technology and its advantages.	3, 8
d) Describing RAID architecture.	3, 8
e) Describing various RAID levels and their use.	3, 8
f) Describing Storage Area Network (SAN) backup technology and its advantages.	3, 8
g) Describing various types of NAS implementation.	3, 8

Competency 14. The student will be able to demonstrate an understanding of network incident response and management by:	
a) Defining Incident Handling and Response (IH&R).	3, 8
b) Describing the roles and responsibilities of Incident Response Team (IRT).	3, 8
c) Describing the Incident Handling and Response (IH&R) process.	3, 8
d) Explaining the goals of forensic investigation.	3, 8
e) Describing the forensics investigation methodology.	3, 8