CompTIA Security+ (SY0-701) Complete Course & Exam - 2

Study online at https://quizlet.com/_efgdrq

Jane, a database administrator at Dion Training, wants to ensure that a file has not changed since the last time she uploaded it to her cloud storage. She has created an SHA-256 hash digest of the file and will compare the stored file's hash digest against the one she calculated when she initially uploaded the file. Which of the following pillars of the CIANA pentagon is she focused on?	Integrity
Vikas, a developer at Dion Training, just digitally signed the company's new app before releasing it in the App Store. Before the app is installed, the user's device will validate the digitally signature to ensure that it was actually developed and uploaded by Dion Training. Which of the following pillars of the CIANA pentagon is she focused on?	Non-repudiation
Jason, an instructor at Dion Training, is logging into the company's exam application to write some new questions for the CompTIA Security+ exam. He enters his username/password at the login prompt and then receives a one-time code on his smartphone that he enters to validate his identity. Which of the following pillars of security was he focused on when performing this action?	Authentication
David, the CTO of Dion Training, just sent out a new policy that will require all of the company's users to reset their password every 60 days using a long, strong, and complex password. Which of the following type of security controls best classifies this policy?	Directive
Christle, a student support manager at Dion Training, is logging into the company's exam voucher application to help a student schedule their CompTIA Security+ exam. Even though she is already connected to the corporate network, the application asks her to validate her identity by sending her a one-time code on her smartphone that she enters to validate her identity. Which of the following security concepts is being utilized by the company's architecture?	Zero trust
Which of the following is a primary motivation for a hacktivist threat actor?	Ideological beliefs
Which attribute of a threat actor indicates the amount of financial, technological, and human resources they can use for their operations?	Their resource level
Which of the following threat actors primarily operates based primarily on financial motivations and is considered to be highly structured and sophisticated in their attacks?	Organized crime
Which type of threat actor would BEST describe a disgruntled employee who may exploit their legitimate access for malicious purposes?	Insider threat
Which deceptive technology is a piece of data or a system entity that exists solely to alert the organization when someone accesses it?	Honeytoken
Jennifer, a facilities manager at Dion Training, wants to prevent unauthorized vehicles from getting too close to the building and ramming into it. Which of the following physical security control measures should they utilize to achieve this?	Bollards
Jacob, a security manager at Dion Training, wants to protect a sensitive server room against unauthorized physical access without relying on electronic locking mechanisms. Which of the following door locks should they utilize to achieve this?	Cipher lock
Jonni, a security manager at Dion Training, wants to implement a physical security control measure at the main entrance of their new corporate headquarters. Their primary objective is to authenticate individuals in a space between two sets of doors to help prevent tailgating by ensuring that unauthorized persons don't	Access control vestibule

follow authorized individuals inside. Which of the following security controls should he implement to best achieve this?	
Sheryl, a penetration tester at Dion Training, wants to break into the RFID-protected server room. She sees Mazen sitting in a coffee shop, so she briefly places her purse near Mazen's backpack. Later, she uses a device from her purse to access the server room. She receives a message stating, "Welcome, Mazen" when she authenticates with the RFID-based lock using the device. Which of the following types of attacks did she utilize to gain access to the server room?	Access badge cloning
Which of the following sensors is used to detect changes in environmental heat that is typically emitted by warm bodies such as humans or animals?	Infrared sensors
Which of the following types of phishing attacks is used to specifically target high-level executives or important officials within an organization?	Whaling
During an anti-phishing campaign, what primary action should a company take after simulating a successful phishing attack on its employees?	Provide remedial training to employees who fell for the attack
Which social engineering technique involves searching through a target's trash or discarded items to obtain sensitive or valuable information?	Dumpster diving
Which social engineering attack involves an attacker creating a fabricated scenario to manipulate or deceive someone into divulging confidential information?	Pretexting
Which of the following is a common motivational trigger used in social engineering attacks to manipulate victims to act or respond without taking time to think about the consequences?	Urgency
Which of the following best describes a Trojan?	A Trojan is a malicious program disguised as legitimate software.
Which of the following is designed to give cybercriminals access to a system that can carry out malicious tasks, such as distributed denial-of-service (DDoS) attacks or to spread malware, without the user's knowledge?	Zombie
Which of the following is a type of malware that operates behind the scenes to deliver ads or track user activity?	Spyware
Which of the following BEST describes what a rootkit is used for? Encrypt user files and demand payment for decryption Hide malware activities and maintain privileged access to a system Log the user's keystrokes to steal their credentials Replicate themselves across networks without human intervention	A rootkit is used to hide malware activities while maintain privileged access to the system.
Which of these is a common indication of a malware attack?	Fewer logs than usual during peak hours
Which of the following data classifications is typically accessible by anyone and is not harmful if disclosed?	Public
Dion Training Solutions is revising its data governance approach to align with GDPR and other regulatory standards. They have designated Samantha, the Vice President of Operations, to determine data classification and access control. David, the Compliance Officer, ensures all data processing complies with legal standards. Rachel, an IT Services Partner, handles the processing of client data on cloud servers. Lastly, Mike, the Head of the IT Department, is in charge of data storage, transportation, and security policy enforcement. Based on these details, identify who among them fills the roles of data owner, data controller, data processor, and data custodian.	Samantha is the data owner, David is the data controller, Rachel is the data processor and Mike is the data custodian

Which of the following is NOT a recognized state of data in the context of data security?	Data in flux
Which type of data refers to any information about health status, provision of healthcare, or payment for healthcare that can be linked to a specific individual?	Protected Health Information (PHI)
Dion Training is exploring Data Loss Prevention (DLP) systems. They want a system that will protect data while it's at rest on their on-premises server, using encryption or a watermark?	Storage DLP
Jennifer, a network administrator at Dion Training, wants to ensure that a secret communication between two servers remains confidential using a single key for both encryption and decryption processes. Which of the following should they utilize?	AES
Robert, a system engineer at Dion Training, wants to securely exchange cryptographic keys over a public channel to initiate encrypted communications with another department. Which of the following should they utilize?	Diffie-Hellman
Samantha, a cybersecurity analyst at Dion Training, wants to use the most secure hashing algorithm for ensuring the integrity of sensitive documents. Which of the following should she utilize?	SHA-256
Rebecca, a digital forensics expert at Dion Training, wants to discreetly embed a message within an image file without noticeably altering its apparent appearance or structure. Which of the following techniques should she utilize?	Steganography
Miguel, a cybersecurity specialist at Dion Training, is concerned about the potential threats that the evolving technologies, like qubit-powered computers, might pose to the company's current encryption algorithms and cryptographic implementation methods. Which of the following solutions should he explore to ensure future cryptographic resilience?	Post-quantum Cryptographic Algorithm
John is the owner of a small construction company. He recently signed a contract for a new project. The contract includes a clause stating that John's company will be responsible for any damages that occur during the construction process. As a result, John has decided to purchase insurance that will cover the cost of any damage that might occur during the construction process. Which risk management strategy is John using?	Risk Transference
Solarflare, an energy company, has identified a risk that, if it occurs, could halt their production line. They have determined that they can tolerate a disruption of up to 3 hours before it severely impacts their operations. Which of the following metrics does this scenario represent?	Recovery Time Objective (RTO)
What does the term 'Risk Appetite' refer to?	The amount of residual risk an organization is willing to accept
You are managing a construction project and a potential risk is the delay in delivery of critical materials. The likelihood of this risk is high and the impact is also high. What would be an appropriate mitigation strategy based on Qualitative Risk Analysis?	Secure multiple vendors
You are managing a company's IT infrastructure. One of your servers, valued at $20,000, has an Exposure Factor (EF) of 60% in the event of a crash. The server crashes once every five years. What is the Annualized Loss Expectancy (ALE) for this server?	$2,400
Sarah, a compliance officer at Dion Training, is hiring a consultant. She wants to ensure that the consultant doesn't share information about the proprietary project he is being hired to complete. Which of the following should she utilize?	NDA
Jamie, a procurement manager at Dion Training, wants to ensure the quality, timelines, and scope of the services provided by a new third-party vendor. Which of the following should they utilize?	SLA

Alex, a project manager at Dion Training, wishes to provide details about specific tasks, deliverables, and timelines for a project so the vendor they hire will have a complete picture of the project. Which of the following should they utilize?	SOW
Samuel, an operations director at Dion Training, wants to hire his brother's company to provide security for Dion Training. He is told this is a bad idea. Which of the following would be the main problem with hiring his brother's company?	There would be a potential conflict of interest for Samuel
Which of the following is the BEST way for companies to limit the risks of using third-party vendors?	Conduct Due Diligence
Which of the following best describes the role of governance in an organization's IT operations?	Board of Directors
Which of the following policies outlines the steps an organization will take to continue its critical operations during and after a disruption or disaster?	Business Continuity Policy
Which of the following is NOT typically a part of physical security standards in an organization?	Regular software updates
Which of the following procedures involves tasks such as retrieving company property, disabling access to systems, and conducting exit interviews?	Offboarding
Which of the following is an example of a global governance consideration?	A European regulation affecting data collection practices worldwide
Which of the following terms best describes the requirement to comply with laws and regulations applicable to an organization's operations?	Regulatory considerations
Which of the following is a punitive measure taken by regulatory bodies to enforce compliance in the IT and cybersecurity world?	Sanctions
Jane, a business development manager at Dion Training, is working on finalizing an order for 50 courses and exam vouchers by one of the company's larger clients. This order would have an approximate cost of $25,000 and will be delivered to the company within the next 30 days. Which of the following should she expect to receive from the client to pay for these courses and exam vouchers?	Purchase order
David, an IT manager at Dion Training, wants to deploy mobile devices to employees while maintaining a high level of control and standardization, but also wants to give employees some choice in the type of device they use. Which of the following deployment models should he choose?	CYOD
Julia, a Data Security Analyst at Dion Training, wants to ensure that data on an old hard drive is made inaccessible and irretrievable, while still allowing the device to be reused. Which of the following should she use to accomplish this?	Cryptographic Erase
Maria, a Change Manager at Dion Training, wants to evaluate the consequences of a proposed change before she provides her approval. Which of the following should she utilize to accomplish this?	Impact Analysis
Fahad, a Network Administrator at Dion Training, is proposing to implement a new critical security patch for the company's main server during an upcoming scheduled maintenance window to patch a security vulnerability in the print spooler. The print server involved in this change is actively used by employees throughout the company and the change must be validated after being implemented to ensure that the security patch was correctly applied. Which of the following technical implications would be	Service restarts

most important for him to consider before the change is scheduled and approved for implementation?	
Which of the following is NOT typically a part of an internal IT audit? Reviewing the organization's password policies.	Identifying potential threats to the organization's information systems.
Which type of penetration testing involves a proactive and aggressive approach to uncover as many vulnerabilities as possible?	Offensive
Jonathan, a penetration tester at Dion Training, has been asked to conduct reconnaissance for an upcoming penetration test. He was given little to no information about the target. Which of the following types of environments will Jonathan be conducting his penetration test on?	Unknown Environment
Which of the following would provide an attestation of their findings when conducting a penetration test for an organization that must prove they are in compliance with HIPAA regulations?	An external assessor
Which of the following terms refers to an evaluation conducted by an external organization that is not affiliated with the entity being evaluated and is often to ensure compliance with specific standards or regulations?	A third-party audit
Juan, a network administrator at Dion Training, wants to build a backup facility that is partially equipped with hardware and infrastructure to minimize downtime in case of a disaster. Which of the following types of redundant sites should they utilize?	Warm site
In preparing their disaster response strategy, the emergency management team at Dion Training wants to facilitate a scenario-based discussion among key stakeholders to evaluate their crisis preparedness and decision-making abilities without the need for deploying actual resources. Which of the following testing method should they employ?	Tabletop exercise
Which of the following backup methods involves creating point-in-time copies of data in a storage system to capture its state at specific moments to help facilitate data recovery and system consistency?	Snapshots
Which power backup technology typically provides a longer duration of power supply during extended outages and is often used as a primary source of backup power for critical systems, such as data centers?	Propane generator
Emile, a system administrator at Dion Training, wants to optimize both the performance and data redundancy of the company's critical data storage solution. Which of the following RAID configurations should they utilize?	RAID 10
Which term in cloud computing refers to the speed at which the system can adapt to changes in demand and why is it important for businesses to ensure a smooth customer experience?	Responsiveness
Which concept refers to the shifting of some risks from the customer to the cloud service provider?	Risk Transference
Which of the following is a solution to mitigate shared physical server vulnerabilities?	Implementing strong isolation mechanisms
What is a crucial step in preventing inadequate user access management?	Enforcing strong password policies
Which of the following statements about virtualization and containerization is NOT correct?	Type 1 hypervisors operate within a standard operating system, such as Windows, Mac or Linux
Which of the following is NOT a benefit of serverless computing?	Easier testing and debugging
Which of the following is a challenge in microservices architecture?	Network Latency

Which of the following is NOT a method of achieving logical separation in network infrastructure?	Physically disconnecting a system from other networks
Which of the following best describes the role of the control plane in Software-Defined Networking (SDN)?	It decides where traffic is sent across the network
What is a significant challenge in securing embedded systems?	Inability to Patch
In an Internet of Things (IoT) ecosystem, which component serves as the central point that connects all IoT devices and enables them to communicate?	Hub/Control System
Which of the following best describes a non-idempotent operation in the context of Infrastructure as Code (IaC)?	An operation that produces different results each time it is executed
Which of the following scenarios best illustrates a potential risk associated with a decentralized architecture?	The remote work arrangement exposes the network to additional threats, as each remote connection is a potential entry point for cybercriminals
Which system is typically used for geographically dispersed industrial processes?	SCADA
Lucia, a security analyst at Dion Training, wants a comprehensive solution that integrates various security features for her company's network, including antivirus, anti-spam, firewall, and intrusion detection capabilities in a single network appliance. Which of the following types of firewalls should she utilize to accomplish this?	UTM
Satoshi, a network administrator at Dion Training, wants to mediate requests from clients seeking resources from other servers by helping to simplify requests, improve performance, and filter content. Which of the following should he utilize to accomplish this?	Proxy server
Priya, a network engineer at Dion Training, wants to improve the management and operation of a wide area network by decoupling the networking hardware from its control mechanism. Which of the following should she utilize to accomplish this?	SD-WAN
Rajesh, a security specialist at Dion Training, wants to install a IDS or IPS so that is can actively block and prevent malicious traffic from entering a screened subnet in real-time. Which of the following should he do to accomplish this?	Install the IPS as an in-line device
Ling, a cybersecurity consultant at Dion Training, wants to select some effective security controls by prioritizing and implementing the controls based on the specific vulnerabilities and threats that the enterprise infrastructure is facing. Which of the following principles of effective control selection should they emphasize to more effectively use their limited resources while providing the best protection for the organization's infrastructure?	Risk-based Approach
Helena, a cybersecurity analyst at Dion Training, is analyzing a security alert and trying to determine which type of attack was being used by a threat actor. The alert details an incident where an attacker exploited a timing vulnerability that caused the system to process operations out of the intended sequence and allowing unauthorized actions. Which of the following BEST describes this type of attack?	Race Condition
Liam, a cybersecurity analyst at Dion Training, is analyzing a security alert and trying to determine which type of attack was being attempted by a threat actor. The following line in the log file appears to be suspicious: 2023-11-02 14:23:56 [IP:192.168.1.101] [ERROR] User login failed for username: 'admin' OR '1'='1'; Which of the following BEST describes the type of attack attempted by this threat actor?	SQL injection
Sasha, a cybersecurity analyst at Dion Training, is analyzing a security alert and trying to determine which type of attack was	

being used by a threat actor. The alert details an incident where an attacker sent unsolicited messages to a user's smartphone via Bluetooth without any evidence of taking control of the device. Which of the following BEST describes this type of attack?	Bluejacking
Cristian, a cybersecurity analyst at Dion Training, is analyzing a security alert and trying to determine which type of attack was being used by a threat actor. The alert details an incident where an attacker deliberately inputs an excessive amount of data into an application's buffer to try and cause the system to crash and potentially allow for the execution of arbitrary code. Which of the following BEST describes this type of attack?	Buffer Overflow
Jonathan, a cybersecurity analyst at Dion Training, is analyzing a security alert and trying to determine which type of attack was being used by a threat actor. The alert details an incident where an attacker inserted malicious scripts into input fields on a website, which were then executed in the browser of any user viewing that data. Which of the following BEST describes this type of attack?	Cross-site Scripting
Susan, a cybersecurity analyst at Dion Training, is analyzing a security alert and trying to determine which technique can enhance security by ensuring that only explicitly approved applications are allowed to run on a system. Which of the following BEST describes this technique?	Application Restriction
Sahra, a cybersecurity analyst at Dion Training, is reviewing a system's configurations and notices several software processes running that are not required for essential functionality. Which of the following actions should she take to enhance security?	Disable Unnecessary Services
Margo, a cybersecurity engineer at Dion Training, is tasked with establishing a safe starting point for the configurations of computer systems and networks. Which of the following BEST describes what she is aiming to create?	Secure Baselines
Roberto, a cybersecurity analyst at Dion Training, is responsible for maintaining the security and functionality of computer systems by systematically identifying, testing, deploying, and monitoring software updates. Which of the following BEST describes his responsibility?	Patch Management
Sonia, a cybersecurity analyst at Dion Training, is implementing a set of rules and configurations in a Windows environment to centrally manage and control user and computer settings. Which of the following BEST describes what she is configuring?	Secure Baselines
Which of the following answers can be used to describe technical security controls?	1) Sometimes called logical controls, 2) Executed by computer systems instead of people, 3) Implemented with technology
Which of the answers listed below refer to examples of technical security controls?	Encryption, IDS, Firewall
Which of the following answers refer to the characteristic features of managerial security controls	1) Also known as administrative controls, 2) Focused on reducing the risk of security incidents, 3) Documented in written policies
Examples of managerial security controls include:	Organizational security policy, risk assessments and security awareness training
Which of the answers listed below can be used to describe operational security controls (Select 3 answers)	Focused on the day-to-day procedures of an organization, Used to ensure that the equipment continues to work as specified, Primarily implemented and executed by people (as opposed to computer systems)
Which of the following examples fall into the category of operational security controls? (Select 3 answers)	Configuration management, system backups and patch management
Which of the answers listed below refers to security controls designed to deter, detect, and prevent unauthorized access, theft, damage, or destruction of material assets?	Physical security controls

Which of the following examples do not fall into the category of physical security controls? (Select 3 answers)	Data backups, firewalls and asset management
What are the examples of preventive security controls? (Select 3 answers)	Encryption, Firewalls and AV software
Examples of deterrent security controls include: (Select 3 answers)	Warning signs, Lighting, Fencing/Bollards
Which of the following answers refer(s) to corrective security control(s)?	Incident Response Plans, Backups and system recovery, Disaster Recovery Plans, and Forensic analysis
Which of the answers listed below refer(s) to compensating security control(s)? (Select all thatapply)	Temporary service disablement, MFA and temporary port blocking
The term "Directive security controls" refers to the category of security controls that areimplemented through policies and procedures.	True
Which of the following terms fall into the category of directive security controls? (Select 2 answers)	Incident Response Plans and Acceptable Use Policy
Which of the terms listed below can be used to describe the basic principles of information security?	Confidentiality, Integrity, Availability
The term "Non-repudiation" describes the inability to deny responsibility for performing a specific action. In the context of data security, non-repudiation ensures data confidentiality, provides proof of data integrity, and proof of data origin.	False
Which of the following best applies to the concept of non-repudiation?	Digital certificate
Which type of user account violates the concept of non-repudiation?	Shared account
Which part of the AAA security architecture deals with the verification of the identity of a person or process?	Authentication
In the AAA security architecture, the process of granting or denying access to resources is known as:	Authorization
In the AAA security architecture, the process of tracking accessed services as well as the amountof consumed resources is called:	Accounting
Which of the following solutions provide(s) the AAA functionality?	RADIUS and TACACS+
In the context of the AAA framework, common methods for authenticating people include: (Select 3 answers)	Usernames and passwords, biometrics and MFA
Which of the answers listed below refer to common methods of device authentication used withinthe AAA framework? (Select 3 answers)	Digital certificates, IP addresses, MAC addresses
Which of the following terms describes the process of identifying differences between an organization's current security posture and its desired security posture?	Gap analysis
The term "Zero Trust security" refers to a cybersecurity model that eliminates implicit trust fromnetworks and requires all users and devices to be continuously verified before being granted accessto resources. The implementation of the Zero Trust security involves two distinct components: aData Plane, responsible for defining and managing security policies, and a Control Plane,responsible for enforcing the security policies established by the Data Plane.	False
Which of the answers listed below refers to a Zero Trust Control Plane security approach thattakes into account user identity, device security, network conditions, and other contextualinformation to enable dynamic access decisions?	Adaptive identity
What are the key components of the Zero Trust Control Plane's Policy Decision Point (PDP)?(Select 2 answers)	Policy Engine (PE) and Policy Administrator (PA)

In the Zero Trust security architecture, the Policy Enforcement Point (PEP) is a Data Plane component that enforces the security policies defined at the Control Plane by the Policy Decision Point (PDP).	True
An access control vestibule (a.k.a. mantrap) is a physical security access control system used toprevent unauthorized users from gaining access to restricted areas. An example mantrap could be atwo-door entrance point connected to a guard station wherein a person entering from the outsideremains locked inside until he/she provides authentication token required to unlock the inner door.	True
Which of the following statements about honeypots are true?	1) Honeypots mimic real systems to attract cyber attackers 2) Honeypots contain apparent vulnerabilities that are closely monitored by a security team
What is a honeynet in the context of cybersecurity?	A network of honeypots
Which of the answers listed below refers to a honeynet example?	A network of fake websites, a network of fake servers, a network of fake databases, a network of fake file shares
A honeyfile can be any type of file (e.g., a document, email message, image, or video file)containing real user data intentionally placed within a network or system to attract potential attackers or unauthorized users.	False
A honeyfile can be used for:	Attracting cyber attackers, triggering alerts when accessed, and monitoring network activity
What is a honeytoken?	A unique identifier that is used to track attackers
Which of the following should not be used as honeytokens?	Active user account credentials, Actual URLs to live websites or resources
A process used by organizations to assess and evaluate the potential impact of disruptiveincidents or disasters on their critical business functions and operations is referred to as:	BIA
A hierarchical system for the creation, management, storage, distribution, and revocation of digitalcertificates is known as:	PKI
Which of the answers listed below best describes the characteristics of a public-private key pair?	A pair of keys where one is used for encryption and the other for decryption
What is the typical use of a public key?	Data encryption
Key escrow is a cryptographic technique that enables storing copies of encryption keys with atrusted third party. A Recovery Agent (RA) is a trusted third party (an individual, entity, or system)who is authorized to assist in the retrieval of encryption keys and data on behalf of the data owner.Key escrow and RA are both used to ensure that encrypted data can be decrypted even if the dataowner loses access to their encryption key. Since key escrow and RAs are both components of asingle security solution, the only way to implement key escrow systems is with the use of RAs.	True
Which of the following answers refers to a data storage device equipped with hardware-level encryption functionality?	Self Encrypting Drives (SEDs)
Which of the answers listed below refers to software technology designed to provide confidentiality for an entire data storage device?	Full Disk Encryption (FDE)
An MS Windows component that enables encryption of individual files is called:	Encrypting File System (EFS)
Which of the following software application tools are specifically designed for implementingencryption algorithms to secure data communication and storage? (Select 2 answers)	GNU Privacy Guard (GPG) and Pretty Good Privacy (PGP)
What is the name of a network protocol that secures web traffic via SSL/TLS encryption?	HTTPS

Which of the answers listed below refers to a deprecated TLS-based method for securetransmission of email messages?	SMTPS - SMTPs is a method for securing SMTP with transport layer security and is intended to provide authentication of the communication partners.
Which of the following answers refers to an obsolete protocol used for secure data transfer over the web?	SHTTP
The MIME specification extends the email message format beyond plain text, enabling the transferof graphics, audio, and video files over the Internet mail system. S/MIME is an enhanced version ofthe MIME protocol that enables email security features by providing encryption, authentication,message integrity, and other related services.	True
What is the name of a network protocol that enables secure file transfer over SSH?	SFTP
SFTP is an extension of the FTP protocol that adds support for SSL/TLS encryption.	False
A type of cryptographic network protocol for secure data communication, remote command-linelogin, remote command execution, and other secure network services between two networked computers is known as:	SSH
Which of the answers listed below refers to a suite of protocols and technologies providingencryption, authentication, and data integrity for network traffic?	IPSec
Which part of IPsec provides authentication, integrity, and confidentiality?	ESP
A system that uses public network (such as the Internet) as a means for creating private encrypted connections between remote locations is referred to as:	VPN
Which protocol enables secure, real-time delivery of audio and video over an IP network?	SRTP (Secure Real Time Protocol)
An encryption protocol primarily used in Wi-Fi networks implementing the WPA2 security standardis called:	CCMP
A security protocol designed to improve the security of existing WEP implementations is known as:	TKIP
Which of the following answers refer(s) to deprecated/insecure encryption protocols and cryptographic hash functions? (Select all that apply)	DES, MD-5, SHA-1, SSL, RC4
Which cryptographic protocol is designed to provide secure communications over a computernetwork and is the successor to SSL?	TLS
Examples of techniques used for encrypting information include symmetric encryption (also calledpublic-key encryption) and asymmetric encryption (also called secret-key encryption, or session-keyencryption).	False
In asymmetric encryption, any message encrypted with the use of a public key can only bedecrypted by applying the same algorithm and a matching private key (and vice versa).	True
Which of the algorithms listed below are not symmetric ciphers? (Select 3 answers)	DHE, ECC, and RSA
Which of the following algorithms do(es) not fall into the category of asymmetric encryption?(Select all that apply)	AES, DES, IDEA, RC4
The term "KEK" refers to a type of cryptographic key often used in key management systems toadd an additional layer of security when encrypting and decrypting other cryptographic keys.	True
	PSK

Which of the answers listed below refers to a shared secret authentication method used in WPA,WPA2, and EAP?	
Which of the following answers refers to a protocol used to set up secure connections and exchange of cryptographic keys in IPsec VPNs?	IKE
Which of the answers listed below refers to a key exchange protocol that generates temporary keys for each session, providing forward secrecy to protect past and future communications?	DHE (Diffie-Hellman exchange)
Which of the following answers refers to a cryptographic key exchange protocol that leverages ECC for enhanced security and efficiency?	ECDHE (Elliptic Curve Diffie-Hellman)
Which of the answers listed below refers to a solution designed to strengthen the security of session keys?	PFS (Perfect Forward Secrecy)
Which of the following answers refers to a public-key cryptosystem that leverages themathematical properties of large prime numbers to facilitate secure key exchange, create digitalsignatures, and encrypt data?	RSA
Which cryptographic solution would be best suited for low-power devices, such as IoT devices,embedded systems, and mobile devices?	ECC
Which of the cryptographic algorithms listed below is the least vulnerable to attacks?	AES (of DES, RC4, 3DES), IDEA and RC4 also symmetric algorithms
Which of the following answers refers to a legacy symmetric-key block cipher encryption algorithm?	DES
Which of the answers listed below refers to a deprecated stream cipher used in some legacyapplications, such as WEP?	RC4
Which of the following answers refers to a deprecated (largely replaced by AES) symmetric-keyblock cipher encryption algorithm?	IDEA
What is the recommended replacement for DES?	AES
An IV is a random or pseudorandom value used in cryptography to ensure that the same plaintextinput does not produce the same ciphertext output, even when the same encryption key is used.The IV is typically used with encryption algorithms in block cipher modes to enhance security byintroducing randomness to the encryption process.	True
Which of the answers listed below refers to a logical operation commonly used in the context of cybersecurity, particularly in encryption and obfuscation techniques?	XOR
Which of the following answers refers to a block cipher mode that works by chaining the ciphertextblocks together, such that each ciphertext block depends on the previous block?	CBC (Cipher Block Chaining)
Which block mode transforms a block cipher into a stream cipher enabling the encryption of individual bits or bytes of data?	CFB (Cipher Feedback)
A block cipher mode that combines a unique counter with encryption key to generate a stream of pseudorandom data blocks which are then used for encrypting data is called:	CTM (Counter mode)
Which of the block cipher modes listed below is the simplest/weakest and therefore not recommended for use?	ECB (Electronic Code Book)
Which block cipher mode combines CTM for encryption with an authentication mechanism toensure both data confidentiality and integrity?	Galois/Counter Mode (GCM)
In cryptography, the number of bits in a key used by a cryptographic algorithm is referred to as keysize or key length. The key length determines the maximum number of combinations required	True

tobreak the encryption algorithm, therefore typically a longer key means stronger cryptographicsecurity.	
Which AES key length provides the highest level of security?	AES
Which of the following answers refers to an embedded microcontroller used for secure boot, diskencryption, and system integrity verification?	TPM
Which of the answers listed below refers to a piece of hardware and associated software/firmwaredesigned to provide cryptographic and key management functions?	HSM
Which of the following answers refers to a centralized server that is used to distributecryptographic keys and authenticate users and services within a computer network?	KDC
In a Kerberos-protected network, this type of secure token is granted to users during their initiallogin to enable them access to multiple network services without the need to re-enter their logincredentials.	TGT
In cryptography and security, the term "Secure enclave" typically refers to a protected and isolatedhardware or software environment within a computing device, such as a smartphone, tablet, orcomputer, where sensitive data and cryptographic operations can be stored and processedsecurely.	True
The term "Obfuscation" is used to describe techniques employed to obscure or hide the truemeaning or nature of data, making it challenging for unauthorized parties to decipher or reverse-engineer the information.	True
What is the purpose of steganography?	Hiding data within another piece of data
In the field of data security, the term "Tokenization" refers to the process of replacing sensitive data with nonsensitive information which holds a reference to the original data and enables its processing but has no value when breached.	False
Replacing password characters in a password field with a series of asterisks is an example of:	Data masking
A hash function is a mathematical algorithm that maps data of arbitrary size to a fixed-size hashvalue, typically represented as a short string of characters. The hash function result, also known asa digest or checksum, provides a unique representation of the original data input. The functionalityof hash functions relies on the fact that if there is any change to the data after the original hash wasgenerated, the new hash value calculated after content modification will be different from theoriginal result because hash functions are designed to be sensitive to changes in the input data.	True
Hash functions find use in a variety of applications, including:	Cryptography, Data integrity verification, Password verification and storage, digital signatures and blockchain technology
Which of the answers listed below refers to a cryptographic hash function that has been widely used in the past but is now considered deprecated for security-sensitive applications due to known vulnerabilities?	MD-5
Which of the following answers refers to a family of cryptographic hash functions designed forvarious security-related applications, including digital signatures, password storage, securecommunications, and data integrity verification?	SHA
Which of the hash functions listed below offers the highest level of security?	SHA-3 (of MD-5, SHA-3, RIPEMD-160, HMAC)
Which of the following combines a cryptographic hash function with a secret key to provide a means of verifying both the authenticity and integrity of a message or data?	HMAC

Which of the answers listed below refers to a non-cryptographic hash function often used for error-checking purposes?	CRC
Which of the following answers refers to a type of additional input that increases password complexity and provides better protection against brute-force, dictionary, and rainbow table attacks?	Salt
A pseudo-random data added to a password before hashing is referred to as:	Salt
Which cryptographic technique is used to prevent the effectiveness of rainbow tables in crackinghashed passwords?	Salting
Which of the answers listed below refers to a cryptographic technique that verifies the authenticityand integrity of digital documents or messages by using a unique encrypted identifier from thesender?	Digital signature
Which of the following answers refer to algorithms used for generating and verifying digitalsignatures? (Select 3 answers)	ECDSA, RSA, DSA
Which of the answers listed below refer to DSA? (Select 2 answers)	Specifically designed for creating and verifying digital signatures, Based on the mathematical properties of large prime numbers
Which of the following answers refer to the characteristic features of RSA?	Primarily used for secure communication and digital signatures, used for data encryption
Which of the answers listed below best describe the characteristics of ECDSA? (Select 2 answers)	Used for digital signatures, and does not include a native encryption function
Given the computational limitations of IoT devices, smartcards, and mobile devices, which of thefollowing digital signature algorithms would be the most efficient choice due to its smaller key sizeand lower processing requirements?	ECDSA
Key stretching is a cryptographic technique that enhances the security of sensitive data, such ascryptographic keys and passwords. It works by repeatedly applying a resource-intensive function oralgorithm to the input data, thus increasing the computational effort required to derive the originalkey or password, which makes the data more resistant to brute-force, dictionary, or rainbow tableattacks.	False
Which of the following is an example of a key stretching algorithm?	PBKDF2
The term "Open public ledger" is used to describe a distributed database stored across multiplecomputers in a P2P network.	True
Blockchain technology is an example of:	Open public ledger
Which of the answers listed below refers to a set of standards and specifications that definevarious cryptographic techniques, including formats for public keys, private keys, digital signatures,and digital certificates?	PKCS
Which of the following defines a file format for storing and exchanging personal identity information, including private keys and digital certificates?	P12
A type of digital document that verifies the identity of an individual, device, service, or organizationin online communications is known as:	Digital certificate
What is the role of Registration Authority (RA) in PKI? (Select 2 answers)	Accepting requests for digital certificates and authenticating the entity making the request
Which of the answers listed below refers to a trusted third party responsible for issuing, revoking,and managing digital certificates?	CA
Which of the following answers refers to a means for periodic publication of all digital certificates that have been revoked?	CRL
	OCSP

Which of the answers listed below refers to a protocol that enables on-demand querying of therevocation status of a digital certificate?	
What is the fastest way to check the validity of a single digital certificate?	OCSP
Which of the following answers can be used to describe self-signed digital certificates? (Select 3 answers)	Not trusted by web browsers and other applications, Used in trusted environments such as internal networks and development environments, Not backed by a well-known and trusted party
A self-signed digital certificate is just a	self-signed digital certificate
Third-party digital certificates, issued by trusted CAs, are automatically trusted by most browsers and operating systems, involve a cost, and require validation of the applicant's identity. In contrast, self-signed certificates, issued by the entity to itself, are not automatically trusted, are free to createand use, and do not require validation by a CA.	True
In the context of digital certificates, the term "Root of trust" refers to the highest level of trust within a PKI system. It is typically represented by a root CA, which is a trusted third party that serves as the foundation for the entire PKI. All other entities in the PKI hierarchy, including intermediate CAs and end-entities (such as web servers, email servers, user devices, IoT devices, and individual users), derive their trust from this root. When a certificate is issued and signed by an intermediate CA, it gains trust through a chain of trust back to the root CA. This hierarchical trust model allows users and systems to trust certificates presented by websites, services, or individuals because they can trace the trust back to the well-established root of trust.	True
Which of the following answers can be used to describe self-signed digital certificates?	Not trusted by default web browsers and other applications, Used in trusted environments such as internal networks and development environments, Not backed by a well-known and trusted third party
Which of the answers listed below refers to a PKI trust model?	Single CA model, Hierarchical model (root CA + intermediate CA's), mesh model(cross-certifying CA's), web of trust model (all CAs function as root CAs), Chain of trust model (multiple CAs in a sequential chain), Bridge model (cross-certifying between separate PKIs), Hybrid model (combining aspects of different models)
Which of the following answers refers to a cryptographic file generated by an entity requesting adigital certificate from a CA?	CSR (Certificate Signing Request)
A type of digital certificate that can be used to secure multiple subdomains within a primary domainis known as:	Wildcard certificate
Which digital certificate type allows to secure multiple domain names or subdomains with a single certificate?	Subject Alternative Name (SAN) certificate
Which of the answers listed below refers to an identifier used for PKI objects?	OID - Object Identifier
In IT security, the term "Shadow IT" is used to describe the practice of using IT systems, software,or services within an organization without the explicit approval or oversight of the organization's ITdepartment.	True
Choose an answer from the drop-down list on the right to match a threat actor type on the left with its common attack vector attribute.	Nation-state: External Unskilled attacker: Internal/external Hacktivist: External Insider threat: Internal Organized crime: External Shadow IT: External
	Nation-state: High resources and funding Unskilled attacker: Low resources and funding Hacktivist: Low to medium resources and funding

Match each threat actor type with its corresponding resources/funding attribute.	Insider threat: Low to high resources and funding Shadow IT: Low to medium resources and funding
Assign the level of sophistication attribute to each threat actor type listed below.	Nation-state: High level of sophistication Unskilled attacker: Low level of sophistication Hacktivist: Low to medium level of sophistication Insider threat: Low to high level of sophistication Organized crime: Medium to high level of sophistication Shadow IT: Low to medium level of sophistication
From the drop-down list on the right, select the typical motivations behind the actions of each threat actor type.	Nation-state: Espionage, political/philosophicalbeliefs, disruption/chaos, war Unskilled attacker: Disruption/chaos, financial gain,revenge Hacktivist: Ethical beliefs, philosophical/politicalbeliefs, disruption/chaos Insider threat: Revenge, financial gain, servicedisruption Organized crime: Financial gain, data exfiltration,extortion Shadow IT: Convenience, lack of awareness ofsecurity risks, meeting specific needs
Which of the following terms is used to describe sophisticated and prolonged cyberattacks often carried out by well-funded and organized groups, such as nation-states?	APT
An attack surface is the sum of all the potential points (vulnerabilities) through which an attackercan interact with or compromise a system or network, indicating the overall exposure to potentialthreats. Examples of attack surfaces can be all software, hardware, and network interfaces withknown security flaws. A threat vector represents the method or means through which a cyber threatis introduced or delivered to a target system. It outlines the pathway or avenue used by attackers toexploit vulnerabilities. Common threat vector types include phishing emails, malware, drive-bydownloads, and social engineering techniques.	True
Which of the answers listed below refers to an email-based threat vector?	Spoofing, Phishing, BEC attacks, Malicious links, Malware attachments
Which of the following terms refers to a threat vector commonly associated with SMS-based communication?	Smishing
Which of the answers listed below refers to an example of a potential threat vector in IM-based communication?	Phishing attack, Malware distribution, Spoofing attack, eavesdropping, account hijacking, malicious link/attachment
Which of the following answers refer to examples of image-based threat vectors? (Select 3 answers)	Steganography, Image spoofing and malware embedded images
Which of the answers listed below refers to a file-based threat vector?	PDF exploits, malicious macros in documents, compressed files (ZIP, RAR), Malicious scripts in web pages, infected images, malicious executables
Which of the following answer choices is an example of a threat vector type that is typical for voicecommunication?	Vishing
Examples of threat vectors directly related to the use of removable devices include: (Select 2 answers)	Malware delivery, data exfiltration
Which of the answers listed below refer(s) to client-based software threat vector(s)? (Select all that apply)	Drive-by download via web browser, malicious macro, USB-based attack, Infected executable file, malicious attachment in email application
Which of the following answers refer to agentless software threat vectors? (Select 2 answers)	Network protocol vulnerability and packet sniffing
Exploiting known vulnerability is a common threat vector for:	Unsupported systems/apps
A solution that simplifies configuration of new wireless networks by allowing non-technical users toeasily configure network security settings and add new devices to an existing network is called:	Wi-Fi Protected Setup (WPS)
	WPS, WPA, WPA2, WEP

Which of the wireless technologies listed below are considered potential threat vectors and shouldbe avoided due to their known vulnerabilities? (Select all that apply)	
The term "Evil twin" refers to a rogue WAP set up for eavesdropping or stealing sensitive userdata. Evil twin replaces the legitimate AP and by advertising its own presence with the same ServiceSet Identifier (SSID, a.k.a. network name) appears as a legitimate AP to connecting hosts.	True
Which of the following answers refers to a threat vector characteristic only to wired networks?	Cable tapping
Examples of threat vectors related to Bluetooth communication include: bluesmacking (a type ofDoS attack that targets Bluetooth devices by overwhelming them with excessive traffic), bluejacking(the practice of sending unsolicited messages or data to a Bluetooth-enabled device), bluesnarfing(gaining unauthorized access to a Bluetooth device and data theft), and bluebugging (gainingremote control over a Bluetooth device).	True
Which of the answers listed below refers to the most probable cause of an unauthorized access caused by the exploitation of a specific network entry point?	Open service ports
The importance of changing default usernames and passwords can be illustrated by the example of certain network devices (such as routers), which are often shipped with default and well-known admin credentials that can be looked up on the web.	True
Which of the following would be the best solution for a company that needs IT services but lacksany IT personnel?	MSP (Managed Service Provider)
Which of the terms listed below refers to a third-party vendor offering IT security management services? (Select best answer)	MSSP (Managed Security Service Provider)
Which of the following answers refer to common threat vectors that apply to MSPs, vendors, and suppliers in the supply chain?	Propagation of malware and social engineering techniques
A social engineering technique whereby attackers under disguise of a legitimate request attempt togain access to confidential information is commonly referred to as:	Phishing
Which social engineering attack relies on identity theft?	Impersonation
A BEC attack is an example of:	Phishing
Which of the answers listed below refers to a social engineering technique where an attackercreates a false scenario or situation to deceive the victim into revealing sensitive information?	Pretexting
Which of the following terms refers to a platform used for watering hole attacks?	Websites
The term "URL hijacking" "Typosquatting" refers to a deceptive practice involving the deliberate registration of domain names with misspellings or slight variations that closely resemble well-established and popular domain names. The primary goal of this strategy is to exploit the common typographical errors made by users while entering URLs into their web browser's address bar. Beyond capturing inadvertent traffic, typosquatting may also be used for hosting phishing sites to trick users into divulging sensitive information, distributing malware through deceptive websites, generating ad revenue by redirecting mistyped traffic, or engaging in brand impersonation to harm the reputation of authentic brands or deceive users.	True
Which type of application attack relies on introducing external code into the address space of a running program?	Memory injection
	DLL

A collection of precompiled functions designed to be used by more than one Microsoft Windowsapplication simultaneously to save system resources is known as:	
Which of the answers listed below refers to an application attack that relies on executing a library of code?	DLL injection
A type of exploit in which an application overwrites the contents of a memory area it should not have access to is called:	Buffer overflow
A malfunction in a preprogrammed sequential access to a shared resource is described as:	Race condition
A type of vulnerability where the state of a resource is verified at one point in time but may changebefore the resource is actually used is referred to as:	TOC/TOU
A malicious application update is a type of malware that can be installed through a seemingly legitimate software update. The introduction of a malicious update into the application code can been enabled through various means, including:	Unsigned application code, unencrypted update channel (HTTP vs HTTPS), fake update website, unauthorized access to update server, compromised software development processMemory-related vulnerabilities (memory leaks, buffer overflows, race conditions)
Which of the following answers does not refer to a common type of OS-based vulnerability?	Access control and permissions vulnerabilities (weak passwords, privilege escalation), Vulnerabilities in installed applications, system utilities, and device drivers, Memory-related vulnerabilities (memory leaks, buffer overflows, race conditions), Patch and update management vulnerabilities (security patch and update delays, malicious updates), Vulnerabilities related to system/security misconfigurations, Network-related vulnerabilities (DoS attacks, remote code execution attacks)
Which of the answers listed below refers to a security vulnerability that enables inserting malicious code into input fields, such search bars or login forms, to execute unauthorized commands on a database?	SQLi
Which of the following indicates an SQL injection attack attempt?	SELECT * FROM users WHERE userName = 'Alice' AND password = '' OR '1' = '1';
Which of the answers listed below describe the characteristics of a cross-site scripting attack? (Select 3 answers)	Exploits the trust a user's web browser has in a website, A malicious script is injected into a trusted website, User's browser executes attacker's script
Which of the following answers refers to a type of software embedded into a hardware chip?	Firmware
Which of the terms listed below refers to a situation in which a product or service may no longerreceive security patches or other updates, making it more vulnerable to attack?	EOL
What is the main vulnerability related to legacy hardware?	Lack of security updates and patches
The term "VM escape" refers to the process of breaking out of the boundaries of a guest operating system installation to access the primary hypervisor controlling all the virtual machines on the host machine.	True
Which of the following answers refers to a virtualization-related vulnerability where virtualized assets allocated to one VM are improperly isolated and can be accessed or compromised by another VM?	Resource reuse
Which of the answers listed below refers to a cloud-related vulnerability type?	Insecure APIs, Poor access controls, lack of security updates, misconfigured cloud storage, Shadow IT / malicious insiders
The practice of installing mobile apps from websites and app stores other than the officialmarketplaces is referred to as:	Sideloading
Which of the following terms is used to describe the process of removing software restrictionsimposed by Apple on its iOS operating system?	Jailbreaking

The term "Rooting" refers to the capability of gaining administrative access to the operating systemand system applications on:	Android devices
A type of attack aimed at exploiting vulnerability that is present in already released software butunknown to the software developer is known as:	Zero-day attack
Malware that restricts access to a computer system by encrypting files or locking the entire systemdown until the user performs requested action is called:	Ransomware
A Trojan horse is a type of software that performs harmful actions under the guise of a legitimate and useful program. The most characteristic feature of Trojan horse is that while it may function as a legitimate program and possess all the expected functionalities, it also contains a concealed portion of malicious code that the user is unaware of.	True
Which type of Trojan enables unauthorized remote access to a compromised system?	RAT
A standalone malicious computer program that typically propagates itself over a computer networkto adversely affect system resources and network bandwidth is referred to as:	Worm
Malicious software collecting information about users without their knowledge/consent is known as:	Spyware
Which of the answers listed below refer to the characteristic features of bloatware? (Select 3 answers)	Pre-installed on a device by the device manufacturer or retailer, Generally considered undesirable due to negative impact on system performance, Installed without user consent
Which of the following answers refer to the characteristics of a PUP? (Select 3 answers)	Often installed without clear user consent, Generally considered undesirable due to negative impact on system performance, privacy, and security, Can be pre-installed, downloaded, or bundled with other software
Which of the statements listed below apply to the definition of a computer virus? (Select 3 answers)	A self-replicating computer program containing malicious segment, Malware that typically requires its host application to be run to make the virus active, Malicious code that typically attaches itself to an application program or other executable component
Which of the following is an example of spyware?	Keylogger
Malicious code activated by a specific event is called:	Logic bomb
Which of the following answers refers to a collection of software tools used by a hacker to maskintrusion and obtain administrator-level access to a computer or computer network?	Rootkit
The term "RFID cloning" refers to copying the data stored on any RFID-enabled device (includingtags, cards, key fobs, implants, and other objects embedded with RFID technology) onto anotherRFID-enabled device, which then can be read and used in the same way as the original tag. WhileRFID cloning can be utilized for legitimate purposes, such as replicating important tags for backupand testing purposes, it also poses significant security risk, as duplicate tags can potentially be usedfor gaining unauthorized access or unauthorized information disclosure.	True
As opposed to simple DoS attacks that usually are performed from a single system, a DDoS attack uses multiple compromised computer systems to perform the attack against its target. The intermediary systems that are used as a platform for the attack (often referred to as zombies, and collectively as a botnet) are the secondary victims of the DDoS attack.	True
A type of DDoS attack where an attacker exploits vulnerabilities in certain services or protocols to generate responses that are much larger than the original request is referred to as:	Amplified DDoS attack

What defines a reflected DDoS attack?	Utilizing third-party servers to reflect and amplify attack traffic towards the target
A DNS amplification attack is a type of DDoS attack wherein an attacker sends a small, speciallycrafted DNS query containing a spoofed IP address (the victim's IP) to a compromised DNS server.Upon receiving the query, the DNS server generates a much larger response packet, which is thensent to the victim's IP address, causing potential disruption due to overwhelming traffic.	True
Which of the answers listed below refers to a cyberattack technique that relies on providing false DNS information to a DNS resolver for the purpose of redirecting or manipulating the resolution of domain names to malicious IP addresses?	DNS spoofing
Remapping a domain name to a rogue IP address is an example of what kind of exploit?	DNS cache poisoning
When domain registrants due to unlawful actions of third parties lose control over their domainnames, they fall victim to:	Domain hijacking
Which of the following can be classified as malicious activity indicator on a wireless network?	Rogue AP
The practice of gaining unauthorized access to a Bluetooth device is known as:	Bluesnarfing
A wireless disassociation attack is a type of: (Select 2 answers)	Deauthentication and DoS attack
A wireless jamming attack is a type of:	DoS attack
Which of the answers listed below refers to RFID vulnerability?	Spoofing, eavesdropping, RFID cloning, Data interception, Replay attack, DoS attack
Which of the following is a vulnerability characteristic to NFC communication?	Eavesdropping, data interception, replay attacks, DoS attacks
Which wireless attack focuses on exploiting vulnerabilities found in WEP?	IV attack
Which of the statements listed below can be used to describe the characteristics of an on-path attack? (Select all that apply)	An on-path attack is also known as MITM attack, Attackers place themselves on the communication route between two devices, Attackers intercept or modify packets sent between two communicating devices
A network replay attack occurs when an attacker captures sensitive user data and resends it to the receiver with the intent of gaining unauthorized access or tricking the receiver into unauthorized operations.	True
What are the characteristic features of a session ID? (Select 3 answers)	A unique identifier assigned by the website to a specific user, A piece of data that can be stored in a cookie, or embedded as an URL parameter, Typically stored on the client side (in the user's browser) rather than on the server
In a session replay attack, an attacker intercepts and steals a valid session ID of a user and resends it to the server with the intent of gaining unauthorized access to the user's session or tricking the server into unauthorized operations on behalf of the legitimate user.	True
A technique that allows an attacker to authenticate to a remote server without extracting clear text password from a digest is called:	Pass the hash
What type of action allows an attacker to exploit the XSS vulnerability?	Code injection
Which of the following exploits targets a protocol used for managing and accessing networked resources?	LDAP injection attack
Which type of exploit targets web applications that generate content used to store and transport data?	XML injection attack

Which of the following facilitate(s) privilege escalation attacks? (Select all that apply)	System/application vulnerabilities, System/application misconfigurations, Social engineering techniques
Which of the statements listed below apply to the CSRF/XSRF attack? (Select 3 answers)	Exploits the trust a website has in the user's web browser, A user is tricked by an attacker into submitting unauthorized web requests, Website executes attacker's requests
A dot-dot-slash attack is also referred to as:	Directory traversal attack
Jenna, a new hire at Dion Training, wants to ensure her work conversations remain confidential and are not susceptible to eavesdropping or shoulder surfing attacks. Which of the following should she do?	Holding discussions in secure areas equipped with privacy measures is crucial for maintaining confidentiality. Secure areas prevent unauthorized access and are less prone to surveillance, significantly reducing the risk of eavesdropping or shoulder surfing attacks. These measures ensure that sensitive information is not inadvertently exposed to individuals who might exploit it, thereby maintaining the integrity of the conversation and protecting organizational data.
Lisa, an executive at Dion Training, is using a password manager to maintain different strong passwords for her accounts. What additional step should she take to ensure the security of her password manager?	Enabling multi-factor authentication (MFA) adds an extra layer of security to Lisa's password manager. This approach requires another piece of evidence besides the master password, making unauthorized access much more difficult even if the master password is compromised. MFA could involve something you know (password), something you have (a secure device), or something you are (biometric verification) to significantly enhance the security of your sensitive account information.
Derek, a senior manager at Dion Training, discovers a USB drive in the parking lot and wants to identify the owner. Considering the risks, what should be his course of action?	Giving the USB drive to the IT department is the safest action to take since the IT professionals are equipped with the right tools and protocols to examine the drive safely without risking a potential security breach. Plugging an unknown USB into a computer could introduce malware into the network, while ignoring it or asking around doesn't mitigate the risk of malicious content or ensure the device's proper handling. The IT department can take precautionary measures to safeguard your organization's security.
Sandra, a team leader at Dion Training, is concerned about phishing attempts targeting her team members working remotely. To address this threat, what approach should she advocate for within the team?	Ignoring unsolicited emails requesting sensitive data is vital in defending against phishing attempts. Phishing typically tricks individuals into divulging personal information, often arriving via email. These emails may appear genuine but contain deceptive content, urging quick actions like clicking links or sharing passwords or bank details. By dismissing such requests, teams can lower the risk of unintentionally compromising security. It's essential not to interact with these messages as they often lead to fraudulent sites aimed at data theft.
Chris, the head of the IT department at Dion Training, wants to fortify the company's defense against social engineering attacks. Which strategy should he incorporate to enhance the overall security culture?	Regular training and simulated cyber-attacks are crucial for bolstering defenses against social engineering. This proactive approach enhances employee awareness and response skills. Simulated attacks provide real-world experience without actual risk, testing and reinforcing correct reactions to threats. These practices cultivate a robust security culture, where everyone plays a role in preventing breaches, strengthening the overall defense strategy.
Jessica, a cybersecurity analyst at Dion Training, wants to streamline the process of responding to incidents where employees click on links in phishing emails to ensure that certain steps are automated while others require human analysis. Which of the following should they utilize to achieve this?	A runbook is essentially an automated version of a playbook that includes clearly defined interaction points for human intervention and analysis, making it the ideal choice for Jessica's needs to automate certain steps in incident response while still requiring human judgment at specific stages.
Michael, a lead software engineer at Dion Training, is tasked with optimizing a complex deployment process that involves coordinating multiple automated tasks across various systems to achieve a synchronized, efficient workflow. Which of the following should he focus on to ensure a seamless integration of these tasks?	Orchestration involves the coordinated and sequenced execution of multiple automated tasks, ensuring they work harmoniously within a larger, complex process.
Jordan, a system administrator at Dion Training, is tasked with optimizing the process of regularly updating software applications	

on all company workstations. These updates are released at predictable intervals and require the same series of repetitive and consistent steps to install the software updates across multiple systems. Which of the following strategies should they choose to ensure these updates are applied efficiently and reliably every time they are released?	Given that the software updates are regular, predictable, and require the same steps for each system, setting up automation would allow these tasks to be completed efficiently without the need for manual intervention each time. Automation excels in managing repetitive tasks that do not require complex, multi-step solutions or human decision-making during each stage.
Which of these practices specifically involves an administrator setting up a system to assign and manage system permissions. Once established, it won't require further administrative actions to ensure that consistent access controls based on individuals' roles within the organization are being utilized?	Automating RBAC (Role-based Access Controls) directly relates to the systematic management of system permissions which is an essential aspect of an organization's cybersecurity strategy. This automation ensures that individuals have appropriate access levels consistent with their roles to enhance your security by preventing unauthorized access. Automated provisioning and de-provisioning in RBAC allow for the dynamic updating of permissions when individuals join, change roles, or leave the organization to ensure that you maintain tight control over who has access to sensitive information.
Which of the following best describes the difference between Continuous Delivery and Continuous Deployment in CI/CD?	Continuous Delivery is a software development practice where new code changes are automatically tested and prepared for a release that allows for reliable, manual deployments to a production environment at any chosen time. Continuous Deployment is a practice that extends Continuous Delivery so that automatic deployment of every validated change is made directly to the production environment so that the time to go live is reduced while eliminating the need for manual interventions in deployments.
Jason, a cybersecurity analyst at Dion Training, is reviewing the log from a web application firewall and believes an attack was attempted by a threat actor. Here is the log snippet used during the review: Time | Source IP | Request URL | Status | Action --- 12:30:15 | 203.0.113.5 | /products?category=' OR '1'='1 | 200 | Allowed 12:30:16 | 203.0.113.5 | /login?username=admin'-- | 200 | Allowed 12:30:17 | 203.0.113.5 | /search?query=laptops | 200 | Allowed 12:30:18 | 203.0.113.5 | /products?category='; DROP TABLE users; -- | 403 | Blocked	SQL injection
Tony, a cybersecurity analyst at Dion Training, is examining the following snippet from an authentication log: Time | Source IP | Username | Event | Password Attempted --- 15:32:00 | 203.0.113.7 | Admin | Authentication Attempt | admin1 15:32:01 | 203.0.113.7 | Admin | Authentication Attempt | Xyz@123 15:32:02 | 203.0.113.7 | Admin | Authentication Attempt | qwertyABCD! 15:32:02 | 203.0.113.7 | Admin | Authentication Attempt | 1Adm!nP@ss 15:32:03 | 203.0.113.7 | Admin | Authentication Attempt | $ecUr3P@55 Based on the log snippet above, which type of attack is most likely being attempted?	The log shows multiple authentication attempts from the same source IP for the same username with various complex and random passwords in a very short time frame. This pattern is indicative of a brute force attack in which an attacker tries numerous password combinations to gain unauthorized access.
Jackie, a cybersecurity analyst at Dion Training, is reviewing the following snippet from a web server log: Time | Source IP | Request URL | HTTP Status | Payload -- 21:45:00 | 203.0.113.4 | /api/createUser | 200 | <user><name>John</name><password>abc123</password></user> 21:45:05 | 203.0.113.4 | /api/createUser | 200 | <user><name>Jane</name><password>xyz789</password></user>	The log shows malformed XML payloads in the request URLs, specifically at 21:45:10 and 21:45:15, indicating an attempt to inject malicious XML content (1 and <!-- injected -->). This pattern is indicative of an XML Injection attack, where an attacker tries to manipulate the logic of the application by injecting malicious XML data.

```
21:45:10 | 203.0.113.4 | /api/createUser | 400 | <user><name>Bob</name><password>123&<isAdmin>1</isAdmin></password></user>
```