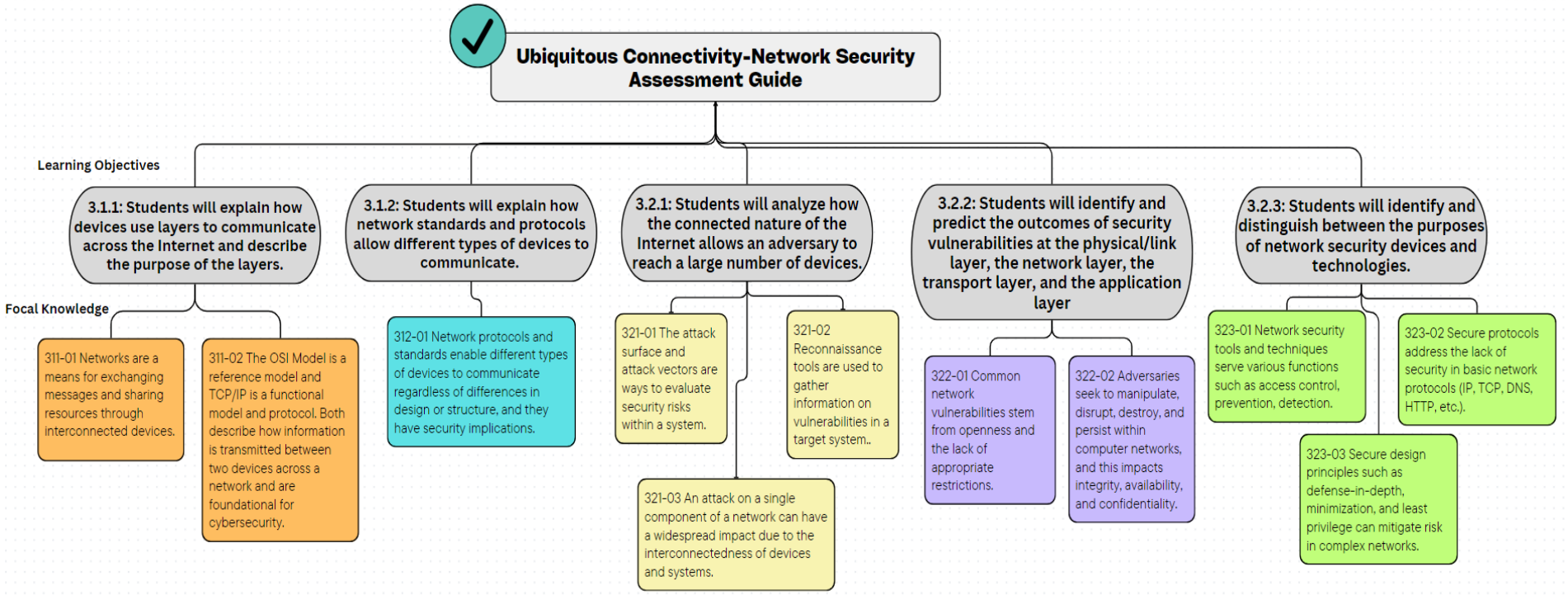
Ubiquitous Connectivity (Network Security) Assessment Guide

7/8/24

3.1.1: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers.
311-01 Networks are a means for exchanging messages and sharing resources through interconnected devices.
311-02 The OSI Model is a reference model and TCP/IP is a functional model and protocol. Both describe how information is transmitted between two devices across a network and are foundational for cybersecurity.
3.1.2: Students will explain how network standards and protocols allow different types of devices to communicate.
312-01 Network protocols and standards enable different types of devices to communicate regardless of differences in design or structure, and they have security implications.
3.2.1: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices.
321-01 The attack surface and attack vectors are ways to evaluate security risks within a system.
321-02 Reconnaissance tools are used to gather information on vulnerabilities in a target system.
321-03 An attack on a single component of a network can have a widespread impact due to the interconnectedness of devices and systems.
3.2.2: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network layer, the transport layer, and the application layer.
322-01 Common network vulnerabilities stem from openness and the lack of appropriate restrictions.
322-02 Adversaries seek to manipulate, disrupt, destroy, and persist within computer networks, and this impacts integrity, availability, and confidentiality.
3.2.3: Students will identify and distinguish between the purposes of network security devices and technologies.
323-01 Network security tools and techniques serve various functions, such as access control, prevention, and detection.
323-02 Secure protocols address the lack of security in basic network protocols (IP, TCP, DNS, HTTP, FTP, etc.).
323-03 Secure design principles, such as defense-in-depth, minimization, and least privilege, can mitigate risk in complex networks.


Ubiquitous Connectivity-Network Security Assessment Guide
Learning Objectives
3.1.1: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers.
3.1.2: Students will explain how network standards and protocols allow different types of devices to communicate.
3.2.1: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices.
3.2.2: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network layer, the transport layer, and the application layer
3.2.3: Students will identify and distinguish between the purposes of network security devices and technologies.
Focal Knowledge
311-01 Networks are a means for exchanging messages and sharing resources through interconnected devices.
311-02 The OSI Model is a reference model and TCP/IP is a functional model and protocol. Both describe how information is transmitted between two devices across a network and are foundational for cybersecurity.
312-01 Network protocols and standards enable different types of devices to communicate regardless of differences in design or structure, and they have security implications.
321-01 The attack surface and attack vectors are ways to evaluate security risks within a system.
321-02 Reconnaissance tools are used to gather information on vulnerabilities in a target system..
321-03 An attack on a single component of a network can have a widespread impact due to the interconnectedness of devices and systems.
322-01 Common network vulnerabilities stem from openness and the lack of appropriate restrictions.
322-02 Adversaries seek to manipulate, disrupt, destroy, and persist within computer networks, and this impacts integrity, availability, and confidentiality.
323-01 Network security tools and techniques serve various functions such as access control, prevention, detection.
323-02 Secure protocols address the lack of security in basic network protocols (IP, TCP, DNS, HTTP, etc.).
323-03 Secure design principles such as defense-in-depth, minimization, and least privilege can mitigate risk in complex networks.

3.1.1: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers.

Focal Knowledge	311-01 Networks are a means for exchanging messages and sharing resources through interconnected devices.
Knowledge Statements	• Data are bits that are represented as ones and zeros. • A network is composed of two or more devices that are connected via a network interface card (NIC). • NICs are hardcoded with a physical address. • The purpose of linking the computer devices together into a network is to share data and resources. • A physical connection between devices can be established using copper cable, fiber optics, or wireless media to transport bits. • Protocols are agreed upon rules used by devices so that they know what to do with the data. • A computer network can be as small as two laptops connected through an Ethernet cable or as complex as the Internet, which is a global system of computer networks. • A computer network must be physically and logically designed in such a way that makes it possible for the underlying network components to communicate with each other. • The core components of computer networks are network-capable devices, physical links and communication protocols. • Network devices include modems, routers, personal computers (PCs), servers, firewalls, switches, and gateways. • Network switches permit multiple devices to be connected and to exchange packets. • Routers connect two or more networks or subnetworks. • A network gateway connects networks that use different protocols. • A link is the transmission medium used for connecting the nodes and enabling them to transmit to each other. Links can be wired, wireless, or optical, such as an Ethernet cable or a wireless signal. • Links can be configured in different ways, both physically and logically, and the network topology dictates the way links and nodes relate to each other. • Communication protocols are the rules that all nodes on the network must follow for information transfer. • Devices attached to computer networks use Internet Protocol (IP) addresses that are resolved into hostnames through a domain name system server to communicate with each other over the Internet and on other computer networks. • Port numbers are logical addresses used to connect data to a service. • Some common port numbers are port 80 for http, port 25 for SMTP, port 443 for https, ports 20 and 21 for FTP, and port 3389 for RDP. • There are numerous network protocols, but TCP/IP is the predominant network protocol. • Once a connection is established, communication protocols, such as TCP/IP, Simple Mail Transfer Protocol and Hypertext Transfer Protocol, are used to exchange data between the networked devices. • Packets are a logical unit of data that are grouped together and transferred over a computer network using a protocol • Packet-based switching was developed to overcome the limitations of circuits, which are direct connections.

	• Packet-based switching is efficient and scalable. • Packets contain header data, which includes among other things, the source and destination address. • Packets can take different routes, can arrive in different order, and are resorted at the destination. • The composition of IP packets includes header data and a payload. • Routing is the process of selecting a path for packets in a network or across multiple networks.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Given a network diagram, explain… • Diagram a basic functioning network that can exchange messages and share resources. • Given a network diagram, identify the function of network devices in exchanging messages and sharing resources. • Troubleshoot device connectivity issues.
Focal Knowledge	311-02 The OSI Model is a reference model and TCP/IP is a functional model and protocol. Both describe how information is transmitted between two devices across a network and are foundational for cybersecurity.
Knowledge Statements	• The OSI Model is not a protocol, it is a representational model of what a communication protocol should include. • The OSI model serves as a common basis for the coordination of standards development for the purpose of system interconnection. • TCP/IP is a protocol and a functional model of network communication. • Layer 1 of the OSI Model is the Physical Layer and it functions to establish, maintain and terminate communication between two endpoints so that data bits can physically be transmitted over a communication channel. • The Physical Layer has a network interface controller, which is a hardware component that connects a computer to a network allowing data to be sent and received. • The Physical Layer defines the connection type (wired or wireless), the transmission medium (fiber optic, copper wire, etc.), and the signal type (analog or digital) used in data transmission for sending a signal (whether it is electrical, light, or radio impulses that become data bits). • Devices at the Physical Layer include modems, multiplexers, repeaters, and transceivers. • Ethernet (IEEE 802.3) is the most common Layer 1 protocol. Ethernet is an example of a protocol that operates at multiple layers (it operates at layer 2). • A computer can have more than one network interface controller. A PC normally has at least two network interfaces (Ethernet and Wi-Fi). If Bluetooth is enabled, that would be a third interface. • Layer 2 of the OSI Model is the Data Link Layer and its function is to provide reliable data transmission over a physical communication link. • The Data Link Layer is concerned with local delivery of data between devices on the same LAN. • MAC (Media Access Control) addresses are used to deliver data. • MAC addresses are unique identifiers of a network interface card assigned during manufacture. • Given that devices can have more than one network interface, they also have more than one MAC address. • To reliably transmit data, the Data Link Layer needs a way to give packets to the Network Layer. This is called framing. • Framing is the encoding, decoding and organizing of data bits in the Data Link Layer.

	• A frame is a protocol data unit, or protocol data packet, which is the smallest unit of bits on a layer 2 network. Frames contain basic data, such as a source address, a destination address, and a payload, which is often called a header. Each frame also includes the MAC address of the source and the MAC address of the destination. • Layer 3 of the OSI Model is the Network Layer and it functions to transfer data from a host on one network to a destination host on a different network. • Layer 3 is responsible for data transmission, the quality of data, and determining the best path for data to be transmitted from source to destination. • Layer 3 uses the Internet Protocol (IP) as the standard for addressing and routing packets (called datagrams). • Layer 3 moves data segments in the form of packets from one network to another using IP addressing, which is a logical address. • The data are moved from one IP address to the other using IP routing. • There are various protocols for IP routing. The aim of all of them is to route data efficiently. • Routers are a type of gateway connecting networks or connecting to the Internet. • Network switches operate at either Layer 2 of the OSI Model (using MAC addresses within a LAN or VLAN) or Layer 3 (using IP addresses). A Layer 3 switch has routing capabilities. • The Address Resolution Protocol (ARP) is a process of connecting MAC addresses to IP addresses. • At the Data Link Layer, a MAC table identifies MAC addresses to a port. • Dynamic Host Configuration protocol (DHCP) is a mechanism for dynamically assigning IP addresses within a network as opposed to manually assigning IP addresses. • DNS is a mechanism for resolving domain names to IP addresses and vice versa. • The function of Layer 4 is to manage network traffic to ensure complete data transfer. • The Transport Layer segments the data stream into packets that can be sent over the network and reconstructs the data on the other end. • As packets come in, the Transport Layer reorders the packets by segment number so that data are presented in the correct order. • The Transport Layer uses port numbers to determine which application receives the packet, allowing for the reliable delivery of data. • While an IP address identifies a device, the port identifies a service or application within that device. • Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are protocols in Layer 4. • For devices to communicate using TCP, they use TCP ports. For devices to communicate using UDP, they use UDP ports. • TCP uses a 3-way handshake in which an initial request is sent, an acknowledgment is returned, and an agreement confirms the process. • UDP does not use the 3-way handshake and is less reliable than TCP. UDP is faster because it begins by sending data. • Layer 5 of the OSI Model is the Session Layer and it establishes, manages, and ends connections between local and remote applications. • A session is a temporary, interactive exchange of information between two or more devices that are communicating over a network. • The Session Layer ensures that the session transfers the data being exchanged by synchronizing data transfer.

	• Layer 6 of the OSI Model, the Presentation Layer, ensures that data is in a usable format. • The Presentation Layer is known as the data translator. It converts data from network formats into application formats and vice versa. This format is generic and not application specific. For example, if you receive a text file encoded in XML, but your system uses ASCII or Unicode, the Presentation Layer translates the data. • The Presentation Layer also formats and encrypts data to be sent across the network. • Encryption, translation, and compression occur in the Presentation Layer. Protocols specify how this translation will take place. • Common Presentation Layer protocols are TLS and SSL. • Layer 7 of the OSI Model, the Application Layer, is where applications and network services meet. • The Application Layer provides services to end-users, such as web browsing, email, chat, access to printers and other network resources. • Layer 7 ensures an application can effectively communicate with other applications on different computer systems and networks. • When a user submits a request through an application, the Application Layer communicates it to the Presentation Layer using a protocol. • Web browsers and email clients use protocols such as HTTP and SMTP to enable communication in Layer 7. • Each layer of the OSI Model can only communicate with the layers above and below it. • Cybersecurity attacks can occur at any of the OSI Model layers. • The Physical Layer is susceptible to packet sniffing and eavesdropping. • MAC spoofing, MAC flooding, ARP spoofing, and ARP poisoning can occur at the Data Link Layer. • Layer 2 switches do not have security features. • Layer 3 switches can implement access control. • SYN floods and Smurf (DDoS) attacks can occur at the Transport Layer. • DDoS attacks can occur at the Network, Transport, Session, Presentation, and Application Layers. • The Application Layer is the most susceptible to attack because it is the source of sensitive data used by humans.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify protocols that operate at each layer of the OSI Model and the role of the protocol in transmitting information between two devices and provide a justification for the answer. • Identify devices that operate at each layer, the role of the device in transmitting information, and provide a justification for the answer. • Identify attacks on the transmission of information, the OSI Model layer involved and provide a justification. • Given an actual attack, diagnose which layer(s) of the network were exploited, the impact of information transmission, and provide a justification for the answer.

3.1.2: Students will explain how network standards and protocols allow different types of devices to communicate.

Focal Knowledge	312-01 Network protocols and standards enable different types of devices to communicate regardless of differences in design or structure and they have security implications.
Knowledge Statements	• Open standards are developed and maintained by independent organizations and can be implemented by any manufacturer. • Standards are used in the encoding of electronic communication (e.g. UTF-8). • Standards are technical specifications that detail how software and hardware components must work. • Standards enable the implementation of protocols, and each standard will include one or more sets of protocols. • Network protocols are the logical rules that govern how data is communicated. • Protocols span all layers of the OSI Model. • Application Layer protocols supply network services to applications. (e.g., HTTP). • Presentation Layer protocols translate data from different sources to the Application Layer (e.g., SSL, TLS). • Session Layer protocols establish, maintain and end communication sessions between applications (e.g., NetBIOS). • Transport Layer protocols transfer data between hosts and end systems, such as TCP and UDP. • Network Layer protocols convert data from the Transport Layer into packets and transfer them to the Data Link Layer (e. g. IP, IPSec). • Data Link protocols are responsible for communication between adjacent network nodes and move data in and out across the Physical Layer (e.g. IEEE 802.11, USB). • Physical Layer protocols connect two devices and send bits from one node to another using binary. • Protocols can be open or proprietary. • Proprietary protocols are developed by an organization to work with specific devices or technologies and may involve licensing. • Open (nonproprietary) protocols are developed, widely shared and typically supported by many different companies. • The Internet protocols are open and permit any computing device that follows the protocol to join the network of networks. • The Internet Engineering Task Force (IETF) is the open standards committee that maintains the Internet protocols. • The Internet was designed based on open protocols to encourage growth and development. • Security was not a consideration when the Internet protocols were originally developed. • Failure to comply with protocols and standards can have serious consequences for network performance and security. • Open Internet protocols include HTTP, DNS, TCP, and IP. • Domain Name System (DNS) is an open protocol operating at the Application Layer. • Protocol vulnerabilities are weaknesses or flaws in one of the communication protocols.

	• These vulnerabilities can be exploited by attackers to compromise the security of a system, steal sensitive information, or carry out other malicious actions. Examples of protocol vulnerabilities include buffer overflow, unencrypted data transmission, and insufficient authentication mechanisms. • Examples of attacks that exploited vulnerabilities in commonly used protocols include: • Eternal Blue exploits a protocol vulnerability at the Presentation Layer in the Microsoft OS implementation of the SMBv1 file sharing protocol. The vulnerability does not only apply to Microsoft Windows. Anything that uses the Microsoft SMBv1 server protocol, such as Siemens ultrasound medical equipment, is potentially vulnerable. SMBv1 was developed in the early 1980s as a way for networked computers to share access to files, printers, and ports. Windows implementations of SMBv1 allow buffer overflow. To carry out the EternalBlue exploit, attackers send a malicious SMBv1 data packet to a Windows server that has the vulnerability. The packet contains a payload of malware, which could then be rapidly disseminated to other devices installed with the vulnerable Microsoft software. • SSL/TLS stripping is a Adversary-in-the-Middle attack that exploits vulnerabilities in the SSL/TLS encryption protocol allowing attackers to steal sensitive information. The attacker downgrades a web connection from HTTPS to the less secure HTTP. • The ARP protocol is stateless and does not require authentication. ARP resolves Ipv4 addresses to MAC addresses. In an ARP cache poisoning attack, an attacker positions as an Adversary-in-the-Middle to reply to an ARP request with their MAC address. The deception works because on a local network segment the ARP reply is stored in the ARP cache. The attacker's reply to the ARP request makes the device appear to be the intended device. • The Remote Desktop Protocol (RDP) is a communication protocol for remote access and is not secure by default. BlueKeep (2019) is a remote code vulnerability that is exploited by an unauthenticated attacker connecting to a target system using RDP and then sending specially crafted requests. Microsoft released multiple patches for the vulnerability.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Provide a written explanation of the role of protocols in network communication. • Compare and contrast the roles of protocols and standards in network communication. • List features that distinguish proprietary protocols and standards from open protocols and standards and give examples of each. • Generate the steps for a successful DNS request given a specific application. • Given a network device with one structure and another network device with a different structure, explain how standards enable them to communicate. • Explain how buffer overflow exploits a protocol vulnerability.

3.2.1: Students will analyze how the connected nature of the Internet allows an adversary to many devices.

Focal Knowledge	321-01 The attack surface and attack vectors are ways to evaluate security risks within a system.

Knowledge Statements	• An attack involves the exploitation of a vulnerability by an adversary. • Vulnerabilities are weaknesses in a system, procedure, internal control, or implementation. • An attack is a malicious act that attempts to disrupt, deny, degrade, or destroy information system resources or the information itself. • An adversary is a person, group, organization, or government who works with malicious intent to defeat the security protections in a system and can include an insider seeking to exploit a vulnerability. • An attack vector is a point for an attacker to make unauthorized entry into a network or system. Common attack vectors include buffer overflow, exploited applications on websites and web servers, weak credentials, credential theft, default passwords, hardcoded passwords, missing or weak encryption, misconfigurations, unpatched software, social engineering, and supply chain attacks. • Humans are an attack vector. • The attack surface is the sum of the possible points, or attack vectors, where an unauthorized user can access a system and cause harm. Large, complex networks provide a potentially large attack surface for adversaries. (The smaller the attack surface, the easier it is to protect.) • The digital attack surface area encompasses all the hardware and software that connect to an organization's network. This includes applications, code, ports, servers, and websites, as well as shadow IT, which sees users bypass IT to use unauthorized applications or devices. • The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, and Universal Serial Bus (USB) drives. The physical attack surface includes carelessly discarded hardware that contains user data and login credentials, users writing passwords on paper, and physical break-ins. • The attack surface and attack vector are different but related. An attack vector is the method an adversary uses to gain unauthorized access by breaching user accounts or an organization's systems. The attack surface is the space that the adversary attacks or breaches. • Eternal Blue exploited a vulnerability in SMBv1. Because SMBv1 is widely used, this exploit has a large attack surface. WannaCry and NotPetya both used the Eternal Blue exploit. WannaCry spread ransomware at a rate of 10,000 devices per hour. • Boundary protection devices, such as firewalls, gateways, routers, intrusion detection systems, and intrusion prevention systems, provide a layer of defense. • Botnets are created when attackers take control of devices and organize them into a network that can be remotely managed to attack multiple devices simultaneously. • A denial-of-service attack blocks availability of a resource. • A data breach can impact the confidentiality, integrity, and/or availability of data. • A cyber incident is an action resulting in adverse effects on a network, system, or the information residing on it. • The principle of minimization decreases the number of ways an attacker can exploit a program or device. • The principle of layering is a strategy to slow the progress of an attacker. • The convergence of Information Technology (IT) and Operational Technology (OT) expands the attack surface to include sensors, controls, and communication. • Stuxnet is malware that exploited multiple vulnerabilities to attack industrial control system devices. • Risk is a function of the likelihood that a threat source will exploit a vulnerability, and the resulting harm of a successful attack.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Given a cyber attack, diagnose what happened, identify the attack vector(s), and justify the answer.

	• Explain the difference between attack vectors and the attack surface and why the difference matters. • Given a network, identify measures to reduce the attack surface. • Explain in writing (a narrative explanation or a diagram) how minimizing the attack surface reduces risk.
Focal Knowledge	321-02 Reconnaissance tools are used to gather information on vulnerabilities in a target system.
Knowledge Statements	• Reconnaissance is the systematic gathering of information about the target of a potential attack. • Reconnaissance involves scanning systems (hardware and software), web applications, network configuration (topology, IP addresses, DNS), security measures (firewalls, proxy servers, intrusion detection systems), and gathering information that leads to potential vulnerabilities that can be exploited. • Reconnaissance includes both passive data gathering (i.e., open source intelligence or OSINT) and active scanning and probing of a network or system. • Reconnaissance may include the purchase of information from private sources and databases. It may also include sources on the dark web or cybercrime black-markets. • Adversaries may search code repositories, scan databases, and use search engine queries. • Reconnaissance is a preliminary phase where the information gathered is used to create a plan of attack. • The knowledge, abilities, and resources of the adversary impact what attack vectors they plan to exploit. • Open source intelligence (OSINT) tools are used to collect publicly available data about a target. This data can include employee names, email addresses, job titles, physical locations, and other personal information. • OSINT tools include social media applications, search engines, websites, public databases, etc. • OSINT information can include key personnel in the organization, key suppliers and customers, IP addresses, registered domains, geolocation data, etc. • Reconnaissance tools gather raw data that can become actionable in a plan of attack. • Reconnaissance tools include network traffic analysis tools (Wireshark), specialized Google queries (Google dorking), specialized search engines (Shodan), network scanners (nmap), vulnerability scanners (Nessus, Burp Suite), and exploitation toolkits (Metasploit). • Spearphishing or phishing may be used to trick humans into sharing sensitive information about the target. Social engineering techniques are frequently used. • Reconnaissance is the first phase of the Cyber Kill Chain.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Compare and contrast passive gathering of data and active scanning of a network and discuss the ethics of each. • Given a need to gather reconnaissance information, identify possible sources of OSINT. • Given a list of information gathered during reconnaissance, list the ways it would be used to identify vulnerabilities in a target system and justify the answer. • Diagram an attack, accurately identify where reconnaissance tools are used, and justify the answer.

Focal Knowledge	321-03 An attack on a single component of a network can have a widespread impact due to the interconnectedness of devices and systems.
Knowledge Statements	• Network components are the hardware and software that function to connect devices and provide data transmission in a network. • Interconnection is the direct connection of two or more devices or systems for the purpose of sharing data or other resources. • Interconnection for sharing data or resources involves at least two endpoints and a mechanism for data to travel from one endpoint to the other. • Mobile devices and Internet of Things (IoT) devices become potential attack vectors when they connect to other devices or systems. • Connected devices and networks are inherently not secure. • A network interconnection is a link between two or more networks. • Network switches receive packets from devices and send them on through ports leading to the destination device. • Network switches can provide an attacker with access to an entire network segment or access to servers. • Routers transfer data packets between computer networks performing a traffic function. • Routers and Wi-Fi access points can provide an attacker with an entry point to a network. • The smallest hardware component of a network or a connected device can be a vulnerability. • Wireless connections provide easy connectivity and security concerns. • Bluetooth and NFC use radio waves to establish connections and to communicate across short distances. • Piggybacking, wardriving, bluesnarfing, air cracking, and evil twin are all attacks involving wireless networks. • Adversary-in-the-Middle is a technique in which a network device masquerading as a legitimate device enables the attacker to intercept messages, capture credentials, eavesdrop, and exploit vulnerabilities, such as injecting malware onto a device. • Worms are self-replicating code that propagate throughout a system. NotPetya is malware used by Sandworm that contained worm-like features to spread across computer networks. The NotPetya attack (2017) began as an attack on Ukraine, and then spread globally. • The Colonial Pipeline (2021) was attacked via a single exposed password for a VPN account. A ransomware attack followed, resulting in the shutdown of the pipeline even though the pipeline operational technology systems were not directly impacted. The ransomware targeted the information technology systems. • Supply chain compromise can take place through source code, software distribution, or other dependencies. The SolarWinds compromise (2020) involved injected code that was then distributed through software updates. • Third-party relationships involving vendors can be breached by adversaries. The Target data breach (2013) involved stolen credentials from an HVAC vendor.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer.

	• Diagram a network of networks, show how they are interconnected to allow the sharing of resources, then explain how an attack on a single network can spread because of network interconnectedness. • Explain how by directing an attack on a collection of devices (or even all devices on a network), an adversary can attack multiple devices simultaneously in hopes of compromising a few select devices. • Describe the role of network segmentation on interconnectedness. • Explain how worms propagate throughout interconnected systems. • Determine the role of network segmentation in mitigating the impact of interconnectedness during a cyber attack.

3.2.2: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network layer, the transport layer, and the application layer.

Focal Knowledge	322-01 Common network vulnerabilities stem from openness and the lack of appropriate restrictions.
Knowledge Statements	• Devices operating at each layer of the OSI Model can have vulnerabilities. • Attacks on routers include IP spoofing and denial-of-service. • The lack of authentication in network protocols, such as ARP, allow spoofing and poisoning attacks. • The lack of authentication and encryption in protocols, such as HTTP, can be used by an attacker to steal credentials or other sensitive information. • Unpatched software and firmware provide potential weaknesses for attackers to exploit. • Misconfigured switches, routers, and firewalls can provide unauthorized access. • Unsecured network access points, such as open Wi-Fi networks, supply chain and vendor access points, are vulnerabilities. • IoT devices operating with default credentials and minimal security are vulnerable points in a network. • Wi-Fi, Bluetooth, and NFC are vulnerable to data interception and unauthorized access. • Software vulnerabilities and user interactions make the Application Layer the most vulnerable OSI layer.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Given an attack, identify whether it succeeded due to openness, a lack of restriction, or both and justify the answer. • Compare and contrast two attacks and write a report on the vulnerability(ies) exploited. In the report, discuss the layer(s) where the vulnerability exists and whether it is due to openness or a lack of appropriate restrictions. • Explain threats to open, public Wi-Fi networks.
Focal Knowledge	322-02 Adversaries seek to manipulate, disrupt, destroy, and persist within computer networks; and this impacts integrity, availability, and confidentiality.
Knowledge Statements	• Exfiltration of data violates confidentiality. • Disclosure of information to unauthorized parties is a breach of confidentiality.

	• Spoofing includes impersonating, masquerading, piggybacking, and mimicking tactics to gain unauthorized entry to a system. • Destruction of data involves erasing, overwriting, or physically damaging storage media so that data cannot be recovered. • Firmware can be manipulated, overwritten, or corrupted making network devices inoperable. • Access to backups and other recovery mechanisms can be shut down or destroyed thus denying the availability of recovery services. • During the 2022 Ukraine power grid attack, Sandworm deployed data wiper software destroying files related to OT capabilities, including physical drive partitions. • Unauthorized modification or the destruction of information is a breach of integrity. • Attacks involving integrity can include defacement of visual content internally or externally to a network. • Disruption is an unplanned event that causes a system to be inoperable for an unacceptable length of time. • Disruption of a system impacts the availability of data, account access for legitimate users, and access to resources. • Endpoint denial of service attacks impact availability of services to users by exhausting resources or crashing systems. • Network denial of service attacks can exhaust network bandwidth impacting the availability of web servers, email, DNS, and web applications. • Availability of systems and network resources can be interrupted by adversaries encrypting data on a system (for example, using ransomware). • Unauthorized modification of file and directory permissions or system shutdowns are disruption techniques used along with malware attacks. • The impact on industrial control systems can include manipulating controls, disrupting safety or protective system functions, denial of operator oversight of controls, and modifying parameters. • Stuxnet malware utilized multiple behaviors, including data encoding techniques, privilege escalation, exfiltration, file deletion, file modification, use of remote services, a rootkit, masquerading, modifying parameters, and more. • Denial of control attacks prevent system operators from adjusting process controls. (In 2015 the Ukraine power grid attack involved Sandworm's use of malware to disrupt transmission and distribution substations.) • Cyber physical systems are susceptible to attacks when connected to IT networks. • Attacks involving integrity and availability of cyber physical systems (e.g.,water and power) can endanger human populations.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Given an attack, describe whether the attack affected confidentiality, integrity and/or availability and justify the answer. • Given an attack, identify both the objective(s) and the impact(s) of specific attacks and justify the answer.

3.2.3: Students will identify and distinguish between the purposes of network security devices and technologies.

Focal Knowledge	323-01 Network security tools and techniques serve various functions, such as access control, prevention, and detection.
Knowledge Statements	• Security controls are the protection measures for a system (also referred to as safeguards or countermeasures). • A physical control is one that prevents specific physical actions from occurring. Physical security controls include bollards/barricades, alarms, badges, access control vestibules, cameras, motion recognition, guards, locks, fencing, lighting, fire/temperature/moisture detection, USB data blockers, etc. • Technical controls use some form of technology. Technical controls include identification and authentication, access control, audit and accountability, and system and communication protection. • Authentication, authorization, and accounting (AAA) work together to provide access security. • Authentication is the process of validating an identity previously established. • Authorization permits or denies access to a specific resource. • Accounting tracks resource access by users or objects. • Baselining is the measuring of a system's current state of security readiness. It helps determine typical patterns so that significant deviations can be detected. • Patch management is the process of updating a system with required patches. • Hardening involves determining the needs of a system to properly operate and enabling only the necessary items. • Network segmentation with firewalls at the boundaries enforces access control. • Access control lists can control which users can change network configurations, change firewall rules, and other decisions that impact network security. • Firewalls filter traffic by blocking unauthorized traffic, including blocking unneeded open ports and unused services. • VPNs can provide secure access for remote users by encrypting data and hiding the IP address. • Data loss prevention technology monitors and protects sensitive data from unauthorized access or loss. • Intrusion detection systems monitor incidents, provide logging and reporting mechanisms. • Intrusion prevention systems monitor incidents, provide logging and reporting, and can take action such as blocking traffic. • SIEM systems gather information, provide alerts, and develop correlation logs to identify malicious activities. • Endpoint security is the practice of securing the entry points of end-user devices (laptops, desktops, mobile devices) from being exploited by adversaries.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify tools used for access control, prevention, and detection. • Describe and distinguish between the purpose of tools for access control, prevention, and detection.

	• Given a security goal, select the appropriate tool for the intended purpose and justify the answer. • Compare and contrast the functionality and purpose of given security tools and techniques (such as intrusion detection, intrusion prevention, firewalls and VPNs).
Focal Knowledge	323-02 Secure protocols address the lack of security in basic network protocols (IP, TCP, DNS, HTTP, etc.).
Knowledge Statements	• The legacy protocols that were developed to support the Internet were designed for functionality, not for security. • Secure protocols have security built-in, but they are still vulnerable to attacks. • Secure protocols often use cryptographic techniques to provide confidentiality and/or integrity. • The use of a secure protocol does not ensure security. • DNSSEC is an extension to the DNS protocol. It enables origin authentication, authenticated denial of existence, and data integrity. It uses port 53. • IPSec is a protocol securing data sent across public networks. It encrypts and authenticates network packets at OSI Layer 3. • SSL and TLS encrypt data, provide authentication, and ensure message integrity. SSL has been replaced by TLS, but it continues to be called SSL/TLS. • HTTPS is the secure version of HTTP. It secures communication between the web browser and websites. HTTPS uses the SSL/TLS protocol. HTTPS uses port 443 for secure transfers. • FTPS is the secure implementation of File Transfer Protocol using SSL/TLS. It uses ports 989 and 990. • SFTP is Secure File Transfer Protocol over an SSH channel. It uses port 22. • S/MIME is Secure Multipurpose Internet Mail Extension and is the standard for public key encryption and signing of MIME data in emails.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Connect the protocol to a use case. • Explain the purpose of IPSec, HTTPS and SSH. • Explain the purpose of the Domain Name System Security Extension (DNSSEC).
Focal Knowledge	323-03 Secure design principles such as defense-in-depth, minimization, and least privilege can mitigate risk in complex networks.
Knowledge Statements	• Open protocols, standards, and designs can improve security due to the examination by many reviewers. • A simple implementation means fewer opportunities for mistakes and fewer attack vectors (simplicity or economy of mechanism). For example, using role-based access control (RBAC) simplifies managing user access. • Minimization means using the least functionality necessary in a program or device. As an example, in a computer network it means blocking unused ports and services via firewall rules. • Least privilege protects information by granting a user the minimal privileges needed to accomplish an assigned task or role. Least privilege applies to devices, applications, and systems. • Layering involves creating separate levels that must be conquered for an adversary to breach a system. Layering slows down the advancement of the attack. Layering may focus on physical security, network, and host security measures as layers of defense.

	• Defense-in-depth is the application of multiple countermeasures in a layered manner to achieve the desired level of security. It is often considered a multifaceted strategic plan. • Mitigation is a decision, action, or practice intended to reduce the level of risk of a threat or vulnerability.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Given a scenario, identify a set of cybersecurity techniques that lead toward defense-in-depth and justify the answer. • Given a network, identify techniques that could be applied to minimize the number of ways in which attackers can exploit the network. • Recap least privilege in lay terms. • Given a set of users and sensitive information, design an access control matrix and justify the answer. • Identify techniques for restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.