

Network Security

Apply Problem-solving and Critical Thinking Skills to Network Security 1.0

- 1 Describe methods to determine priorities in establishing and maintaining a computer network 1.1
- 2 Prepare a plan of work and schedule network technology tasks 1.2
- 3 Apply problem-solving processes to network technology tasks (i.e., bottom-up, divide-and-conquer, top-down, etc.) 1.3
- 4 Prepare and present technical information for nontechnical and technical audiences in writing and verbally 1.4

Maintain a Safe and Environmentally Conscious Work Environment

- 1 Identify personal responsibility for developing and maintaining a safe and healthy work environment 2.1
- 2 Use equipment, materials, and tools commonly used in the field of network security correctly and safely 2.2
- 3 Identify ergonomic solutions to prevent injuries common to network security tasks 2.3
- 4 Determine safe working practices to avoid or eliminate electrical hazards and physical injuries 2.4
- 5 Identify techniques used to manage power consumption in the networked environment (i.e., cloud-based, software defined, etc.) 2.5
- 6 Explain environmental considerations when disposing of computer/network components 2.6
- 7 Describe and resolve most common electrostatic discharge (ESD) hazards in a network environment 2.7

Specify Network Security Best Practices, Risks, and Threats

- 1 Perform risk management activities (e.g., define risk, determine risk level, and identify methods to address risk) 3.1
- 2 Define policies to manage system and data availability, confidentiality, and integrity 3.2

-
- 3 Classify data according to its sensitivity and criticality (i.e., mission critical, protect cafeteria menu vs. personal, financial and health information, trade secrets, etc.)** 3.3

 - 4 Identify security threats related to computer data, hardware, and software (i.e., denial of service, eavesdropping, intrusion, unauthorized access, unauthorized use, etc.)** 3.4

 - 5 Explain the importance of physical security of computer and network hardware following best practices (i.e., cameras, locks, USB port blocking, etc.)** 3.5

 - 6 Describe network threats (i.e., denial of service, email spoofing, hacking/cracking, intrusion, malware, phishing, social engineering, spamming, system vulnerabilities, website defacement, etc.)** 3.6

 - 7 Describe best practices to protect against network threats (i.e., access control, antivirus software, awareness and training, encryption, firewalls, incident detection systems/tools, intrusion detection prevention, network segmentation, port/service blocking, software updates/patches, etc.)** 3.7

 - 8 Define best practices to protect data at rest, data in transit, and data during processing** 3.8

 - 9 Describe password best practices (i.e., age, complexity, history, length, lockout, etc.)** 3.9

 - 10 Analyze authentication methods used to secure access to the network [i.e., biometrics, key cards, multi-factor authentication (MFA), passwords, single sign-on (SSO), two-factor authentication (2FA), etc.]** 3.1

 - 11 Identify best practices for access control (i.e., changing default passwords, disabling unused accounts, least privileges, privileged account management, role-based access control, etc.)** 3.12
-

Investigate Legal and Ethical Issues Related to Network Security

- 1 Explore issues regarding intellectual property rights including software licensing and software duplication [i.e., Business Software Alliance, Creative Commons, Digital Right Management (DRM), <https://www.ip-watch.org/about/>, <https://www/eff.org/>, etc.]** 4.1

 - 2 Differentiate among freeware, open source, proprietary, and shareware software relative to legal and ethical issues** 4.2

 - 3 Identify issues, laws, and trends affecting data and privacy [e.g., Certified Network Professional (CNP), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and Sarbanes-Oxley Act (SOX)]** 4.3

 - 4 Describe acceptable use of industry-related data, private and public networks, and social networking** 4.4
-

Demonstrate Basic Computer Mathematics Required for Network Security

- 1 Explain the function of base number systems in mathematics as it relates to network technology** 5.1
- 2 Perform decimal to binary and binary to decimal conversions** 5.2
- 3 Perform decimal to hexadecimal and hexadecimal to decimal conversions** 5.3
- 4 Perform hexadecimal to binary and binary to hexadecimal conversions** 5.4
- 5 Determine the appropriate method to perform conversions (e.g., paper-pencil and electronic resources)** 5.5
- 6 Apply basic Boolean logic for actions such as Google searches and scripting (e.g., “and,” “nor,” “not,” and “or”)** 5.6

Describe the Development and Evolution of Computers and Network Security

- 1 Describe a computer and its components and functions** 6.1
- 2 Explain the historical evolution of the computer and computer networks** 6.2
- 3 Explain how the development of computers has impacted modern life** 6.3
- 4 Identify the components and structure of an information system [e.g., applications, media (cables, fiber, and wireless), network devices (router, switches, etc.), operating systems, and servers]** 6.4
- 5 Discuss future trends and societal impacts in digital devices and network technology [i.e., Internet of Things (IoT), privacy, etc.]** 6.5

Demonstrate Network Media and Topologies

- 1 Specify the characteristics and main features of various networking topologies (e.g., bus, mesh, ring, and star)** 7.1
- 2 Compare proper physical network topology** 7.2
- 3 Identify appropriate connectors, media types, and uses for various networks** 7.3
- 4 Compare physical and virtual networks [i.e., Software-Defined Wide-Area Network (SD-WAN), Virtual Local Area Network (VLAN), etc.]** 7.4
- 5 Specify the characteristics of physical network technologies including cable types, length, speed, and topology** 7.5
- 6 Specify the characteristics of wireless network technologies including frequency, speed, topology, and transmission (i.e., local area, metropolitan area, wide area networks, etc.)** 7.6
- 7 Describe the structure of the internet (network of networks)** 7.7

8 Identify the features, functions, and purpose of commonly used network components [i.e., routers, modem, switches, bridges, hubs, NIC (network interface card), etc.] 7.8

Describe Network Protocols and Standards

1 Describe the parts and use of a Media Access Control (MAC) address 8.1

2 Describe the characteristics, name, and use of the seven layers of the Open Systems Interconnect (OSI) model 8.2

3 Describe the characteristics, name, and use of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model 8.3

4 Explain the purpose of dynamic and static routing protocols 8.4

5 Explain the concept of ports and identify the three port ranges used in networking services and protocols [i.e., dynamic/private (49152-65535), system (0-1023), user (1024-49151), etc.] 8.5

6 Describe standard network ports and protocols [e.g., Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Point-of-Presence (POP), Simple Mail Transfer Protocol (SMTP), etc.] 8.6

7 Describe the applications and characteristics of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) 8.7

8 Differentiate IPv4/IPv6 addresses and their corresponding subnet masks [i.e., classful networks, Classless Interdomain Routing (CIDR), private vs public IP] 8.8

9 Summarize the basic characteristics and protocols of Metropolitan Area Network (MAN), Software-Defined Wide Area Network (SD-WAN), and Wide Area Network (WAN) technologies [i.e., Asynchronous Transfer Mode (ATM), frame relay, Multiprotocol Label Switching (MPLS), etc.] 8.9

10 Describe remote access protocols and services 8.1

11 Describe the function and purpose of security protocols [i.e., Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), tunneling, Virtual Private Network (VPN), etc.] 8.11

12 Explain the importance of proper documentation in accordance with industry standards 8.12

Configure a Basic Network

1 Design a network map with virtual and physical segments 9.1

2 Construct dynamic and static routes 9.2

3 Explain proper labeling in accordance with industry standards (i.e., cable, device, rack, wall plates, etc.) 9.3

-
- 4 Describe the components needed and purpose to build fault tolerance into a network** 9.4
 - 5 Describe the purpose of a disaster recovery plan for a network** 9.5
 - 6 Install and configure a physical and/or virtual networked system (i.e., Linux/UNIX, Windows, etc.)** 9.6
 - 7 Configure network cards, network settings, and operating system** 9.7
 - 8 Configure and connect devices to the network (i.e., computers, printers, routers, switches, etc.)** 9.8
 - 9 Identify the appropriate tools to use for diagnostic tasks or network repair (i.e., execute Traceroute, ipconfig, Ping, etc.)** 9.9
-

Harden a Network

- 1 Identify common network threats (i.e., denial of service, eavesdropping, intrusion, probing, unauthorized access, etc.)** 10.1
 - 2 Identify physical network threats [i.e., disrupting media (like cutting fiber), environmental/power disruption, unauthorized access to devices, etc.]** 10.2
 - 3 Describe the benefits and purpose of segmenting networks** 10.3
 - 4 Describe the benefits of disabling ports and network services** 10.4
 - 5 Describe the techniques to secure a Wi-Fi network [i.e., Extensible Authentication Protocol (EAP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), etc.]** 10.5
 - 6 Compare the various types of firewalls and their uses (i.e., application, packet filtering, stateful, etc.)** 10.6
 - 7 Describe the benefits, disadvantages, and purpose of using a proxy service** 10.7
 - 8 Describe the benefits, disadvantages, and purpose of using network intrusion detection/prevention systems [i.e., Intrusion Detection System / Intrusion Prevention System (IDS/IPS), etc.]** 10.8
 - 9 Modify an existing network diagram with appropriate network hardening devices or systems** 10.9
-

Perform Network Maintenance and Resolve Issues

- 1 Identify maintenance tasks and create a schedule** 11.1
- 2 Describe the purpose and benefits of network utilities [i.e., Network Statistics (Netstat), Name Server Lookup (Nslookup), Ping, Traceroute, etc.]** 11.2
- 3 Demonstrate the use of visual indicators (i.e., indicator lights on devices, etc.) and diagnostic utilities (i.e., Wireshark, etc.) to interpret problems** 11.3

4 Identify connectivity issues in various node environments (i.e., smart phones, switches, tablets, Linux/UNIX, Windows, etc.) 11.4

5 Identify and resolve network issues (i.e., cable failure, connection failure, environmental, misconfigurations, power, user error, etc.) 11.5

6 Identify common tools and methods of monitoring a network 11.6