

# Cybersecurity I

Level 2: Student may have explored previously; first pathway specific course

Pathway(s): Networking Systems & Security

## Description

Cybersecurity I is a course intended to teach students the basic concepts of cybersecurity. The course places an emphasis on security integration, application of cybersecurity practices and devices, ethics, and best practices management. The fundamental skills in this course cover both in house and external threats to network security and design, how to enforce network level security policies, and how to safeguard an organization's information. Upon completion of this course, proficient students will demonstrate an understanding of cybersecurity concepts, identify fundamental principles of networking systems, understand network infrastructure and network security, and be able to demonstrate how to implement various aspects of security within a networking system.

## Student Learning Outcomes

### Cybersecurity Fundamental Concepts

- 1) Analyze ethical security practices, including but not limited to the issues of
  - a. Data security
  - b. Confidentiality
  - c. Integrity
  - d. Availability
  - e. Authentication
  - f. Nonrepudiation
  - g. Physical security
  - h. HIPPA Laws
  - i. Payment Card Industry (PCI) Compliance
- 2) Understand the importance of ISO27000 standards
- 3) Research current events on breaches with focus on particular Information Assurance (IA) areas that were compromised
- 4) Analyze security threats, vulnerabilities, and exploits
  - a. Explain how they impact an organization

### Risk Management Techniques

- 5) Read and interpret technical information to define risk management and how it applies to information security
- 6) Perform a simulated risk assessment by using the common industry framework from ISO

### Access Controls

- 7) Explain the core concepts of access control as they relate to authentication and authorization
- 8) Analyze the use of administrative, logical (technical) and physical controls applied to systems and organizations

- 9) Demonstrate the use of access controls that apply to user account management, including basic and advanced techniques

### Fundamental Principles of Networking

- 10) Identify and describe common Local Area Network (LAN) methodologies
- 11) Analyze the various LAN topologies including perimeter networks which may include the use of a Demilitarized zone (DMZ)
- 12) Indicate and explain the standards of Ethernet
- 13) Describe the characteristics of LAN cabling
- 14) Explain industry standards used in wireless networks including security protocols used to protect the wireless network
- 15) Describe how routing protocols are used in the differences between static and dynamic methods of routing
- 16) Explain how to install and configure Routing and Remote Access Service (RRAS) to function as a network router and how to install and configure Routing Information Protocols
- 17) Choose between technologies and topologies used for wide area networks (WAN)
- 18) Explain how the different types of personal and small business internet connectivity has changed throughout history and identify current internet systems most commonly used

### Fundamental Principles of Open Systems and Internet (OSI) Protocol

- 19) Summarize the common OSI model and the function used by each layer
- 20) Analyze and describe the differences between the Transmission Control Protocol/ Internet Protocol (TCP/IP) and OSI models for networking
- 21) Define and describe the various services used by networks for the transmission of data such as DNS, NAT, and DHCP
- 22) Analyze the differences among the addressing techniques used by networks, including IPv4 and basic IPv6
- 23) Demonstrate the use of subnets in an organizations network environment
- 24) Research the features and requirements of a working model of a client server network and how services function in a networked window environment

### Network Infrastructures and Network Security

- 25) Compare and contrast the differences and uses of the Internet, Intranets, and Extranets
- 26) Research and describe the most common methods and technology used to secure networks
- 27) Investigate and distinguish among the following common methods to secure a network
  - a. VPNs for remote access
  - b. Firewalls
  - c. Perimeter network designs
  - d. Preventative technologies

### Fundamental Network Components of Cybersecurity

- 28) Research the different applications of network security devices
  - a. Optical drives
  - b. Combo drives and burners
  - c. Connection types

- d. Hard drives
  - e. Solid state/flash drives
  - f. RAID types
  - g. Floppy drive
  - h. Tape drive
  - i. Media capacity
- 29) Demonstrate secure networking techniques by designing a simple secure network

### Basic and Advanced Command Prompts

- 30) Analyze the various networking commands used to test and examine networks
- 31) Research the features and uses of command line utilities to configure and examine networking services and construct a flow chart that a security analyst could reference

### Application Security and Host Systems

- 32) Explore various operating and file systems used in networks
- 33) Identify the pros and cons of how systems are designed to provide the security necessary in a multiuser environment
- 34) Describe the most common security threats to computer systems, such as social engineering, malware, phishing, viruses, etc.
- 35) Distinguish among the following common prevention methods to secure a computer system
- a. Physical security (e.g., lock doors, tailgating, biometrics, badges, key fobs, retinal, etc.)
  - b. Digital security (e.g., antivirus, firewalls, antispyware, user authentication, etc.)
  - c. User education
  - d. Principles of least privilege
- 36) Report on recent threats and vulnerabilities to systems in networking environments
- 37) Differentiate between threats and vulnerabilities and what constitutes a network attack
- 38) Identify how to differentiate between the different types of applications attacks
- 39) Explain ways to install and configure antivirus software

### Security Administration

- 40) Research the features and requirements of common security procedures used to protect system resources on a network
- 41) Describe the differences among various methods to create baseline security measures
- 42) Research storage devices and backup media outlining their purpose, characteristics, proper maintenance, and methods used to back up and protect data from unauthorized use and access of data
- a. Optical drives
  - b. Combo drives and burners
  - c. Connection types
  - d. Hard drives
  - e. Solid state/flash drives
  - f. RAID types
  - g. Floppy drive
  - h. Tape drive
  - i. Media capacity

- 43) Demonstrate the methods used to protect against unauthorized use of files
- 44) Configure file and folder permissions
- 45) Analyze various protocols and services used by systems for securing them in a network environment

### Cryptology

- 46) Illustrate cryptology's historical evolution including but not limited to public key infrastructures, asymmetric and symmetric encryptions
- 47) Analyze common methods and use of cryptology to protect data