Number: 112-51
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 112-51

Exam Name: Network Defense Essentials Exam

Exam A

QUESTION 1
Which of the following solutions is a software or a hardware device on a network or host that filters the incoming and outgoing traffic to prevent unauthorized access to private networks?

A. Firewall
B. Router
C. Hub
D. Switch

Correct Answer: A
Section:
Explanation:
A firewall is a software or a hardware device on a network or host that filters the incoming and outgoing traffic to prevent unauthorized access to private networks. A firewall can use various criteria, such as IP addresses, ports, protocols, or application rules, to allow or deny the traffic. A firewall can also perform other functions, such as logging, auditing, encryption, or proxy services. A firewall can be deployed at different levels of a network, such as network perimeter, network segment, or host level12.
Reference: Network Defense Essentials - EC-Council Learning, Firewall (computing) - Wikipedia

QUESTION 2
Which of the following techniques protects sensitive data by obscuring specific areas with random characters or codes?

A. Data retention
B. Data resilience
C. Data backup
D. Data masking

Correct Answer: D
Section:

QUESTION 3
Which of the following components of VPN is used to manage tunnels and encapsulate private data?

A. Remote network
B. VPN protocol
C. Network access server
D. VPN client

Correct Answer: B
Section:
Explanation:
A VPN protocol is a component of VPN that is used to manage tunnels and encapsulate private data. A VPN protocol defines the rules and standards for establishing and maintaining a secure connection between the VPN client and the VPN server. A VPN protocol also specifies how the data is encrypted, authenticated, and transmitted over the tunnel. Some common VPN protocols are IPSec, SSL/TLS, PPTP, L2TP, and OpenVPN12.
Reference: Network Defense Essentials - EC-Council Learning, VPN Protocols Explained & Compared: OpenVPN, IPSec, PPTP, IKEv2

QUESTION 4

Which of the following practices helps security professionals protect mobile applications from various attacks?

A. Always cache app data
B. Use containerization for critical corporate data
C. Use query string while handling sensitive data
D. Allow apps to save passwords to avoid multiple logins

Correct Answer: B
Section:
Explanation:
Containerization is a practice that helps security professionals protect mobile applications from various attacks. Containerization is a technique that isolates critical corporate data from the rest of the device data and applications. Containerization creates a secure and encrypted environment on the device where the corporate data and applications can be accessed and managed. This way, containerization prevents unauthorized access, data leakage, malware infection, or device theft from compromising the corporate data and applications12.
Reference: Network Defense Essentials - EC-Council Learning, Mobile Application Security: Containerization vs. App Wrapping vs. SDK

QUESTION 5
Which of the following layers of loT architecture employs protocols and networks for connecting, sending, and receiving data between devices and network?

A. Device layer
B. Cloud layer
C. Communication layer
D. Process layer

Correct Answer: C
Section:
Explanation:
The communication layer of IoT architecture employs protocols and networks for connecting, sending, and receiving data between devices and network. The communication layer is responsible for enabling data exchange among the IoT devices and the cloud or other devices. The communication layer can use various types of networks, such as wired, wireless, cellular, or satellite, and various types of protocols, such as TCP/IP, MQTT, CoAP, or ZigBee12.
Reference: Network Defense Essentials - EC-Council Learning, IoT Architecture: The 4 Layers of an IoT System

QUESTION 6
Cibel.org, an organization, wanted to develop a web application for marketing its products to the public. In this process, they consulted a cloud service provider and requested provision of development tools, configuration management, and deployment platforms for developing customized applications.
Identify the type of cloud service requested by Cibel.org in the above scenario.

A. Security-as-a-service (SECaaS)
B. Platform-as-a-service
C. Infrastructure-as-a-service {laaS)
D. Identity-as-a-service {IDaaS)

Correct Answer: B
Section:
Explanation:
The type of cloud
The type of cloud service requested by Cibel.org in the above scenario is Platform-as-a-service (PaaS). PaaS is a cloud-based service that delivers a range of developer tools and deployment capabilities. PaaS provides a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications. PaaS customers do not need to install, configure, or manage the underlying infrastructure, such as servers, storage, network, or operating system. Instead, they can focus on the application development and deployment process, using the tools and services provided by the cloud service provider. PaaS solutions support cloud-

native development technologies, such as microservices, containers, Kubernetes, serverless computing, that enable developers to build once, then deploy and manage consistently across private cloud, public cloud and on-premises environments. PaaS also offers features such as scalability, availability, security, backup, and monitoring for the applications.PaaS is suitable for organizations that want to develop customized applications without investing in or maintaining the infrastructure123.Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-40 to 3-41
What is PaaS? A Beginner's Guide to Platform as a Service - G2, G2, February 19, 2020
Cloud Service Models Explained: SaaS, IaaS, PaaS, FaaS - Jelvix, Jelvix, July 14, 2020

QUESTION 7
Ben, a computer user, applied for a digital certificate. A component of PKI verifies Ben's identity using the credentials provided and passes that request on behalf of Ben to grant the digital certificate.
Which of the following PKI components verified Ben as being legitimate to receive the certificate?

A. Certificate authority (CA)
B. Registration authority {RA)
C. Certificate directory
D. Validation authority (VA)

Correct Answer: B
Section:
Explanation:
The PKI component that verified Ben as being legitimate to receive the certificate is the registration authority (RA). An RA is an entity that is responsible for identifying and authenticating certificate applicants, approving or rejecting certificate applications, and initiating certificate revocations or suspensions under certain circumstances. An RA acts as an intermediary between the certificate authority (CA) and the certificate applicant, and performs the necessary checks and validations before forwarding the request to the CA. The CA is the entity that signs and issues the certificates, and maintains the certificate directory and the certificate revocation list. A certificate directory is a repository of issued certificates that can be accessed by users or applications to verify the validity and status of a certificate. A validation authority (VA) is an entity that provides online certificate validation services, such as OCSP or SCVP, to verify the revocation status of a certificate in real time123.
Reference:
Public key infrastructure - Wikipedia, Wikipedia, March 16, 2021
Components of a PKI - The National Cyber Security Centre, NCSC, 2020
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-26 to 3-27

QUESTION 8
George, a certified security professional, was hired by an organization to ensure that the server accurately responds to customer requests. In this process, George employed a security solution to monitor the network traffic toward the server. While monitoring the traffic, he identified attack signatures such as SYN flood and ping of death attempts on the server.
Which of the following categories of suspicious traffic signature has George identified in the above scenario?

A. Informational
B. Reconnaissance
C. Unauthorized access
D. Denial-of-service (DoS)

Correct Answer: D
Section:
Explanation:
Denial-of-service (DoS) is the category of suspicious traffic signature that George identified in the above scenario. DoS signatures are designed to detect attempts to disrupt or degrade the availability or performance of a system or network by overwhelming it with excessive or malformed traffic. SYN flood and ping of death are examples of DoS attacks that exploit the TCP/IP protocol to consume the resources or crash the target server. A SYN flood attack sends a large number of TCP SYN packets to the target server, without completing the three-way handshake, thus creating a backlog of half-open connections that exhaust the server's memory or bandwidth. A ping of death attack sends a malformed ICMP echo request packet that exceeds the maximum size allowed by the IP protocol, thus causing the target server to crash or reboot. DoS attacks can cause serious damage to the organization's reputation, productivity, and revenue, and should be detected and mitigated as soon as possible123.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-33 to 3-34

What is a denial-of-service attack?, Cloudflare, 2020
Denial-of-service attack - Wikipedia, Wikipedia, March 16, 2021

QUESTION 9
Identify the IoT communication model that serves as an analyzer for a company to track monthly or yearly energy consumption. Using this analysis, companies can reduce the expenditure on energy.

A. Device-to-device model
B. Cloud-to-cloud model
C. Device-to-cloud model
D. Device-to-gateway model

Correct Answer: C
Section:
Explanation:
The IoT communication model that serves as an analyzer for a company to track monthly or yearly energy consumption is the device-to-cloud model. The device-to-cloud model is a IoT communication model where the IoT devices, such as smart meters, sensors, or thermostats, send data directly to the cloud platform, such as AWS, Azure, or Google Cloud, over the internet. The cloud platform then processes, analyzes, and stores the data, and provides feedback, control, or visualization to the users or applications. The device-to-cloud model enables the company to monitor and optimize the energy consumption of the IoT devices in real time, and to leverage the cloud services, such as machine learning, big data analytics, or artificial intelligence, to perform advanced energy management and demand response. The device-to-cloud model also reduces the complexity and cost of the IoT infrastructure, as it does not require intermediate gateways or servers to connect the IoT devices to the cloud123.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-38 to 3-39
IoT Communication Models: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing, DZone, July 9, 2018
IoT Communication Models: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing, Medium, March 26, 2019

QUESTION 10
Amber is working as a team lead in an organization. She was instructed to share a policy document with all the employees working from remote locations and collect them after filling. She shared the files from her mobile device to the concerned employees through the public Internet. An unauthorized user accessed the file in transit, modified the file, and forwarded it to the remote employees.
Based on the above scenario, identify the security risk associated with mobile usage policies.

A. Lost or stolen devices
B. Infrastructure issues
C. Improperly disposing of devices
D. Sharing confidential data on an unsecured network

Correct Answer: D
Section:
Explanation:
Sharing confidential data on an unsecured network is a security risk associated with mobile usage policies. Mobile devices are often used to access and transmit sensitive information over public or untrusted networks, such as WiFi hotspots, cellular networks, or Bluetooth connections. This exposes the data to interception, modification, or redirection by malicious actors who may exploit mobile security vulnerabilities or use network-based attacks, such as man-in-the-middle, spoofing, or sniffing. To prevent this risk, mobile users should follow best practices such as using encryption, VPN, certificate pinning, and secure protocols to protect the data in transit. They should also avoid sending or receiving sensitive data over unsecured networks or applications, and verify the identity and integrity of the endpoint servers before establishing a connection.
Reference:
The 9 Most Common Security Threats to Mobile Devices in 2021, Auth0, June 25, 2021
7 Mobile App Security Risks and How to Mitigate Them, Cypress Data Defense, July 10, 2020
The Latest Mobile Security Threats and How to Prevent Them, Security Intelligence, February 19, 2019

QUESTION 11
Barbara, a security professional, was monitoring the IoT traffic through a security solution. She identified that one of the infected devices is trying to connect with other IoT devices and spread malware onto the network.
Identify the port number used by the malware to spread the infection to other IoT devices.

A. Port 25
B. Port 443
C. Port 110
D. Port 48101

Correct Answer: D
Section:
Explanation:
Port 48101 is the port number used by the malware to spread the infection to other IoT devices. This port is associated with the Mirai botnet, which is one of the most notorious IoT malware that targets vulnerable IoT devices and turns them into a network of bots that can launch distributed denial-of-service (DDoS) attacks. Mirai scans the internet for IoT devices that use default or weak credentials and infects them by logging in via Telnet or SSH. Once infected, the device connects to a command and control (C&C) server on port 48101 and waits for instructions. The C&C server can then direct the botnet to attack a target by sending TCP, UDP, or HTTP requests. Mirai has been responsible for some of the largest DDoS attacks in history, such as the one that disrupted Dyn DNS in 2016 and affected major websites like Twitter, Netflix, and Reddit.
Reference:
Mirai (malware), Wikipedia, March 16, 2021
Mirai Botnet: A History of the Largest IoT Botnet Attacks, Imperva, December 10, 2020
Mirai Botnet: How IoT Devices Almost Brought Down the Internet, Cloudflare, March 17, 2021

QUESTION 12
Below are the various steps involved in establishing a network connection using the shared key authentication process.
1.The AP sends a challenge text to the station.
2.The station connects to the network.
3.The station encrypts the challenge text using its configured 128-bit key and sends the encrypted text to the AP.
4.The station sends an authentication frame to the AP.
5.The AP uses its configured WEP key to decrypt the encrypted text and compares it with the original challenge text.
What is the correct sequence of steps involved in establishing a network connection using the shared key authentication process?

A. 4 -- >2 -- >1 -- >3 -- >5
B. 4 -- >1 -- >3 -- >5 -- >2
C. 2 -- >4 -- >5 -- >1 -- >3
D. 4 -- >5 -- >3 -- >2 -- >1

Correct Answer: B
Section:
Explanation:
The correct sequence of steps involved in establishing a network connection using the shared key authentication process is 4 -> 1 -> 3 -> 5 -> 2. This is based on the following description of the shared key authentication process from the Network Defense Essentials courseware:
The station sends an authentication frame to the AP, indicating that it wants to use shared key authentication.
The AP responds with an authentication frame containing a challenge text, which is a random string of bits.
The station encrypts the challenge text using its configured WEP key, which is derived from the shared secret key (password) that is also known by the AP. The station sends the encrypted text back to the AP in another authentication frame.
The AP decrypts the encrypted text using its configured WEP key and compares it with the original challenge text. If they match, the AP sends a positive authentication response to the station. If they do not match, the AP sends a negative authentication response to the station.
The station connects to the network if the authentication is successful.
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-18 to 3-19
Shared Key Authentication - Techopedia, Techopedia, June 15, 2017

QUESTION 13
Identify the backup mechanism that is performed within the organization using external devices such as hard disks and requires human interaction to perform the backup operations, thus, making it suspectable to theft or

natural disasters.

A. Cloud data backup
B. Onsite data backup
C. Offsite data backup
D. Online data backup

Correct Answer: B
Section:
Explanation:
Onsite data backup is the backup mechanism that is performed within the organization using external devices such as hard disks and requires human interaction to perform the backup operations, thus, making it susceptible to theft or natural disasters. Onsite data backup means storing the backup data on a local storage device, such as an external hard drive, a USB flash drive, a CD/DVD, or a tape drive, that is physically located in the same premises as the original data source. Onsite data backup has some advantages, such as fast backup and restore speed, easy access, and low cost. However, it also has some disadvantages, such as requiring manual intervention, occupying physical space, and being vulnerable to damage, loss, or theft. If a disaster, such as a fire, flood, earthquake, or power outage, occurs in the organization, both the original data and the backup data may be destroyed or inaccessible. Therefore, onsite data backup is not a reliable or secure way to protect the data from unforeseen events.
Reference:
Should I Use an External Hard Drive for Backup in 2024?, Cloudwards, February 8, 2024
How to Back Up a Computer to an External Hard Drive, Lifewire, April 1, 2022
Best Way to Backup Multiple Computers to One External Drive, AOMEI, December 29, 2020

QUESTION 14
Which of the following types of network traffic flow does not provide encryption in the data transfer process, and the data transfer between the sender and receiver is in plain text?

A. SSL traffic
B. HTTPS traffic
C. SSH traffic
D. FTP traffic

Correct Answer: D
Section:
Explanation:
FTP traffic does not provide encryption in the data transfer process, and the data transfer between the sender and receiver is in plain text. FTP stands for File Transfer Protocol, and it is a standard network protocol for transferring files between a client and a server over a TCP/IP network. FTP uses two separate channels for communication: a control channel for sending commands and receiving responses, and a data channel for transferring files. However, FTP does not encrypt any of the data that is sent or received over these channels, which means that anyone who can intercept the network traffic can read or modify the contents of the files, as well as the usernames and passwords used for authentication. This poses a serious security risk for the confidentiality, integrity, and availability of the data and the systems involved in the file transfer. Therefore, FTP is not a secure way to transfer sensitive or confidential data over the network.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-31 to 3-32
What is FTP, and Why Does It Matter in 2021?, Kinsta, January 4, 2021
FTP Security, Wikipedia, February 9, 2021

QUESTION 15
Alice was working on her major project; she saved all her confidential files and locked her laptop. Bob wanted to access Alice's laptop for his personal use but was unable to access the laptop due to biometric authentication. Which of the following network defense approaches was employed by Alice on her laptop?

A. Retrospective approach
B. Preventive approach
C. Reactive approach

D. Proactive approach

Correct Answer: B
Section:
Explanation:
The network defense approach that was employed by Alice on her laptop was the preventive approach. The preventive approach aims to stop or deter potential attacks before they happen by implementing security measures that reduce the attack surface and increase the difficulty of exploitation. Biometric authentication is an example of a preventive measure that uses a physical characteristic, such as a fingerprint, iris, or face, to verify the identity of the user and grant access to the device or system. Biometric authentication is more secure than traditional methods, such as passwords or PINs, because it is harder to forge, guess, or steal. By locking her laptop and using biometric authentication, Alice prevented Bob from accessing her laptop and her confidential files without her permission.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 1-7 to 1-8
What is Biometric Authentication?, Norton, July 29, 2020
An introduction to network defense basics, Enable Sysadmin, November 26, 2019

QUESTION 16
Kalley, a network administrator of an organization, has installed a traffic monitoring system to capture and report suspicious traffic signatures. In this process, she detects traffic containing password cracking, sniffing, and brute-forcing attempts.Which of the following categories of suspicious traffic signature were identified by Kalley through the installed monitoring system?

A. Reconnaissance signatures
B. Unauthorized access signatures
C. Denial-of-service (DoS) signatures
D. Informational signatures

Correct Answer: B
Section:
Explanation:
Unauthorized access signatures were identified by Kalley through the installed monitoring system. Unauthorized access signatures are designed to detect attempts to gain unauthorized access to a system or network by exploiting vulnerabilities, misconfigurations, or weak credentials. Password cracking, sniffing, and brute-forcing are common techniques used by attackers to obtain or guess the passwords of legitimate users or administrators and gain access to their accounts or privileges. These techniques generate suspicious traffic patterns that can be detected by traffic monitoring systems, such as Snort, using signature-based detection. Signature-based detection is based on the premise that abnormal or malicious network traffic fits a distinct pattern, whereas normal or benign traffic does not. Therefore, by installing a traffic monitoring system and capturing and reporting suspicious traffic signatures, Kalley can identify and prevent unauthorized access attempts and protect the security of her organization's network.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-33 to 3-34
Detecting Suspicious Traffic via Signatures - Intrusion Detection with Snort, O'Reilly, 2003
Threat Signature Categories - Palo Alto Networks, Palo Alto Networks, 2020

QUESTION 17
Finch, a security auditor, was assigned the task of providing devices to all the employees to enable work from remote locations. Finch restricted the devices to work only for organization-related tasks, and not for personal use.
Which of the following mobile usage policies has Finch implemented in the above scenario?

A. CYOD
B. COBO
C. COPE
D. BYOD

Correct Answer: B
Section:
Explanation:

Finch has implemented the COBO (Corporate-Owned, Business-Only) mobile usage policy in the above scenario. COBO is a policy where the organization provides mobile devices to the employees and restricts them to use the devices only for work-related purposes. The organization has full control over the devices and can enforce security measures, such as encryption, password protection, remote wipe, and application whitelisting or blacklisting. The employees are not allowed to use the devices for personal use, such as browsing the internet, making personal calls, or installing personal apps. COBO is a policy that aims to maximize security and minimize distractions and risks for the organization and the employees.
Reference:
Mobile usage policy in office - sample, cell phone policy in companies and organization, HR Help Board, 2020
Employee Cell Phone Policy Template, Workable, 2020
How Employers Enforce Cell Phone Policies in the Workplace, Indeed, 2022

QUESTION 18
In an organization, employees are restricted from using their own storage devices, and only the company's portable storage devices are allowed. As employees are carrying the company's portable device outside their premises, the data should be protected from unauthorized access.
Which of the following techniques can be used to protect the data in a portable storage device?

A. Data retention
B. Data encryption
C. Data resilience
D. Disk mirroring

Correct Answer: B
Section:
Explanation:
Data encryption is the technique that can be used to protect the data in a portable storage device. Data encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Only authorized parties who have the correct key or algorithm can decrypt and access the data. Data encryption provides security and privacy for the data stored on a portable storage device, such as a USB flash drive or an external hard drive, by preventing unauthorized access, modification, or disclosure. If the device is lost or stolen, the data will remain protected and inaccessible to the unauthorized user. Data encryption can be implemented using software or hardware solutions, such as BitLocker, VeraCrypt, or encrypted USB drives. Data encryption is one of the best practices for securely storing data on portable devices123.
Reference:
7 Ways to Secure Sensitive Data on a USB Flash Drive, UpGuard, August 17, 2022
How to Protect Data on Portable Drives, PCWorld, January 10, 2011
Securely Storing Data, Security.org, December 20, 2022

QUESTION 19
Finch, a security professional, was instructed to strengthen the security at the entrance. At the doorway, he implemented a security mechanism that allows employees to register their retina scan and a unique six- digit code, using which they can enter the office at any time.
Which of the following combinations of authentication mechanisms is implemented in the above scenario?

A. Biornetric and password authentication
B. Password and two-factor authentication
C. Two-factor and smart card authentication
D. Smart card and password authentication

Correct Answer: A
Section:
Explanation:
The combination of authentication mechanisms that is implemented in the above scenario is biometric and password authentication. Biometric authentication is a type of authentication that uses an inherent factor, such as a retina scan, to verify the identity of the user. Password authentication is a type of authentication that uses a knowledge factor, such as a six-digit code, to verify the identity of the user. By combining biometric and password authentication, Finch has implemented a two-factor authentication (2FA) system that requires the user to provide two different types of authentication factors to gain access to the office. 2FA is a more secure way of authentication than using a single factor, as it reduces the risk of unauthorized access due to stolen or compromised credentials. Biometric and password authentication is a common 2FA method that is used in many applications, such as banking, e-commerce, or health care123.

Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-28 to 3-29
What is Biometric Authentication?, Norton, July 29, 2020
What is Two-Factor Authentication (2FA)?, Authy, 2020

QUESTION 20
Identify the UBA tool that collects user activity details from multiple sources and uses artificial intelligence and machine learning algorithms to perform user behavior analysis to prevent and detect various threats before the fraud is perpetrated.

A. Nmap
B. ClamWin
C. Dtex systems
D. Wireshark

Correct Answer: C
Section:
Explanation:
Dtex Systems is the UBA tool that collects user activity details from multiple sources and uses artificial intelligence and machine learning algorithms to perform user behavior analysis to prevent and detect various threats before the fraud is perpetrated. Dtex Systems is a user and entity behavior analytics (UEBA) platform that provides visibility, detection, and response capabilities for insider threats, compromised accounts, data loss, and fraud. Dtex Systems collects user activity data from endpoints, servers, cloud applications, and network traffic, and applies advanced analytics and machine learning to establish baselines of normal user behavior, identify anomalies, and assign risk scores. Dtex Systems also provides contextual information, such as user intent, motivation, and sentiment, to help security teams understand and respond to the threats. Dtex Systems can integrate with other security tools, such as SIEM, DLP, or IAM, to enhance the security posture of the organization123.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-35 to 3-36
Dtex Systems - Wikipedia, Wikipedia, March 16, 2021
Dtex Systems - User and Entity Behavior Analytics (UEBA), Dtex Systems, 2020

QUESTION 21
Below is the list of encryption modes used in a wireless network.
1.WPA2 Enterprise with RADIUS
2.WPA3
3.WPA2 PSK
4.WPA2 Enterprise
Identify the correct order of wireless encryption modes in terms of security from high to low.

A. 2 -- >1 -- >4 -- >3
B. 3 -- >1 -- >4 -- >2
C. 4 -- >2 -- >3 -- >1
D. 4 -- >3 -- >2 -- >1

Correct Answer: A
Section:
Explanation:

Explore

The correct order of wireless encryption modes in terms of security from high to low is 2 -> 1 -> 4 -> 3. This is based on the following comparison of the wireless encryption modes:

WPA3: WPA3 is the latest and most secure wireless encryption mode, introduced in 2018 as a successor to WPA2. WPA3 uses the AES encryption protocol and provides several security enhancements, such as stronger password protection, individualized encryption, forward secrecy, and protection against brute-force and dictionary attacks. WPA3 also supports two modes: WPA3-Personal and WPA3-Enterprise, which offer different levels of security for home and business networks. WPA3-Personal uses Simultaneous Authentication of Equals (SAE) to replace the Pre-Shared Key (PSK) method and provide more robust password-based authentication. WPA3-Enterprise uses 192-bit cryptographic strength to provide additional protection for sensitive data and networks123.

WPA2 Enterprise with RADIUS: WPA2 Enterprise with RADIUS is a wireless encryption mode that combines the security features of WPA2 Enterprise and the authentication features of RADIUS. WPA2 Enterprise is a mode of WPA2 that uses the AES encryption protocol and provides stronger security than WPA2 Personal, which uses the PSK method. WPA2 Enterprise uses the 802.1X standard to implement Extensible Authentication Protocol (EAP) methods, such as EAP-TLS, EAP-TTLS, or PEAP, to authenticate users and devices before granting access to the network. RADIUS is a protocol that allows a central server to manage authentication, authorization, and accounting for network access. RADIUS can integrate with WPA2 Enterprise to provide centralized and scalable authentication for large and complex networks, such as corporate or campus networks .

WPA2 Enterprise: WPA2 Enterprise is a wireless encryption mode that uses the AES encryption protocol and provides stronger security than WPA2 Personal, which uses the PSK method. WPA2 Enterprise uses the 802.1X standard to implement Extensible Authentication Protocol (EAP) methods, such as EAP-TLS, EAP-TTLS, or PEAP, to authenticate users and devices before granting access to the network. WPA2 Enterprise is suitable for business or public networks that require individual and secure authentication for each user or device .

WPA2 PSK: WPA2 PSK is a wireless encryption mode that uses the AES encryption protocol and provides better security than WEP or WPA, which use the TKIP encryption protocol. WPA2 PSK uses the Pre-Shared Key (PSK) method, which means that all users and devices share the same password or passphrase to join the network. WPA2 PSK is easy to set up and use, but it has some security drawbacks, such as being vulnerable to brute-force and dictionary attacks, or having the password compromised by a rogue user or device. WPA2 PSK is suitable for home or small networks that do not require individual authentication or advanced security features .

Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both? - How-To Geek, How-To Geek, March 12, 2023

WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences - NetSpot, NetSpot, February 8, 2024

What is WPA3? And some gotchas to watch out for in this Wi-Fi security upgrade - CSO Online, CSO Online, November 18, 2020

[Types of Wireless Security Encryption - GeeksforGeeks], GeeksforGeeks, 2020

[Wireless Security Protocols: WEP, WPA, and WPA2 - Lifewire], Lifewire, February 17, 2021

[WPA vs. WPA2 vs. WPA3: Wi-Fi Security Explained - MakeUseOf], MakeUseOf, January 13, 2021

QUESTION 22

Which of the following IDS components analyzes the traffic and reports if any suspicious activity is detected?

A. Command console
B. Network sensor
C. Database of attack signatures
D. Response system

Correct Answer: B
Section:
Explanation:
The IDS component that analyzes the traffic and reports if any suspicious activity is detected is the network sensor. A network sensor is a device or software application that is deployed at a strategic point or points within the network to monitor and capture the network traffic to and from all devices on the network. A network sensor can operate in one of two modes: promiscuous or inline. In promiscuous mode, the network sensor passively listens to the network traffic and copies the packets for analysis. In inline mode, the network sensor actively intercepts and filters the network traffic and can block or modify the packets based on predefined rules. A network sensor analyzes the network traffic using various detection methods, such as signature-based, anomaly-based, or reputation-based, and compares the traffic patterns with a database of attack signatures or a model of normal behavior. If the network sensor detects any suspicious or malicious activity, such as a reconnaissance scan, an unauthorized access attempt, or a denial-of-service attack, it generates an alert and reports it to the IDS manager or the operator. A network sensor can also integrate with a response system to take appropriate actions, such as logging, notifying, or blocking, in response to the detected activity123.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-33 to 3-34
Intrusion Detection System (IDS) - GeeksforGeeks, GeeksforGeeks, 2020
Intrusion detection system - Wikipedia, Wikipedia, March 16, 2021

QUESTION 23
Which of the following objects of the container network model (CNM) contains the configuration files of a container's network stack, such as routing table, container's interfaces, and DNS settings?

A. Endpoint
B. Sandbox
C. Network drivers
D. IPAM drivers

Correct Answer: B
Section:
Explanation:
The object of the container network model (CNM) that contains the configuration files of a container's network stack, such as routing table, container's interfaces, and DNS settings, is the Sandbox. A Sandbox is a logical entity that encapsulates the network configuration and state of a container. A Sandbox can contain one or more endpoints from different networks, and provides isolation and security for the container's network stack. A Sandbox can be implemented using various technologies, such as Linux network namespaces, FreeBSD jails, or Windows compartments. A Sandbox allows the container to have its own view and control of the network resources, such as interfaces, addresses, routes, and DNS settings123.
Reference:
The Container Networking Model | Training, Training, 2020
A Comprehensive Guide To Docker Networking - KnowledgeHut, KnowledgeHut, September 27, 2023
Design - GitHub: Let's build from here, GitHub, 2020

QUESTION 24
Mark, a network administrator in an organization, was assigned the task of preventing data from falling into the wrong hands. In this process, Mark implemented authentication techniques and performed full memory encryption for the data stored on RAM.
In which of the following states has Steve encrypted the data in the above scenario?

A. Data in use
B. Data in transit
C. Data inactive
D. Data in rest

Correct Answer: A
Section:
Explanation:
The state in which Mark encrypted the data in the above scenario is data in use. Data in use refers to data that is being processed or manipulated by an application or a system, such as data stored on RAM or CPU registers. Data in use is the most vulnerable state of data, as it is exposed to various threats, such as memory scraping, buffer overflow, or side-channel attacks, that can compromise the confidentiality, integrity, or availability of the

data. Data in use encryption is a technique that protects the data while it is being processed by encrypting it in memory using hardware or software solutions. Data in use encryption prevents unauthorized access or modification of the data, even if the system is compromised or the memory is dumped. Data in use encryption is one of the three types of data encryption, along with data at rest encryption and data in transit encryption123.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-23 to 3-24
Encryption: Data at Rest, Data in Motion and Data in Use, Jatheon, 2020
Data in Use Encryption: What It Is and Why You Need It, Fortanix, 2020

QUESTION 25
Jacob, an attacker, targeted container technology to destroy the reputation of an organization. To achieve this, he initially compromised a single container exploiting weak network defaults, overloaded the rest of the containers in the local domain, and restricted them from providing services to legitimate users.
Identify the type of attack initiated by Jacob in the above scenario.

A. Cross-container attack
B. Docker registry attack
C. Container escaping attack
D. Replay attack

Correct Answer: A
Section:
Explanation:
The type of attack initiated by Jacob in the above scenario is a cross-container attack. A cross-container attack is a type of attack that targets container technology and exploits the shared resources and network connections between containers. A cross-container attack can compromise the security and availability of multiple containers and the underlying host by performing actions such as stealing data, executing commands, consuming resources, or spreading malware. A cross-container attack can be launched by an external attacker who gains access to a container through a network vulnerability, or by a malicious insider who runs a rogue container on the same host or cluster. A cross-container attack can be prevented or mitigated by implementing security best practices for container technology, such as isolating containers, limiting privileges, enforcing policies, scanning images, and monitoring network traffic123.
Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-37 to 3-38
6 Common Kubernetes and Container Attack Techniques and How to Prevent Them - Palo Alto Networks, Palo Alto Networks, March 2, 2022
The evolution of a matrix: How ATT&CK for Containers was built - Microsoft, Microsoft, July 21, 2021

QUESTION 26
Which of the following ISO standards provides guidance to ensure that cloud service providers offer appropriate information security controls to protect the privacy of their customer's clients by securing personally identifiable information entrusted to them?

A. ISO/IEC 27001
B. ISO/IEC 27018
C. ISO/IEC 27011
D. ISO/IEC 27007

Correct Answer: B
Section:
Explanation:
ISO/IEC 27018 is the ISO standard that provides guidance to ensure that cloud service providers offer appropriate information security controls to protect the privacy of their customer's clients by securing personally identifiable information entrusted to them. ISO/IEC 27018 is a code of practice for protecting personal information in cloud storage. The term for the personal data it covers is Personally Identifiable Information or PII. ISO/IEC 27018 is an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. It helps cloud service providers who process PII to assess risk and implement controls for protecting PII. ISO/IEC 27018 was created in 2014 and updated in 2019. It has the following objectives:
Help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract.
Enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services.
Assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement.

Provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a multiparty, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place123.
ISO/IEC 27018: Protecting PII in Public Clouds - ISMS.online, ISMS.online, 2019
ISO/IEC 27018 - Wikipedia, Wikipedia, 2021
ISO/IEC 27018:2019 - Information technology --- Security techniques --- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO, 2019

QUESTION 27
John has recently joined an organization and completed his security training. The organization conducted a security campaign on their employees by sending a fake email stating the urgency of password reset. John identified that it was an illegitimate mail and reported it as spam.
Identify the type of attack initiated by the organization as part of the security campaign discussed in the above scenario.

A. Phishing
B. Tailgating
C. Dumpster diving
D. Shoulder surfing

Correct Answer: A
Section:
Explanation:
The type of attack initiated by the organization as part of the security campaign discussed in the above scenario is phishing. Phishing is a form of fraud where cybercriminals use email, instant messaging, or other social media to try to gather information such as login credentials by masquerading as a reputable person or organization. Phishing occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source, and tries to persuade the recipient to click on a link, open an attachment, or provide personal information. The link or attachment may lead to a fake website or install malware on the recipient's device, while the personal information may be used for identity theft, account takeover, or other malicious purposes. Phishing is one of the most common and effective cyberattacks, as it exploits the human factor and relies on social engineering techniques to manipulate the victim's emotions, such as urgency, fear, or curiosity.Phishing can be prevented or mitigated by educating the users on how to recognize and report phishing emails, using strong and unique passwords, enabling multi-factor authentication, and installing security software123.Reference:
Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-30 to 3-31
20 types of phishing attacks + phishing examples - Norton, Norton, October 03, 2022
Types of Email Attacks - GeeksforGeeks, GeeksforGeeks, May 30, 2023

QUESTION 28
Peter, a network defender, was instructed to protect the corporate network from unauthorized access. To achieve this, he employed a security solution for wireless communication that uses dragonfly key exchange for authentication, which is the strongest encryption algorithm that protects the network from dictionary and key recovery attacks.
Identify the wireless encryption technology implemented in the security solution selected by Peter in the above scenario.

A. WPA
B. WPA3
C. EAP
D. WEP

Correct Answer: B
Section:
Explanation:
WPA3 is the latest standard of Wi-Fi Protected Access, which was released in 2018 by the Wi-Fi Alliance. WPA3 uses a new handshake protocol called Simultaneous Authentication of Equals (SAE), which is based on a zero-knowledge proof known as dragonfly. Dragonfly is a key exchange algorithm that uses discrete logarithm cryptography to derive a shared secret between two parties, without revealing any information about their passwords or keys. Dragonfly is resistant to offline dictionary attacks, where an attacker tries to guess the password by capturing the handshake and testing different combinations. Dragonfly is also resistant to key recovery attacks, where an attacker tries to recover the encryption key by exploiting weaknesses in the algorithm or implementation. Dragonfly provides forward secrecy, which means that even if an attacker manages to compromise the password or key in the future, they cannot decrypt the past communication. WPA3 also supports other features such as increased key sizes, opportunistic wireless encryption, and protected management frames, which enhance the security and privacy of wireless networks.
Reference:

WPA3 Dragonfly Handshake
WPA3 Encryption and Configuration Guide
Dragon Fly - Zero Knowledge Proof
What is SAE (Simultaneous Authentication of Equals)?
Dragonfly - people.scs.carleton.ca

QUESTION 29
Jamie wants to send a confidential file to her friend Alice. For this purpose, they installed an application for securely sharing the file. The application employs an encryption algorithm that uses the same shared secret key for encryption and decryption of data.
Identify the type of cryptography employed by the application used by Alice and Jamie for file sharing.

A. Symmetric cryptography
B. Public-key cryptography
C. RSA cryptosystem
D. Asymmetric cryptography

Correct Answer: A
Section:

QUESTION 30
James was recruited as security personnel in an organization and was instructed to secure the organization's infrastructure from physical threats. To achieve this, James installed CCTV systems near gates, reception, hallways, and workplaces to capture illicit activities inside the premises, identify activities that need attention, collect images as evidence, and aid in an alarm system.
Identify the type of physical security control implemented by James in the above scenario.

A. Video surveillance
B. Fire-fighting systems
C. Lighting system
D. Physical barriers

Correct Answer: A
Section:

QUESTION 31
Below are various authentication techniques.
1.Retina scanner
2.One-time password
3.DNA
4.Voice recognition
Identify the techniques that fall under biometric authentication.

A. 1, 3, and 4
B. 1, 2, and 3
C. 2, 3, and 4
D. 1, 2, and 4

Correct Answer: A
Section:
Explanation:

Biometric authentication is a type of authentication that uses the physical or behavioral characteristics of a person to verify their identity. Biometric authentication is more secure and convenient than other methods such as passwords or tokens, as biometric traits are unique, hard to forge, and easy to use. Some examples of biometric authentication techniques are retina scanner, DNA, and voice recognition. Retina scanner uses a low-intensity light beam to scan the pattern of blood vessels at the back of the eye, which is unique for each individual. DNA uses the genetic code of a person to match their identity, which is the most accurate and reliable biometric technique. Voice recognition uses the sound and pitch of a person's voice to verify their identity, which is influenced by factors such as anatomy, physiology, and psychology. These techniques fall under biometric authentication, as they use the physical or behavioral traits of a person to authenticate them.
Reference:
Biometric Authentication - Week 2: Identification, Authentication, and Authorization
Biometric Authentication: What You Need To Know
Biometric Authentication Techniques

QUESTION 32
Kelly, a cloud administrator at TechSol Inc., was instructed to select a cloud deployment model to secure the corporate data and retain full control over the data.
Which of the following cloud deployment models helps Kelly in the above scenario?

A. Public cloud
B. Multi cloud
C. Community cloud
D. Private cloud

Correct Answer: D
Section:
Explanation:
A private cloud is a cloud deployment model that is exclusively used by a single organization and is hosted either on-premises or off-premises by a third-party provider. A private cloud offers the highest level of security and control over the data and resources, as the organization can customize the cloud infrastructure and services according to its needs and policies. A private cloud also ensures better performance and availability, as the organization does not share the cloud resources with other users. A private cloud is suitable for organizations that have sensitive or confidential data, strict compliance requirements, or high demand for scalability and flexibility. A private cloud can help Kelly secure the corporate data and retain full control over the data in the above scenario.
Reference:
Private Cloud - Week 6: Virtualization and Cloud Computing
Private Cloud vs Public Cloud vs Hybrid Cloud
Private Cloud Security: Challenges and Best Practices

QUESTION 33
Steve was sharing his confidential file with John via an email that was digitally signed and encrypted. The digital signature was made using the 'Diffie-Hellman (X9.42) with DSS' algorithm, and the email was encrypted using triple DES.
Which of the following protocols employs the above features to encrypt an email message?

A. S/MIME
B. EAP
C. RADIUS
D. TACACS+

Correct Answer: A
Section:
Explanation:
S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that provides security services for email messages, such as encryption, digital signature, authentication, and integrity. S/MIME is based on the MIME standard, which defines the format and structure of email messages. S/MIME uses public-key cryptography to encrypt and decrypt the message content and to sign and verify the message sender. S/MIME supports various algorithms for encryption and digital signature, such as Diffie-Hellman, DSS, RSA, and triple DES. S/MIME is widely used for secure email communication in various applications and platforms, such as Outlook, Gmail, and Thunderbird. S/MIME is the protocol that employs the features mentioned in the question, namely Diffie-Hellman (X9.42) with DSS for digital signature and triple DES for encryption.
Reference:

S/MIME - Week 7: Email Security
S/MIME - Wikipedia
S/MIME Version 3.2 Message Specification

QUESTION 34
Joseph, a security professional, was instructed to secure the organization's network. In this process, he began analyzing packet headers to check whether any indications of source and destination IP addresses and port numbers are being changed during transmission.
Identify the attack signature analysis technique performed by Joseph in the above scenario.

A. Composite-signature-based analysis
B. Context-based signature analysis
C. Content-based signature analysis
D. Atomic-signature-based analysis

Correct Answer: D
Section:
Explanation:
Atomic-signature-based analysis is a type of attack signature analysis technique that uses a single characteristic or attribute of a packet header to identify malicious traffic. Atomic signatures are simple and fast to match, but they can also generate false positives or miss some attacks. Some examples of atomic signatures are source and destination IP addresses, port numbers, protocol types, and TCP flags. Atomic-signature-based analysis is the technique performed by Joseph in the above scenario, as he analyzed packet headers to check whether any indications of source and destination IP addresses and port numbers are being changed during transmission.
Reference:
[Understanding the Network Traffic Signatures] - Module 12: Network Traffic Monitoring
Network Defense Essentials (NDE) | Coursera - Week 12: Network Traffic Monitoring
[Network Defense Essentials Module 12 (Network Traffic Monitoring) - Quizlet] - Flashcards: What are Network Traffic Signatures?

QUESTION 35
Kevin logged into a banking application with his registered credentials and tried to transfer some amount from his account to Flora's account. Before transferring the amount to Flora's account, the application sent an OTP to Kevin's mobile for confirmation.
Which of the following authentication mechanisms is employed by the banking application in the above scenario?

A. Biometric authentication
B. Smart card authentication
C. Single sign-on (SSO) authentication
D. Two-factor authentication

Correct Answer: D
Section:
Explanation:
Two-factor authentication (2FA) is a type of authentication that requires users to provide two or more forms of verification to access an online account. 2FA is a multi-layered security measure designed to prevent hackers from accessing user accounts using stolen or shared credentials. 2FA typically combines something the user knows (such as a password or PIN), something the user has (such as a phone or a token), and/or something the user is (such as a fingerprint or a face scan). In the above scenario, the banking application employs 2FA by asking Kevin to enter his registered credentials (something he knows) and an OTP sent to his mobile (something he has) before transferring the amount to Flora's account.
Reference:
Improve Your Cybersecurity with Password MFA - Defense.com
What Is Two-Factor Authentication (2FA)? | Microsoft Security
Selecting Secure Multi-factor Authentication Solutions

QUESTION 36
Messy, a network defender, was hired to secure an organization's internal network. He deployed an IDS in which the detection process depends on observing and comparing the observed events with the normal behavior and

then detecting any deviation from it.
Identify the type of IDS employed by Messy in the above scenario.

A. Signature-based
B. Stateful protocol analysis
C. Anomaly-based
D. Application proxy

Correct Answer: C
Section:
Explanation:
Anomaly-based IDS is a type of IDS that detects intrusions by comparing the observed network events with a baseline of normal behavior and identifying any deviation from it. Anomaly-based IDS can detect unknown or zero-day attacks that do not match any known signature, but they can also generate false positives due to legitimate changes in network behavior. Anomaly-based IDS can use various techniques to model the normal behavior, such as statistical analysis, machine learning, or artificial intelligence. Anomaly-based IDS is the type of IDS employed by Messy in the above scenario, as he deployed an IDS that depends on observing and comparing the observed events with the normal behavior and then detecting any deviation from it.
Reference:
Anomaly-Based Intrusion Detection System - Chapter 2: Anomaly-Based Intrusion Detection System
Network Defense Essentials (NDE) | Coursera - Week 10: Intrusion Detection and Prevention Systems
A systematic literature review for network intrusion detection system (IDS) - Section 3.2: Anomaly-based IDS

QUESTION 37
Joseph, a cloud administrator, was recruited for the management and deployment of the software containers. As part of his job, Joseph employed an automated solution that converts images into containers, deploys them to the hosts, and further monitors container workflow from a single location.
Identify the solution employed by Joseph in the above scenario.

A. Port scanners
B. Orchestrators
C. Network monitors
D. Sniffers

Correct Answer: B
Section:
Explanation:
Orchestrators are tools that automate container deployment, administration, and scaling tasks. They allow you to reliably manage fleets of hundreds or thousands of containers in production environments. Orchestrators simplify container admin by letting you think in terms of application components instead of individual containers. They're able to take control of all your app's requirements, including config values, secrets, and network services. Orchestrators are the solution employed by Joseph in the above scenario, as he used an automated solution that converts images into containers, deploys them to the hosts, and further monitors container workflow from a single location.
Reference:
13 Most Useful Container Orchestration Tools in 2024 - Spacelift
Network Defense Essentials - CERT - EC-Council - Module 6: Virtualization and Cloud Computing

QUESTION 38
Mary was surfing the Internet, and she wanted to hide her details and the content she was surfing over the web. She employed a proxy tool that makes his online activity untraceable.
Identify the type of proxy employed by John in the above scenario.

A. SOCKS proxy
B. Anonymous proxy
C. Reverse proxy

D. Explicit proxy

Correct Answer: B
Section:
Explanation:
anonymous proxy is a type of proxy that hides the user's IP address and other identifying information from the web servers they access. An anonymous proxy acts as an intermediary between the user and the internet, and it modifies the HTTP headers to prevent the web servers from tracking the user's location, browser, or device. An anonymous proxy can help the user bypass geo-restrictions, censorship, and online surveillance. However, an anonymous proxy does not encrypt the user's traffic, and it may still leak some information to the proxy provider or other third parties. An anonymous proxy is the type of proxy employed by Mary in the above scenario, as she used a proxy tool that makes her online activity untraceable.
Reference:
What is a Proxy Server and How Does it Work?
13 Best Proxy Tools for PC [2024 Reviewed] - Section: Anonymous proxies
The Fastest Free Proxy

QUESTION 39
Which of the following actors in the NIST cloud deployment reference architecture acts as an intermediary for providing connectivity and transport services between cloud consumers and providers?

A. Cloud provider
B. Cloud auditor
C. Cloud consumer
D. Cloud carrier

Correct Answer: D
Section:

QUESTION 40
Stella, a mobile user, often ignores the messages received from the manufacturer for updates. One day, she found that files in her device are being replaced, she immediately rushed to the nearest service center for inquiry. They tested the device and identified vulnerabilities in it as it ran with an obsolete OS version.
Identify the mobile device security risk raised on Stella's device in the above scenario.

A. Application-based risk
B. System-based risk
C. Network-based risk
D. Physical security risks

Correct Answer: B
Section:
Explanation:
System-based risk is a type of mobile device security risk that arises from the vulnerabilities or flaws in the operating system or firmware of the device. System-based risk can expose the device to malware, spyware, ransomware, or other malicious attacks that can compromise the data, functionality, or privacy of the device. System-based risk can be mitigated by applying regular security updates and patches from the manufacturer or vendor, as well as using antivirus or anti-malware software. In the above scenario, Stella's device faced a system-based risk, as it ran with an obsolete OS version that had vulnerabilities that allowed the files to be replaced. She ignored the messages from the manufacturer for updates, which could have prevented the risk.
Reference:
Mobile Device Security Risks - Week 8: Mobile Device Security
Is It Safe to Use an Old or Used Phone? Here's What You Should Know
Obsolete products - The National Cyber Security Centre

QUESTION 41
Which of the following protocols uses TLS/SSL to ensure secure transmission of data over the Internet?

A. HTTPS
B. SCTP
C. FTP
D. HTTP

Correct Answer: A
Section:
Explanation:
HTTPS (Hypertext Transfer Protocol Secure) is a protocol that uses TLS/SSL to ensure secure transmission of data over the Internet. HTTPS is an extension of HTTP, which is the standard protocol for transferring data between web servers and browsers. HTTPS encrypts the data exchanged between the client and the server, preventing anyone from intercepting, modifying, or stealing the data. HTTPS also verifies the identity of the server using digital certificates, preventing spoofing or phishing attacks. HTTPS is widely used for web applications that handle sensitive information, such as online banking, e-commerce, or social media.
Reference:
HTTPS - Week 7: Email Security
How does SSL work? | SSL certificates and TLS | Cloudflare
SSL and TLS: A Beginners Guide | SANS Institute

QUESTION 42
Which of the following environmental controls options saves the hardware from humidity and heat, increases hardware performance, and maintains consistent room temperature?

A. Hot and cold aisles
B. Lighting systern
C. Temperature indicator
D. EMI shielding

Correct Answer: A
Section:
Explanation:
Hot and cold aisles are a type of environmental control that saves the hardware from humidity and heat, increases hardware performance, and maintains consistent room temperature. Hot and cold aisles are a layout design for data centers, where the server racks are arranged in alternating rows of cold air intake and hot air exhaust. The cold aisle faces the air conditioner output ducts and provides cool air to the front of the servers. The hot aisle faces the air conditioner return ducts and collects the hot air from the back of the servers. This way, the hot and cold air streams are separated and do not mix, resulting in better cooling efficiency, lower energy consumption, and longer hardware lifespan.
Reference:
Hot and cold aisles - Week 4: Network Security Controls: Physical Controls
Hot and Cold Aisles: The Basics of Data Center Cooling
Hot Aisle vs. Cold Aisle Containment: Which One is Best for Your Data Center?

QUESTION 43
Kevin, a security team member, was instructed to share a policy document with the employees. As it was supposed to be shared within the network, he used a simple algorithm to encrypt the document that just rearranges the same characters to produce the ciphertext.
Identify the type of cipher employed by Kevin in the above scenario.

A. Substitution cipher
B. Streamn cipher
C. Transposition cipher
D. Block cipher

Correct Answer: C

Section:
Explanation:
A transposition cipher is a type of cipher that encrypts a document by rearranging the same characters to produce the ciphertext. A transposition cipher does not change the identity or frequency of the characters, but only their position. A transposition cipher can use various methods to permute the characters, such as writing them in a grid and reading them in a different order, or shifting them along a rail fence pattern. A transposition cipher is a simple and fast algorithm, but it can be easily broken by frequency analysis or anagramming. A transposition cipher is the type of cipher employed by Kevin in the above scenario, as he used a simple algorithm to encrypt the document that just rearranges the same characters to produce the ciphertext.
Reference:
Transposition cipher - Wikipedia
Network Security: Transposition Cipher Techniques - Coding Streets
Network Defense Essentials (NDE) | Coursera - Module 4: Cryptography Techniques
Columnar Transposition Cipher - GeeksforGeeks

QUESTION 44
George, a professional hacker, targeted a bank employee and tried to crack his password while he was attempting to log on to the remote server to perform his regular banking operations. In this process, George used sniffing tools to capture the password pairwise master key (PMK) associated with the handshake authentication process. Then, using the PMK, he gained unauthorized access to the server to perform malicious activities.
Identify the encryption technology on which George performed password cracking.

A. WPA3
B. WPA
C. WPA2
D. WEP

Correct Answer: C
Section:
Explanation:
WPA2 (Wi-Fi Protected Access 2) is an encryption technology that secures wireless networks using the IEEE 802.11i standard. WPA2 uses a four-way handshake to authenticate the client and the access point, and to generate a pairwise transient key (PTK) for encrypting the data. The PTK is derived from the password pairwise master key (PMK), which is a shared secret between the client and the access point. The PMK can be obtained either by using a pre-shared key (PSK) or by using an 802.1X authentication server. In the above scenario, George performed password cracking on WPA2, as he used sniffing tools to capture the PMK associated with the handshake authentication process. Then, using the PMK, he was able to derive the PTK and decrypt the data exchanged between the client and the access point.
Reference:
WPA2 - Wikipedia
How WPA2-PSK encryption works? - Cryptography Stack Exchange
WPA2 Encryption and Configuration Guide - Cisco Meraki Documentation

QUESTION 45
John, from a remote location, was monitoring his bedridden grandfather's health condition at his home. John has placed a smart wearable ECG on his grandfather's wrist so that he can receive alerts to his mobile phone and can keep a track over his grandfather's health condition periodically.
Which of the following types of IoT communication model was demonstrated in the above scenario?

A. Device-to-gateway model
B. Device-to-cloud model
C. Cloud-to-cloud communication model
D. Device-to-device model

Correct Answer: B
Section:
Explanation:
A device-to-cloud model is a type of IoT communication model that connects the IoT devices directly to the cloud platform, where the data is stored, processed, and analyzed. The device-to-cloud model enables remote access, real-time monitoring, and scalability of IoT applications. The device-to-cloud model requires the IoT devices to have internet connectivity and cloud compatibility. In the above scenario, John used a device-to-cloud

model to monitor his grandfather's health condition, as he placed a smart wearable ECG on his grandfather's wrist that sent the data to the cloud platform, where John could access it from his mobile phone and receive alerts periodically.
Reference:
Communication Models in IoT (Internet of Things) - Section: Device-to-Cloud Model
IoT Communication Models - IoTbyHVM - Section: Device to Cloud Communication Model
Logical Design of IoT | Communication Models | APIs | Functional Blocks - Section: Device-to-Cloud Communication Model

QUESTION 46
Which of the following algorithms is an iterated block cipher that works by repeating the defined steps multiple times and has a 128-bit block size, having key sizes of 128, 192, and 256 bits?

A. DSA
B. MD5
C. SHA
D. AES

Correct Answer: D
Section:
Explanation:
AES (Advanced Encryption Standard) is an iterated block cipher that works by repeating the defined steps multiple times and has a 128-bit block size, having key sizes of 128, 192, and 256 bits. AES is a symmetric-key algorithm that encrypts and decrypts data using the same secret key. AES operates on a 4x4 matrix of bytes called the state, which undergoes 10, 12, or 14 rounds of transformation depending on the key size. Each round consists of four steps: sub-bytes, shift-rows, mix-columns, and add-round-key. AES is widely used for securing data in various applications and platforms, such as web browsers, VPNs, wireless networks, and smart grids. AES is the algorithm that matches the description given in the question.
Reference:
AES - Week 4: Cryptography Techniques
Advanced Encryption Standard (AES) - NIST
AES Encryption and Decryption Online Tool - Code Beautify

QUESTION 47
Johana was working on a confidential project on her laptop. After working for long hours, she wanted to have a coffee break. Johana left the system active with the project file open and went for a coffee break. Soon after Johana left the place, Bob accessed Johana's system and modified the project file.
Which of the following security guidelines did Johana fail to comply with?

A. Always log off or lock the system when unattended
B. Do not share your computer user account details
C. Keep different passwords for the OS and frequently used applications
D. Do not keep a common password for all accounts

Correct Answer: A
Section:
Explanation:
One of the most basic and important security guidelines for laptop users is to always log off or lock the system when unattended. This prevents unauthorized access to the system and the data stored on it by anyone who might have physical access to the laptop. Logging off or locking the system requires a password or other authentication method to resume the session, which adds a layer of protection to the laptop. Johana failed to comply with this security guideline, as she left the system active with the project file open and went for a coffee break, allowing Bob to access her system and modify the project file.
Reference:
Ten simple steps for keeping your laptop secure - Step 1: Require a password when logging in
6 Steps to Practice Strong Laptop Security - Step #1: Set complex passwords where it counts
A Practical Guide to Securing Your Windows PC - Section: Lock your computer when you step away

QUESTION 48

Jay, a network administrator, was monitoring traffic flowing through an IDS. Unexpectedly, he received an event triggered as an alarm, although there is no active attack in progress.
Identify the type of IDS alert Jay has received in the above scenario.

A. True negative alert
B. False positive alert
C. True positive alert
D. False negative alert

Correct Answer: B
Section:
Explanation:
A false positive alert is a type of IDS alert that occurs when the IDS mistakenly identifies benign or normal traffic as malicious or suspicious, and triggers an alarm, although there is no active attack in progress. A false positive alert can be caused by various factors, such as misconfigured IDS rules, outdated signatures, network anomalies, or legitimate traffic that resembles attack patterns. A false positive alert can waste the time and resources of the security team, as they have to investigate and verify the alert, and also reduce the trust and confidence in the IDS. A false positive alert can be reduced by tuning and updating the IDS, filtering out irrelevant traffic, and using multiple detection methods. A false positive alert is the type of IDS alert Jay has received in the above scenario, as he received an event triggered as an alarm, although there is no active attack in progress.
Reference:
False Positive Alert - Week 10: Intrusion Detection and Prevention Systems
What is a False Positive in Cybersecurity?
How to Reduce False Positives in Intrusion Detection Systems

QUESTION 49
Fernandez, a computer user, initiated an action to access a file located on a remote server. In this process, his account went through certain security constraints to check for any restrictions on his account with regard to access to the file.
Which of the following terms is referred to as a file in the above scenario?

A. Operation
B. Subject
C. Reference monitor
D. Object

Correct Answer: D
Section:

QUESTION 50
Clark, a security team member of an organization, was instructed to secure the premises from unauthorized entries. In this process, Clark implemented security controls that allow employees to enter the office only after scanning their badges or fingerprints.
Which of the following security controls has Clark implemented in the above scenario?

A. Administrative security controls
B. Technical security controls
C. Physical security controls
D. System access controls

Correct Answer: C
Section:
Explanation:
Physical security controls are security measures that prevent or deter unauthorized physical access to a facility, resource, or information. Physical security controls include locks, doors, gates, fences, guards, cameras, alarms, sensors, biometrics, and badges. Physical security controls protect the network and its components from theft, damage, sabotage, or natural disasters. Clark implemented physical security controls in the above scenario, as he

installed security controls that allow employees to enter the office only after scanning their badges or fingerprints.
Reference:
Understanding the Various Types of Physical Security Controls - Week 4: Network Security Controls: Physical Controls
The Role of Physical Security in Maintaining Network Security
Physical Security: Planning, Measures & Examples + PDF

QUESTION 51
Bob has secretly installed smart CCTV devices (IoT devices) outside his home and wants to access the recorded data from a remote location. These smart CCTV devices send sensed data to an intermediate device that carries out pre-processing of data online before transmitting it to the cloud for storage and analysis. The analyzed data is then sent to Bob for initiating actions.
Identify the component of IoT architecture that collects data from IoT devices and performs data pre-processing.

A. Streaming data processor
B. Gateway
C. Data lakes
D. Machine learning

Correct Answer: B
Section:
Explanation:
A gateway is a component of IoT architecture that collects data from IoT devices and performs data pre-processing. A gateway acts as a bridge between the IoT devices and the cloud platform, and it can filter, aggregate, compress, encrypt, or transform the data before sending it to the cloud for storage and analysis. A gateway can also perform edge computing, which means processing the data locally and providing real-time feedback or actions. A gateway can support various communication protocols, such as WiFi, Bluetooth, Zigbee, or cellular, and it can enhance the security and reliability of the IoT system. A gateway is the component that matches the description given in the question123

QUESTION 52
Clark, a security professional, was instructed to monitor and continue the backup functions without interrupting the system or application services. In this process, Clark implemented a backup mechanism that dynamically backups the data even if the system or application resources are being used.
Which of the following types of backup mechanisms has Clark implemented in the above scenario?

A. Full backup
B. Offline backup
C. Cold backup
D. Hot backup

Correct Answer: D
Section:
Explanation:
A hot backup is a type of backup mechanism that dynamically backs up the data even if the system or application resources are being used. A hot backup does not require the system or application to be shut down or paused during the backup process, and it allows the users to access the data while the backup is in progress. A hot backup ensures that the backup is always up to date and consistent with the current state of the data, and it minimizes the downtime and disruption of the system or application services. A hot backup is suitable for systems or applications that have high availability and performance requirements, such as databases, web servers, or email servers. A hot backup is the type of backup mechanism that Clark implemented in the above scenario, as he performed a backup that dynamically backs up the data even if the system or application resources are being used.
Reference:
Hot Backup - Week 5: Data Security
Hot Backup vs. Cold Backup: What's the Difference?
Network Defense Essentials (NDE) | Coursera - Module 5: Data Security

QUESTION 53
Which of the following techniques is referred to as a messaging feature that originates from a server and enables the delivery of data or a message from an application to a mobile device without any explicit request from the

user?

A. Push notification
B. PIN feature
C. Geofencing
D. Containerization

Correct Answer: A
Section:

QUESTION 54
Bob, a security professional, was recruited by an organization to ensure that application services are being delivered as expected without any delay. To achieve this, Bob decided to maintain different backup servers for the same resources so that if one backup system fails, another will serve the purpose.
Identify the IA principle employed by Bob in the above scenario.

A. Authentication
B. Confidentiality
C. Integrity
D. Availability

Correct Answer: D
Section:

QUESTION 55
Stephen, a security specialist, was instructed to identify emerging threats on the organization's network. In this process, he employed a computer system on the Internet intended to attract and trap those who attempt unauthorized host system utilization to penetrate the organization's network.
Identify the type of security solution employed by Stephen in the above scenario.

A. Firewall
B. Honeypot
C. IDS
D. Proxy server

Correct Answer: B
Section:

QUESTION 56
Carol is a new employee at ApTech Sol Inc., and she has been allocated a laptop to fulfill his job activities.
Carol tried to install certain applications on the company's laptop but could not complete the installation as she requires administrator privileges to initiate the installation process. The administrator imposed an access policy on the company's laptop that only users with administrator privileges have installation rights.
Identify the access control model demonstrated in the above scenario.

A. Rule-based access control {RB-RBAC)
B. Mandatory access control {MAC)
C. Role-based access control (RBAC)
D. Discretionary access control (DAC)

Correct Answer: C
Section:
Explanation:
Role-based access control (RBAC) is a model that assigns permissions and privileges to users based on their roles in an organization. In RBAC, the administrator defines the roles and the access rights for each role, and then assigns users to those roles. This way, the administrator can control the access of users to the resources without having to manage each user individually. In the scenario, Carol is assigned a role that does not have the installation rights, while the administrator has a role that does. Therefore, the access control model demonstrated in the scenario is RBAC.
Reference: Network Defense Essentials - EC-Council Learning, Network Defense Essentials (NDE) | Coursera, EC-Council Network Defense Essentials | NDE Certification