Miami Dade College

Course Description

CTS1120 | Cybersecurity Fundamentals | 4.00 credits

This course provides a foundation of knowledge in the information technology security field. The student will learn general network security concepts; compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; cryptography. Hands on training benefits the novice as well as the experienced network professional. No prerequisite but prior knowledge in Networking Technologies recommended.

Course Competencies:

Competency 1: The student will demonstrate understanding and knowledge of threats, attacks, and vulnerabilities by:

1. Identifying various threat actors, including hacktivists, cybercriminals, insiders, nation-states, and nature.
2. Discussing the adversary model for each threat.
3. Comparing and contrasting different types of attacks, including social engineering, password cracking, malware, sniffing, spoofing, session hijacking, denial of Service (DoS), and distributed denial of service (DDoS).
4. Explaining attack timing, Advanced Persistent Threats (APT), and zero-day vulnerabilities.
5. Defining covert channels.
6. Analyzing indicators of compromise and determine the type of malware, for a given scenario.
7. Explaining penetration testing concepts.
8. Explaining vulnerability scanning concepts.
9. Explaining the impact associated with types of vulnerabilities.

Competency 2: The student will demonstrate understanding and knowledge of security technologies and tools by:

1. Installing and configuring hardware and software-based network components to support organizational security.
2. Using appropriate software tools to assess an organization's security posture, for a given scenario.
3. Troubleshoot common security issues for a given scenario.
4. Analyzing and interpreting outputs from security technologies for a given scenario.
5. Deploying mobile devices securely for a given scenario.
6. Implementing secure protocols for a given scenario.

Competency 3: The student will demonstrate understanding and knowledge of secure architecture and design by:

1. Explaining use cases and purpose for frameworks, best practices, and secure configuration guides.
2. Implementing secure network architecture concepts for a given scenario.
3. Implement secure systems design for a given scenario.
4. Explaining the importance of secure staging deployment concepts.
5. Explaining the security implications of embedded systems.
6. Selecting the appropriate solution to establish host security.
7. Implementing the appropriate controls to ensure data security.
8. Summarizing secure application development and deployment concepts.
9. Summarizing cloud and virtualization concepts.
10. Explaining how resiliency and automation strategies reduce risk.
11. Explaining the importance of physical security controls (man in the middle).
12. Explaining Session and Exception management.

Competency 4: The student will demonstrate understanding and knowledge of access control and identity

management by:

1. Comparing and contrasting identity and access management concepts.
2. Installing and configuring identity and access services for a given scenario.
3. Implementing identity and access management controls for a given scenario.
4. Identifying Access Control Models (MAC, DAC, RBAC, Lattice).
5. Differentiating standard account management practices, for a given scenario.
6. Installing and configuring security controls when
7. performing account management, based on best practices.

Competency 5: The student will demonstrate understanding and knowledge of risk management by:

1. Explaining the importance of policies, plans, and procedures related to organizational security.
2. Summarizing business impact analysis concepts.
3. Explaining risk management processes and concepts.
4. Identifying relevant countermeasures for risk mitigation.
5. Following incident response procedures for a given scenario.
6. Summarizing basic concepts of forensics.
7. Explaining disaster recovery and continuity of operations concepts.
8. Comparing and contrasting various types of controls.
9. Carrying out data security and privacy practices for a given scenario.

Competency 6: The student will demonstrate understanding knowledge of cryptography by:

1. Comparing and contrasting basic cryptography concepts (Confidentiality, Integrity, Authentication, Non-Repudiation).
2. Comparing and contrasting symmetric cryptography and public key cryptography
3. Comparing block and stream encryption methods.
4. Compare and contrast the different modes of block encryption algorithms.
5. Identifying cryptographic standards, such as the FIPS 140 series.
6. Compare and contrast the various attacks against cryptography (including brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)
7. Comparing cryptographic algorithms such as DES, 3DES, Two Fish, AES, DH, RSA ECC, etc.
8. Explaining implementation errors in cryptography (e.g., WEP).
9. Using appropriate cryptographic algorithms.
10. Explaining hashing functions and their properties, such as pre-image and collision resistance.
11. Listing the uses of hash functions in cryptography, including integrity checking and message authentication codes.
12. Comparing various hash algorithms (MD4, MD5, SHA1, SHA2, SHA3).
13. Identify key management issues (including key
14. escrow, key revocation, and various trust models)
15. Implementing a Public Key Infrastructure.

Competency 7: The student will demonstrate an understanding of cybersecurity principles by:

1. Explaining the cybersecurity goals: confidentiality, integrity, availability, authenticity, accountability, non-repudiation, and privacy.
2. Defining the principles of cybersecurity (isolation, encapsulation, modularity, simplicity of design, minimization of implementation, open design, complete mediation, layering, defense-in-depth, Least Privilege, Fail Safe Default/Fail Secure, Least Astonishment, Minimize Trust Surface, usability, trust relationships, separation of duties).
3. Describe the importance of each principle and how it enables the development of security mechanisms to implement desired security policies.
4. Explaining the Security Life-Cycle.
5. Describing Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security).
6. Identifying Cyber Defense Partnerships (Federal, State, Local, Industry).

Competency 8: The student will demonstrate an understanding of operational and organizational security by:

1. Examining the placement of security functions in a system and describing the strengths and weaknesses.
2. Develop contingency plans for various-size organizations to include business continuity, disaster recovery, and incident response.
3. Describing the roles of personnel in planning and managing security.
4. Identifying Legal and ethical issues associated with the cybersecurity profession and cyber threats.

Learning Outcomes:

1. Communication
2. Information Literacy
3. Ethical Issues