Glossary

Module 1: Data and Privacy

Term	Definition
Administrative controls	Guidelines, policies, and procedures written to meet and enforce security goals.
Antimalware (antivirus) software	Software that detects, quarantines, and destroys malware that threatens data or networks.
Asymmetric encryption	An encryption process that involves using two keys: a public key to encrypt data and a private key to decrypt it.
Availability	An objective of the CIA triad that means ensuring timely and reliable access to and use of data.
Authentication	A measure to verify the source of a message.
A1Z26 cipher	An encryption process that replaces each plaintext letter with a number corresponding to that letter's order in the alphabet
Backup software	Software that creates extra copies of data that can be used to recover critical data lost due to breaches, system failures, or other security events.
Brute force attack	A cyberattack in which the attacker tries different passwords until they find one that works.
Caesar cipher	An encryption process that replaces each plaintext letter with the letter three places before or after it in the alphabet.
CIA triad	An information security model with confidentiality, integrity, and availability as the objectives of data protection.
Cipher	A set of transformations that convert plaintext, the intelligible, human-readable data, into ciphertext, the data's encrypted form.
Cloud DLP	A type of data loss prevention that involves detecting and encrypting sensitive data before it is stored in the cloud.
Confidential data	Data that an organization protects from unauthorized access, such as proprietary information, source code, employee records, personally identifiable information (PII), and protected health information (PHI).
Confidentiality	An objective of the CIA triad that means protecting data by ensuring that only authorized people can access or disclose it.
Control	A measure that you can take to mitigate risks. Controls come in three types: administrative, physical, and technical.
Cyberattacker (attacker)	A hacker who tries to bypass system or network security to access data without authorization for malicious purposes.
Data at rest	Data residing in a storage device.
Data erasure software	Software that permanently clears a repository's unneeded or unused data.

Term	Definition
Data in motion (Data in transit)	Data that is actively moving across a network or between systems.
Data in use	Data that a computer or application is actively using and processing.
Data loss prevention (DLP) systems	Processes, procedures, and tools that help detect and prevent data loss.
Data privacy	Data security focused only on preventing unauthorized collection, disclosure, or use of customers' and employees' private data.
Data security	How an organization protects confidential data from unauthorized access, disclosure, or destruction.
Differential backups	A data backup process that starts with a full backup, and then each additional backup includes only the changes made since the last full backup.
Encryption	Technical control that ensures data confidentiality by converting readable data into an unreadable form.
Encryption software	Software that converts data into a format that unauthorized people cannot understand, preserving confidentiality.
Endpoint DLP	A system that monitors all endpoints for data loss or leakage.
File encryption	The process of encrypting files or file systems so that only those with the key can access them.
File-level DLP	A system that identifies sensitive files in a file system.
Full backups	A data backup process in which you copy the entire content of your system or device.
Full drive encryption	The process of encrypting an entire hard disk, including its data, files, programs, and operating system.
Generally Accepted Privacy Principles (GAPP)	A standard for data privacy developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).
Hacker	Someone who tries to bypass system or network security to access data.
Hard disk encryption	The process of encrypting data stored on a hard disk and new files being added.

Term	Definition
Incremental backups	A data backup process that captures only the changes made since the last backup.
Integrity	An objective of the CIA triad that means protecting data from unauthorized modification and destruction to ensure it is trustworthy and accurate.
Malware	Software or firmware intended to conduct unauthorized actions that negatively affect system security.
Monoalphabetic cipher	An encryption process that replaces each plaintext letter with another letter in the alphabet. For example, maybe all *A's* become *Z's* and all *B's* become *Y's*.
Network DLP	A system that protects data at rest, in motion, or in use on an organization's network.
Network encryption	Encryption used to protect sensitive data in motion between the server and the client.
Non-repudiation	Assurrance that neither the sender nor the receiver of a message can deny its transmission; the sender receives proof of delivery, and the receiver receives proof of the sender's identity.
Personally identifiable information (PII)	Private data that can be used to identify someone, such as birthdays, addresses, phone numbers, and government-issued ID numbers.
Physical controls	Devices or structures designed to restrict access to areas or devices containing sensitive data. Common examples include fences, locks, key cards, security cameras, alarms, and cabinets.
Private data	Data about a person and their private life that other parties should not be able to collect, use, or disclose unless authorized. Some examples include financial activity, credit card numbers, email login credentials, personally identifiable information (PII), and protected health information (PHI).
Proprietary data	Organization-owned or organization-generated data relevant to the organization's products or actions that must remain confidential.
Protected health information (PHI)	Private data in medical records used to identify someone, such as diagnoses, test results, prescriptions, and health insurance information.
Public data	Data that anyone can access, use, and redistribute without restriction.

Term	Definition
Symmetric encryption	An encryption process that involves using a single private key to encrypt and decrypt data.
Technical controls	Hardware or software that helps secure data or processes. Common examples include antimalware software and encryption software.
Threat	Something that can cause harm to a network, system, or data.
Vulnerability	A weakness in hardware, firmware, or software that a hacker can exploit.

Questions I have

Example: What is the difference between confidential data and private data?

My notes

Example: Confidential data is data that an organization protects from unauthorized access, such as proprietary information, source code, employee records, personally identifiable information (PII), and protected health information (PHI).

Private data is a **type** of confidential data. Specifically, it's confidential data about a **person**, such as login credentials, credit card numbers, and medical test results.

Module 2: Governance, Risk, and Compliance

Term	Definition
California Consumer Privacy Act (CCPA)	A data privacy law that applies to any organization that does business in California and must share with customers the data it collects about them and their children.
Compliance controls	Risk-based controls that companies implement to protect confidentiality, integrity, and availability of data and comply with laws, regulations, and standards.
Compliance (in cybersecurity)	An organization's adherence to applicable laws, regulations, and standards designed to keep data and systems safe from cyberthreats.
Disaster preparedness plan	A written plan that lists the precautions that an organization takes to prevent or mitigate the harm that disasters cause.
Disaster recovery plan (DRP)	A written plan for recovering data or systems if a disaster occurs.
Federal Educational Rights and Privacy Act (FERPA)	A US federal law designed to keep student education records private. The law requires that schools implement appropriate controls, such as policies, procedures, and training, to prevent unauthorized access, disclosure, and use of those records.
General Data Protection Regulation (GDPR)	An extensive data privacy law and regulation that applies to any company that hosts the data of EU residents or does business with EU countries.
Gramm-Leach-Bliley Act (GLBA)	A US federal law that requires financial institutions and companies that offer US consumers financial products or services to disclose their data-sharing practices to customers.
Governance	The process of making and enforcing decisions within an organization. It defines how a governing body structures and sustains rules, norms, and actions and how it holds everyone accountable for them.
Governance, risk, and compliance (GRC)	A structured way to align an organization's business goals with its recognition of risk and risk mitigation to meet all government and industry regulations and standards.
Guideline	A recommended, not required, way to perform a task at an organization. For example, a company guideline might be that employees use a specific PowerPoint template for all internal meetings. But if an employee violates this guideline, they'll probably receive a reminder, not a punishment.
Health Insurance Portability and Accountability Act (HIPAA)	A US federal law that defines the control of protected health information (PHI), such as medical records and diagnoses. HIPAA's Privacy Rule places strict restrictions on access and disclosure of someone's PHI. HIPAA's Security Rule establishes standards for protecting PHI.
IEEE 802 networking standards	Industry-standard guidance for securing area networks of various sizes. For example, the standards cover network access, encryption, and threat detection.

Term	Definition
ISO 2700 and ISO 27001	International standards for a wide range of cybersecurity topics, such as assessing risks, creating information security management systems, and deploying security controls.
Law	A legal requirement established by a congress, parliament, or other legislative group. Laws tend to be broad in scope. Violating them can lead to penalties, fines, and other legal consequences. In the context of cybersecurity, laws protect data and punish those who violate its confidentiality, integrity, or availability without proper authorization.
Multiparty risks	Risks that impact more than one organization. A common example is an internet or service provider outage.
National Institute of Standards and Technology (NIST)	A US federal agency dedicated to advancing American technology and innovation that provides extensive cybersecurity resources, including hundreds of cybersecurity and data privacy standards.
NIST risk management framework (RMF)	A comprehensive, repeatable, and measurable approach to managing data security and privacy risk. It includes seven steps.
NYDFS Cybersecurity Regulation	A New York state regulation that requires financial institutions doing business in the state to perform risk management.
Payment Card Industry Data Security Standard (PCI DSS)	A data security standard for credit cards that applies to organizations storing or transmitting credit card data.
Procedure	Step-by-step processes for completing a task to meet a standard or guideline.
Policy	A broad statement about the overall intent of an organization and how it should be run, including details about the organization's goals, intentions, and values that the organization must defend with the security framework.
Regulation	A legal requirement, established by a government agency, intended to interpret and implement a law. Regulations clarify what organizations must do to stay within the law. Non-compliance with regulations can lead to penalties, fines, and other legal consequences.
Risk	The extent to which a potential cyberattack or other event threatens an organization's operations.
Risk assessment	A process of identifying risks, evaluating their impact, and deciding what to do about them.
Risk management	Process of identifying, assessing, and controlling financial, legal, strategic, and security risks to an organization's capital and earnings.
Risk tolerance	Level of risk or degree of uncertainty that is acceptable to organizations.

Term	Definition
Standard (in compliance)	A set of guidelines or best practices created by experts, industry groups, or governments that organizations might follow.
Standard (in governance)	A measurable requirement that all employees in an organization must follow. Common examples include configuration settings for devices or requirements for using company equipment.

Questions I have

My notes

Module 3: Threats and Vulnerabilities

Term	Definition
Adware	Advertising-supported software that automatically displays unsolicited advertisements on a device.
Bot (standard definition)	A program that performs automated tasks over a network. A common example is a chatbot performing customer service.
Bot (specifically, a malicious bot or zombie)	An internet-connected device infected with malware that enables the attacker to control the device remotely. Often referred to as a bot in cybersecurity.
Botnet	A network of malicious bots that an attacker controls under the same instance to launch cyberattacks.
Defense in depth	A strategy in which you use multiple layers of security controls to protect assets. For example, an employee might have to pass physical controls, such as a security guard and security cameras, before successfully entering their login credentials, a technical control.
Door access control systems	Systems that restrict entrance to only those with the correct credentials.
Dumpster diving	When someone searches a person's or organization's trash for confidential information.
Electromagnetic interference (EMI)	Interference caused by electromagnetic radiation that can hinder hardware performance. EMI typically comes from electronic devices, such as computers, cell phones, microwaves, and LED lights.
EMI shielding	A technique that encloses equipment, such as audio-video (AV) and ethernet cables, within conductive or magnetic materials to block external electromagnetic waves.
Keylogger	Spyware that records each keystroke that you make on your device.
Logic bomb	Malware saved in a file or embedded in software that activates only when specific conditions are met, such as a specific time of the day.
Malware	Software designed to threaten the confidentiality, integrity, or availability of data or systems.
Malwarebytes	An antimalware program that detects and removes malware such as viruses, exploits, and ransomware.
Malware signature	A pattern of attributes that corresponds to known malware. When antimalware software identifies a signature in a file, the software deletes the file, quarantines it, or alerts you that the file might be infected.
Patch management	The process of updating software to add new features or fix vulnerabilities.
Phishing	The practice of sending messages, seemingly from a legitimate organization, to trick users into providing confidential information.
Physical threat	A direct threat to assets, such as unauthorized intrusion into a restricted area and natural hazards such as fires.

Term	Definition
Shoulder surfing	When an attacker steals your personal information by looking over your shoulder as you use a computer or device.
Social engineering	The use of deception to trick people into divulging confidential or private information for fraudulent purposes.
Spear phishing	A type of phishing that targets a specific person, group, or organization.
Tailgating	When an unauthorized person enters a restricted area by following behind an authorized person.
Ransomware	Malware that holds your system hostage, infects it, restricts access to it or its data, and instructs you to pay a ransom to regain access.
Spyware	Malware installed secretly on a device or system to collect and report data, such as keystrokes, web browsing habits, download history, and other internet behavior.
Trojan	A seemingly helpful program designed to give an attacker access to a device secretly to control remotely, steal data, spy on activity, install malware, or perform other malicious actions.
Virus	Malware that attaches to a device's files or programs to replicate itself and then spreads to another device.
Worms	Malware that self-replicates without needing a host device's files or programs and then spreads across systems.
Zero-day vulnerability	A previously unknown security flaw in software that haven't been fixed.

Questions I have

My notes

Module 4: Vulnerability Management

Term	Definition
Cross-site scripting (XSS)	An attack that inserts malicious code into a client web page. When a user accesses the page, their browser recognizes the code as coming from a trusted site, enabling the code to run.
Cyberattacker	Someone who tries to bypass system or network security without authorization for malicious purposes.
Ethical hacker or offensive security researcher	A hacker who works with organizations to identify and fix vulnerabilities, not exploit them for malicious purposes.
Exploitation frameworks	Tools that provide repositories of prebuilt cyberattacks and exploits. For example, with the Metasploit application, you can search for attacks tailored to a specific version of an OS that you want to target and then let Metasploit perform the attack.
Expression	A combination of code components that a program can interpret and use.
Footprinting or reconnaissance	The act of profiling a system and its users to gather threat intelligence. For example, a pen tester might collect a network's IP addresses and domain names and determine its topology.
Host	A device, such as a server or laptop, that can communicate with other devices on a network and grant access to devices outside the network.
Indicators of compromise (IOCs)	The symptoms or evidence of a cyberattack. For example, the subject line of a suspicious email might match that of a known phishing scam.
Intelligence	Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
JavaScript Object Notation (JSON)	A standard text-based data format that uses human-readable text that can be easily stored and transmitted using an automated system.
Network mappers	Tools to find and map out all devices on a network and discover data about each device, such as its IP address.
Open port	A network port that accepts a connection. Attackers want to find and exploit open ports, while network administrators want to close or block them while ensuring that legitimate users still have access.
Open-source intelligence (OSINT)	Intelligence that anyone can create from publicly available information. Common sources of OSINT include blogs, libraries, news organizations, company websites, social media, and public records.
Operational intelligence	Intelligence that helps security teams anticipate and prevent future attacks.
OWASP ZAP	A free, open-source vulnerability scanner and penetration testing tool designed for testing a web application's security.
Packet analyzer	A tool that captures and inspects data in transit across a network.

Term	Definition
Penetration testing	A type of security testing that simulates real hacking techniques to find application, network, or system vulnerabilities that attackers can exploit.
Port scanner	A program that identifies a network's open or available ports.
Spider or web crawler	A program that searches and indexes web content.
Strategic intelligence	High-level intelligence about current worldwide trends in cyberthreats.
Structured Threat Information Expression (STIX)	An open-source programming language that provides a standardized format for sharing threat intelligence.
SQL injection	A cyberattack that places malicious code into a Structured Query Language (SQL) statement through an application or web page. Attackers typically use a user input request, such as a username, to enter the SQL statement, which runs on the server database.
Tactical intelligence	Intelligence that helps security teams detect and respond to cyberattacks in real time.
Threat actor (malicious actor)	An entity, such as a person, group, or organization, that poses a cybersecurity threat.
Threat intelligence	Intelligence that helps organizations make informed decisions about cybersecurity threats.
Vulnerability assessment	A systematic process in which you identify and evaluate system, network, or application vulnerabilities to determine security risk.
Vulnerability scan	A software-assisted evaluation of a system for known vulnerabilities.
Vulnerability scanner	An application that scans a system for known vulnerabilities.

Questions I have

My notes

Module 5: System Security

Term	Definition
Application server	A server that connects clients to software applications through virtual server connections.
Bootkit	Malware that infects a computer's boot loader or master boot record (MBR), which is responsible for starting the operating system.
Boot program	Software that loads the operating system into the computer, allowing applications to interact with its hardware.
Client	A device connected to a network.
Collaboration server	A server that allows multiple users to share and store files, applications, and large amounts of data.
Common Weakness Enumeration (CWE)	A community-developed list of software weaknesses that can lead to security vulnerabilities in firmware.
Database server	A server that functions as a large storage space that the organization uses and accesses to run multiple programs.
Domain name system (DNS) server	A server that transforms readable computer domain names into computer language internet protocol (IP) addresses, taking search data from a user to find the requested address to deliver to another device.
File server	A server that stores data files for multiple users and allows for faster data retrieval.
Firmware	A critical computer program embedded in a device for controlling its specific hardware functions, such as system startup and interacting with a router.
File transfer protocol (FTP) server	A server that relocates files from one computer to another. File transfer protocol also refers to using a server to connect one computer to another to share data safely.
Gaming server	A server that hosts multiplayer online games. Large gaming networks use servers to connect users from around the world.
High-level firmware	Firmware used with flash memory chips for updating and typically has more complex instructions than low-level firmware.
Jailbreaking	A method used to gain access to the underlying operating system of an iPhone.
Kernel	Software that manages essential components of the operating system, such as managing memory and device drivers and scheduling processes, and ensures proper coordination between hardware and software.
Low-level firmware	Firmware stored on a non-volatile memory chip, such as read-only memory (ROM). It provides the most basic control for a device's hardware, typically managing the hardware's initial startup processes.

Term	Definition
Mail server	A server that stores and delivers mail for clients through email service platforms.
Mobile OS	An operating system developed specifically to run on a mobile device. Well-known examples include iOS and Android.
Monitoring and management server	A server designed for recording and tracking digital transactions and receiving user requests.
Operating system (OS)	A type of software that manages all a computer's applications, programs, and hardware resources and provides a user interface for interacting with the computer.
OS security	Process of ensuring the OS's confidentiality, integrity, and availability. It involves protecting the OS from threats, such as viruses, worms, malware, and remote hacker intrusions.
Patch management	Process for keeping computers and networks secure, reliable, and up-to-date with necessary features and functionality.
Print server	A server that connects remotely to local computers to print through a network. With these servers, organizations can use a single printer to serve an entire department.
Proxy server	A server that intercepts data sent by a website to then send it to a computer's IP address.
Rooting	A method used to gain access to the underlying operating system of an Android device.
Rootkit	Malware designed to hide its presence and activities from the user and the operating system's security mechanisms.
Server	A specialized device or software system that stores and processes data and acts as a central hub in a network, providing this data to other devices in the network.
Server OS	An operating system developed specifically to manage and run a server. Examples of widely-used server OSs include Red Hat Enterprise Linux Server and Windows Server.
Software	A set of instructions and data that tells a computer how to perform specific tasks. It includes programs and applications that help users accomplish various activities, such as browsing the internet, writing documents, or playing games.
Subsystem firmware (device firmware)	Specialized firmware that functions independently of the main system firmware. For example, a printer operates with its own firmware, but firmware is also embedded in the ink cartridge chip to manage communication with the printer about ink levels.
System hardening	The process of securing a computer system or server by mitigating potential vulnerabilities.

Term	Definition
Web server	A server that accesses the World Wide Web through public domain software. It connects the stored information from an internet website to the user's computer.
Workstation OS	An operating system developed specifically to run on desktop or laptop computers. Windows, macOS, and Linux are some of the most well-known workstation operating systems.

Questions I have

My notes

Module 6: Network Security

Term	Definition
Access control schemes	Models for providing consistency in access control to network resources.
Advanced Encryption Standard (AES)	A type of router encryption used to secure classified information. Routers made after 2006 should have the option to enable AES along with WPA2.
Air gap	A technique for secure network design that completely isolates a digital device component or private network from other devices and networks. Air gaps frequently protect systems that need very high security, such as those involved with the military, utilities, or medical practices.
Attribute-based access control (ABAC) scheme	An access control model in which decisions are based on attributes that define the user, resource, and environment where users are requesting access.
Bluesnarfing	An attack that exploits Bluetooth vulnerabilities to steal information or use the device.
Buffer overflow attack	An attack in which a program tries to store more data in a temporary storage area, called a buffer, than it can handle. The overflow leaves the program vulnerable to more attacks, including code that crashes the system, damages data, or gives the attacker control of the system.
Denial-of-service (DoS) attack	An attack that interrupts a device's normal functioning so that normal users can't access it. DoS attacks typically function by flooding a targeted machine with requests until normal traffic can't be processed.
Discretionary access control (DAC) scheme	An access control model in which every object or resource in the system has an owner who determines which users can access it.
Distributed denial-of-service (DDoS) attack	An attack that involves multiple connected online devices overwhelming a target website with fake traffic.
DMZ	A separate network that protects and adds an extra layer of security to an organization's internal local area network (LAN) from untrusted traffic.
Domain Name System (DNS) poisoning	A type of spoofing in which the attacker enters fake information into the cache of a domain name server. The result is that users looking for a specific website are instead sent to one of the attacker's choosing.
Evil twin attack	An attack in which malicious actors set up a fake wifi source to steal information or further infiltrate a connecting device. Attackers often use this strategy in public settings such as airports, cafes, or large public parks where people often look for freely available wifi.

Term	Definition
Extranet	A private network open to external users such as business partners, suppliers, and key customers. An extranet can be useful for functions that involve external users or the public, such as online ordering, electronic order tracking, and inventory management.
Filesystem controls	An access control method in which controls determine which accounts, users, groups, or services can perform actions such as reading, writing, and running files.
Firewall	A network's gatekeeper filters traffic blocks outsiders from gaining unauthorized access and blocks malicious software.
Hardware security module (HSM)	A dedicated cryptographic processor that is specifically designed to protect the cryptographic key lifecycle. Enterprises use HSMs to protect transactions, identities, and applications.
Honeypot	A system that attracts attackers by acting like a network full of valuable resources but also contains tools for monitoring and performing security functions. For example, a bank's honeypot system might mimic a fake login page or section of the bank's website to attract attackers and gather information on their tactics. The bank can then use this information to train its employees on how to detect and prevent similar attacks and to improve security defenses.
Intranet	A private network for distributing communications exclusively to the organization's internal users.
IP spoofing	A type of spoofing that involves impersonating another computer system by creating IP packets with false source IP addresses. This attack enables cybercriminals to engage in malicious activity, such as infecting a device with malware, stealing data, or crashing a server without detection.
Jamming	An attack in which malicious nodes intentionally interfere with wireless networks to prevent legitimate communication. A common method of jamming uses a device that emits electromagnetic energy that makes the network unusable by sending out signals and increasing noise.
Load balancer	A dedicated hardware device or an internet-facing server running a load balance service, distributing traffic among multiple servers and decrypting website traffic. Cloud load balancing is rapidly becoming the most popular form.
Man-in-the-middle attack	An attack in which an attacker breaks into an existing conversation or data transfer between two participants and pretends to be a legitimate participant.

Term	Definition
Media access control (MAC) spoofing	A type of spoofing in which someone or something intercepts or tampers with the control messages exchanged between a networked device and its unique media access control (MAC) address. Attackers can use many methods to do this, such as tampering with messages sent from legitimate access points or capturing and manipulating packets that contain response data before they reach their destination.
Mandatory access control (MAC) scheme	An access control model in which users do not have control over their own access rights.
Network access control (NAC)	A process for controlling and managing access to a network by authenticating users and devices before allowing them to connect.
Network address translation (NAT)	A process by which one unique IP address can represent multiple computers. A network device, often a router or NAT firewall, assigns this single public IP address to a computer or group of computers inside a private network.
Network architecture	A network's structural and logical layout. It describes the network devices used, how they are connected, and the rules that govern data transfer between them.
Network design	Process of creating network architecture for a specific organization and situation. It includes network analysis, hardware selection, and implementation planning, among other planning processes.
Network infrastructure devices	Components of a network that control communications needed for data, applications, services, and multimedia. These devices include routers, firewalls, switches, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks.
Network security	Deployment and monitoring of cybersecurity solutions to protect an organization's IT systems from attacks and breaches.
Network segmentation	A technique for secure network design that splits a larger network into smaller segments, also called subnets, usually through switches and routers.
Network switch	A device that integrates all devices on a network, allowing for seamless sharing and data transfer among them. Connected network devices can include everything from firewalls and wireless access points to Voice Over Internet Protocol (VoIP) phones, printers, servers, and more.
Proxy server (proxy)	A system or router that provides a gateway between users and the internet. When users send requests online, the request travels through the proxy server. The proxy server gets the response from the web server, and then forwards the data to the user's browser.

Term	Definition
Rogue access point	A wireless access point that does not belong to the network. An attacker can use an unauthorized wireless access points for various purposes, such as leaking a business' sensitive information.
Role-based access control (RBAC) scheme	An access control model in which access control decisions are based on the roles assigned to users or groups.
Router	A network's hardware connection to outside data, usually from the internet. That data travels from a modem to a router, which then directs the outside data to network devices.
Spoofing	An attack in which an attacker uses a device or network to trick other computer networks into believing they are a legitimate entity. This deception allows them to take over the devices to use in attacks or gain access to sensitive data.
Wi-Fi Protected Access (WPA)	A type of router encryption that scrambles the encryption key and is more secure than WEP.
Wi-Fi Protected Access 2 (WPA2)	A type of router encryption that scrambles the encryption key and does not allow the use of a less secure protocol.
Wired Equivalent Privacy (WEP)	A type of router encryption that uses radio waves and the same encryption key for every data packet.
Zero-day attack	An attack in which the attacker exploits a software vulnerability unknown to the software's creator before the creator can release a patch to fix it.

Questions I have

My notes

Module 7: Cloud Computing and Virtualization

Term	Definition
Cloud as a service (CaaS)	Application and infrastructure resources that reside on the internet.
Database as a service (DBaaS)	A cloud computing service that provides users with access to a fully managed database system through a CSP. With DBaaS, users can access a database without setting up physical hardware, installing software, or configuring it for performance.
External network virtualization	A type of virtualization that helps service providers create virtual local area networks (VLANs) by either grouping physical systems that are connected to the same LAN or dividing separate LANs into the same VLAN. For example, a provider can use external network virtualization to make separate VLANs for different groups or customers. Each group would have its own security policies and network settings.
Hybrid cloud	A cloud deployment model in which a company uses both public and private cloud infrastructure for data storage and processing.
Hypervisor	A unique software that enables a single physical computer to run multiple virtual machines.
Infrastructure as a service (IaaS)	A cloud computing service that enables you to rent virtualized hardware resources from the cloud service provider (CSP). Examples of these resources include servers, storage, and network components.
Internal network virtualization	A type of virtualization that creates a pretend network inside a single server to make the server more efficient. Internal virtualization provides many benefits, such as using less hardware, being more flexible, and changing network resources to meet different needs.
Network functions virtualization (NFV)	A technology that virtualizes network services, such as routers, firewalls, and load balancers, by packaging them as virtual machines or containers on standard servers.
Network interface card (NIC)	A hardware component that connects a computer or other electronic device to a network.
Network virtualization	A type of virtualization that combines hardware, software resources, and network functionality into a single, software-based system.
Platform as a service (PaaS)	A cloud computing service that enables developers to build, deploy, and manage applications without concern about the technical foundation. Developers can focus on creating applications rather than managing servers, databases, and other infrastructure components.
Private cloud	A cloud deployment model in which a company has its own computer infrastructure in the cloud and it is not shared with anyone else.

Term	Definition
Public cloud	A cloud deployment model in which a cloud service provider (CSP) gives users access to virtual systems, services, and data over the internet.
Software as a service (SaaS)	A cloud computing service that delivers applications over the internet. Examples of SaaS applications include email, document management, and customer relationship management (CRM) software.
Virtual appliance	A preinstalled software on one or more virtual machines that serves a specific function.
Virtual host	A hosting platform that provides computing and storage resources to single or multiple websites, apps, or services, each with a unique domain name and IP address.
Virtualization	A process by which a single physical machine can run multiple operating systems.
Virtual network interface card (VNIC)	A hardware component that connects a computer or other electronic device to a network in a virtualized environment.
VMware software	Software that allows you to create and manage virtual versions of computing functions. It targets home, small business, and enterprise-level users.

Questions I have

My notes

Module 8: Securing Cloud Infrastructure

Term	Definition
Application programming interface (API)	A group of routines, protocols, and tools for building software applications.
Cloud access security broker (CASB)	A security tool or service that acts as a firewall for cloud services, providing a gateway for enforcing security policies to ensure that authorized users' actions adhere to the company's security policies.
Cloud application	A type of software application that runs in the cloud infrastructure.
Cloud application security	Policies, tools, and protocols designed to protect cloud-based applications and data by ensuring visibility, defending against cyberattacks, and restricting access to authorized users.
Cloud disaster recovery	A service that enables organizations to replicate and recover their critical applications and data in the cloud in the event of an IT outage or disaster, ensuring business continuity and minimizing downtime.
Cloud infrastructure entitlement management (CIEM)	A set of tools and practices that enable organizations to understand their entitlements and permissions by analyzing and mapping all identities, roles, groups, and policies across multiple cloud platforms.
Cloud-native application protection platform (CNAPP)	A security solution to protect cloud-native applications that is built using microservices, containers, and other cloud-native technologies.
Cloud security posture management (CSPM)	A critical component of cloud application security that helps organizations identify and mitigate potential security risks.
Data loss prevention (DLP)	A set of tools and processes that help organizations protect sensitive information from unauthorized disclosure or use by detecting and preventing data breaches in real time.
Identity access management (IAM)	A tool that involves managing users' identities and controlling their access to applications, networks, and other resources.
Identity governance and administration (IGA)	A solution that helps organizations manage the identity lifecycle of users and their access to critical applications and data.

Term	Definition
Microservices	A type of architecture used in cloud applications where a software system is broken down into small, independent components that communicate with each other through APIs.
On-demand scalability	The ability of a system or application to quickly and easily adjust its computing resources to meet changing demands or workloads.
Principle of least privilege (POLP)	A security concept that that restricts users or processes to only access and permissions necessary to perform their tasks.
Privileged access management (PAM)	A solution that provides secure and controlled access to privileged accounts, such as those of system administrators, to prevent unauthorized access.
Shadow IT	Use of unauthorized or unsanctioned technology solutions in an organization, often outside the purview of the IT department

Questions I have

My notes

Module 9: Security Operations

Term	Definition
Compliance management	The systematic approach that organizations take to ensure that all applications, systems, and security tools and processes comply with data privacy regulations. Examples of these regulations include but are not limited to the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).
Compliance training	Educational programs and initiatives designed to educate employees about relevant laws, regulations, industry standards, and internal policies that govern their work activities. For example, an organization might host training sessions on identifying and mitigating cyber risks, securing sensitive data, and adhering to regulatory requirements.
Hybrid SOC	A SOC model that combines in-house SOC and SOCaaS models so that the organization can use in-house resources, including internal staff, and outsourced security services.
Incident response (IR)	The set of actions an organization takes to prepare for, expose, and stop cyberattacks.
In-house SOC	A SOC model in which an organization has an internal SOC team and resources dedicated to managing security operations. The organization owns and maintains the infrastructure and tools required to operate the SOC.
Log management	The process of collecting, storing, analyzing, and managing log data generated by various systems, applications, and network devices within an organization.
Onboarding training	The process of educating newly hired employees or contractors about essential cybersecurity principles, practices, policies, and procedures specific to their roles within an organization.
Phishing training	Educational programs designed to teach individuals how to recognize, avoid, and respond to phishing attacks.
Post-mortem and refinement (post-incident review)	A structured analysis conducted after a security incident or breach. Refinement in cybersecurity refers to the process of implementing improvements and adjustments based on the findings and recommendations from a post-mortem or ongoing security assessments.
Recovery and remediation	Critical processes that follow incident response and aim to restore normal operations, mitigate damage, and prevent future occurrences.
Recurring training	Ongoing educational programs and initiatives that provide regular updates, refreshers, and new information to employees and stakeholders about cybersecurity threats, best practices, and compliance requirements.

Term	Definition
Security operations center (SOC)	A dedicated team of cybersecurity professionals that uses specialized software to actively monitor, detect, investigate, and respond to an organization's potential security threats and incidents in real time.
SOC as a service (SOCaaS)	A SOC model in which an organization outsources nearly all its security operations to a third-party provider. In turn, the third party provides the necessary staff and technology to monitor, analyze, and respond to incidents.
SOC facility	A centralized physical location where cybersecurity professionals monitor, detect, analyze, and respond to security incidents and threats.
SOC software	A type of security software that SOC teams use to monitor, analyze, and respond to security threats in real time.
SOC team	A group of cybersecurity professionals responsible for monitoring and analyzing an organization's security posture.
Threat detection	The process of identifying potential security threats and malicious activities within an organization's IT environment.
Virtual SOC (V-SOC)	A cloud-based SOC model in which an organization builds, hosts, and maintains its security infrastructure and tools in the cloud, and the organization's internal SOC team works remotely.

Questions I have

My notes

Module 10: Security Monitoring

Term	Definition
Active monitoring solutions	Software tools that operate in the background and actively search for potential issues or slowdowns. These types of solutions alert network administrators as soon as anomalies or predefined thresholds are met, enabling swift response and resolution.
Agent	A software application installed on an endpoint that collects, processes, and reports data related to the device's security status.
Behavioral analytics	The practice of collecting and analyzing data on user activities, network traffic, and system events to understand patterns of behavior. This analysis helps identify deviations from normal behavior that can indicate security incidents, fraud, or other risks.
Endpoint management	The process of monitoring, securing, and controlling devices connected to a network. This involves deploying security policies, updating software, monitoring device health, and ensuring compliance to protect the network from vulnerabilities associated with endpoints.
Endpoints	Devices such as computers, smartphones, tablets, and IoT devices that connect to a network. These devices act as entry points for communication and interaction within the network, making them critical to network security and management.
Network reconnaissance	The process of gathering information actively or passively about a computer network, its devices, and its services to identify potential vulnerabilities.
Incident response plan	A predefined set of procedures and actions that security teams follow when a security incident is detected. The plan outlines steps for identifying, containing, eradicating, and recovering from threats to minimize damage and restore normal operations.
nslookup	A command-line tool that obtains information about a host system: it helps diagnose and troubleshoot DNS-related issues by retrieving details such as the IP address of a domain or the domain associated with an IP address. One example is running the 'ping' command, such as 'ping google.com', to check the connectivity and measure the round-trip time to the Google servers.
Packet analyzer	A tool that captures and analyzes data in transit across a network. For example, Wireshark is a network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network.

Term	Definition
Passive monitoring solutions	Software tools that observe and record network activities without actively interacting with the traffic. These solutions provide administrators with detailed logs and historical data, enabling them to analyze network behavior, performance, and security trends without affecting the system's operation.
Ping test	A diagnostic tool that measures the time it takes for a data packet, or ping, to travel from one computer or server to another. It tests the reachability of a host and assesses the latency, which is crucial for determining network performance and detecting potential connectivity issues.
Security information and event management (SIEM)	A security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations.
Security posture	An organization's overall security status, reflecting its ability to protect against and respond to cybersecurity threats. This includes the effectiveness of security controls, policies, procedures, and the organization's readiness to manage and mitigate risks.
Traceroute	A diagnostic tool that actively interacts with a computer network to find problems with an internet connection.
User and entity behavior analytics (UEBA)	A cybersecurity approach that focuses on monitoring and analyzing the behavior of users and entities within a network to detect unusual or potentially malicious activities.

Questions I have

My notes

Module 11: Incident Response

Term	Definition
Attack surface	An analysis of all the potential vulnerabilities and entry points through which an unauthorized user can try to access a system, network, or application, to affect, or extract data from the system.
Containment	The process of stopping an attack from proceeding further and causing any more damage or disablement to the system.
Cyber Kill Chain framework	A tool for intrusion analysis that provides a structure to identify, understand, isolate, and respond to malicious behavior.
Eradication	The process of eliminating a threat from all affected devices, such as by reimaging devices, disabling services, and updating software.
Functional impact	The extent to which an attack will affect a system's effectiveness and users' ability to access what they need.
Incident response framework	A structured approach for handling and managing security incidents, outlining the processes and procedures for identifying, investigating, and responding to cybersecurity threats.
Incident response (IR)	The set of actions an organization takes to prepare for, expose, and stop cyberattacks.
Incident response plan (IRP)	Documentation that details the necessary actions in the event of a cyberattack, the order in which they should take place, and the team members who should carry them out.
Indicator	A sign that an incident might have occurred or is occurring now, such as an antimalware program alert indicating that a trojan has infected a device.
Informational impact	The extent to which an attack will affect the information in a system, including the information that might be stolen or destroyed and a measurement of the potential consequences.
Intrusion analysis	The process of using information about an attack to determine the scope of the attack, the method used by the attacker to gain access, and the extent of the damage to the system or network.
MITRE ATT&CK framework	A detailed matrix that categorizes the tactics and techniques attackers use to conduct cyberattacks. It stands for *Adversarial Tactics*, *Techniques*, and *Common Knowledge.*
Precursor	A sign or indication that an attack or security incident might occur in the future.
Recoverability impact	The extent of damage that an attack causes and the time that the organization might need to restore the system and information to its previous state.
Recovery	The process of restoring and returning affected systems, data, and operations to normalcy following a security incident or breach.

Questions I have

My notes

Module 12: Digital System Forensics

Term	Definition
Acquisition and analysis tools	Tools that collect and analyze digital evidence from data sources such as hard disk drives and memory cards.
Analysis	The third phase of digital forensics when investigators analyze the relevant data from the examination phase to draw meaningful conclusions about it.
Autopsy	An open-source data recovery tool used to analyze and recover data from storage media on Windows, Linux, and macOS operating systems.
Chain of custody	A process used in forensic investigations to record the chronological history of evidence. It tracks the possession, handling, and transfer of evidence from the moment someone collects it to its presentation in court, ensuring its integrity and admissibility.
Collection	The first phase of a digital forensic investigation when investigators identify and gather potential sources of evidence. This phase involves labeling, documenting, and collecting data from various digital devices while ensuring the integrity and authenticity of the evidence.
Command-line interface (CLI)	A user interface in which users type commands to navigate and manage the system.
Data carving	The process of extracting data from a storage device without relying on the file system or metadata. This process is especially valuable for retrieving digital evidence from corrupted or reformatted storage devices where traditional file system analysis is impractical. It involves extracting data directly from the storage device by identifying specific file signatures or patterns in the raw data, bypassing the need for file system or metadata dependency.
Data preservation	The process of protecting and safeguarding electronic data to maintain its integrity, authenticity, and usability for investigative purposes.
Data recovery	A process for retrieving lost, deleted, corrupted, or otherwise inaccessible data.
Digital forensics tools	Hardware or software that collects, extracts, triages, preserves, or recovers digital evidence.
Digital forensics	The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.
Examination	The second phase of a digital forensic investigation when investigators sift through the collected data to determine what's relevant and extract it for later analysis.
FTK Imager	An open-source acquisition and analysis tool for creating disk images without modifying or making any changes to the original data, ensuring

Term	Definition
	forensic soundness and preserving evidence for investigative purposes.
Hash value	A series of numbers, generated using a mathematical algorithm, that uniquely identifies a piece of data. It serves as a digital fingerprint, uniquely identifying the data in a way that makes detecting any alterations or tampering easy.
Image	A bit-for-bit copy of a storage device, such as a hard disk drive or USB flash drive, including all its contents and structure.
Imaging tools	Tools that create exact replicas of storage media, such as hard disk drives, USB flash drives, memory cards, or other storage media. They enable investigators to work with copies of data without altering or compromising the original source, thus maintaining its forensic soundness.
Kali Linux	A cybersecurity-focused Linux distribution with an array of standard cybersecurity tools, including Autopsy, data carving utilities, and other digital forensics applications.
Packet	A small piece of data in transit across a network. It contains both the payload, which carries the actual information being sent, and header information, which includes details such as the source and destination addresses and other information needed for routing and delivery.
Problem solving	The use of logic and reason to solve a problem. It involves using creative thinking, knowledge, intuition, and experience to develop solutions that best meet the person or organization's needs.
Raw data	Unprocessed and unanalyzed information that investigators have collected during a digital forensic investigation.
Recovery tools	Tools that recover deleted or otherwise inaccessible files, such as files stored in damaged or corrupted images.
Triage tools	Tools that quickly scan large amounts of acquired data for important files or keywords. They prioritize the extraction of potentially relevant data based on predefined criteria, such as file types, metadata, or keywords.
Virtual machine (VM)	A software-based version of a physical computer system that operates within another computing environment. VMs can run their own applications and other software, just like physical machines can.
Volatile data	Temporary information stored in the device's memory, such as running processes, open files, and network connections, that is lost once the system is shut down or the session ends.
Volatility	An acquisition and analysis tool that can extract volatile data from RAM, such as data from the operating system and processes running in memory.

Term	Definition
Write-blocker	A device that blocks any write commands sent to a storage device, such as a hard disk drive or USB flash drive. By intercepting and blocking write requests, write-blockers ensure that the integrity of the original evidence is preserved during the forensic examination process.

Questions I have

My notes

Module 13: Emerging Threats and the Future of Cybersecurity Technologies

Term	Definition
5G	The fifth generation of cellular networks, which allows for faster speeds because of ultra-low latency and increases network coverage.
Artificial intelligence	Technology that enables computers and machines to simulate human intelligence and problem-solving capabilities. Cybersecurity professionals use AI for various tasks, such as creating predictive models that alert organizations to potential threats before an attack occurs.
Biotechnology	The use of living organisms or their components to create useful products or solve problems. Biotechnology can be used in various fields to develop new treatments, improve crop yields, create vaccines, and find innovative solutions to the challenges that people face.
Domain Name System (DNS)	A fundamental part of the internet infrastructure that translates domain names (such as example.com) into their corresponding IP addresses (such as 192.0.2.1).
Emerging technology	Any innovative product or service still in the early stages of development, testing, or adoption.
Generative AI	A subset of AI that focuses on creating or generating high-quality text, images, and other content based on data on which the AI model is trained. Some well-known examples of generative AI include chatbots and OpenAI's ChatGPT.
Genomics	The branch of molecular biology that studies the structure, function, evolution, and mapping of genomes, which is the complete set of DNA, including all of an organism's genes.
Internet of Things (IoT)	A network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity that allows them to collect and share data.
Nanotechnology	The field of science and engineering that studies the design, synthesis, characterization, and application of materials and devices at the nanoscale.
Quantum computing	A technology that uses quantum mechanics to solve problems that are too complex for classical computers or supercomputers to solve or solve quickly enough.
Ultra-low latency	An extremely short delay in transmitting and receiving data, allowing for near-instantaneous communication or response. Delivering ultra-low latency is one of the most significant advancements that 5G networks introduce.

Questions I have

My notes