Number: 212-82
Passing Score: 800
Time Limit: 120
File Version: 1.0

Exam Code: 212-82

Website: www.Vdumps.com

Exam A

QUESTION 1
Thomas, an employee of an organization, is restricted to access specific websites from his office system. He is trying to obtain admin credentials to remove the restrictions. While waiting for an opportunity, he sniffed communication between the administrator and an application server to retrieve the admin credentials. Identify the type of attack performed by Thomas in the above scenario.

A. Vishing
B. Eavesdropping
C. Phishing
D. Dumpster diving

Correct Answer: B
Section:

QUESTION 2
Kayden successfully cracked the final round of interview at an organization. After few days, he received his offer letter through an official company email address. The email stated that the selected candidate should respond within a specified time. Kayden accepted the opportunity and provided e-signature on the offer letter, then replied to the same email address. The company validated the e-signature and added his details to their database. Here, Kayden could not deny company's message, and company could not deny Kayden's signature.
Which of the following information security elements was described in the above scenario?

A. Availability
B. Non-repudiation
C. Integrity
D. Confidentiality

Correct Answer: B
Section:

QUESTION 3
Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system.
Which of the following type of accounts the organization has given to Sam in the above scenario?

A. Service account
B. Guest account
C. User account
D. Administrator account

Correct Answer: B
Section:

QUESTION 4
Myles, a security professional at an organization, provided laptops for all the employees to carry out the business processes from remote locations. While installing necessary applications required for the business, Myles has also installed antivirus software on each laptop following the company's policy to detect and protect the machines from external malicious events over the Internet.
Identify the PCI-DSS requirement followed by Myles in the above scenario.

A. PCI-DSS requirement no 1.3.2
B. PCI-DSS requirement no 1.3.5
C. PCI-DSS requirement no 5.1
D. PCI-DSS requirement no 1.3.1

Correct Answer: C
Section:

QUESTION 5
Ashton is working as a security specialist in SoftEight Tech. He was instructed by the management to strengthen the Internet access policy. For this purpose, he implemented a type of Internet access policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage.
Identify the type of Internet access policy implemented by Ashton in the above scenario.

A. Paranoid policy
B. Prudent policy
C. Permissive policy
D. Promiscuous policy

Correct Answer: A
Section:

QUESTION 6
Zion belongs to a category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. He was instructed by the management to check the functionality of equipment related to physical security. Identify the designation of Zion.

A. Supervisor
B. Chief information security officer
C. Guard
D. Safety officer

Correct Answer: C
Section:

QUESTION 7
In an organization, all the servers and database systems are guarded in a sealed room with a single entry point. The entrance is protected with a physical lock system that requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs.
Which of the following types of physical locks is used by the organization in the above scenario?

A. Digital locks
B. Combination locks
C. Mechanical locks
D. Electromagnetic locks

Correct Answer: B
Section:

QUESTION 8
Lorenzo, a security professional in an MNC, was instructed to establish centralized authentication, authorization, and accounting for remote-access servers. For this purpose, he implemented a protocol that is based on the client-server model and works at the transport layer of the OSI model.
Identify the remote authentication protocol employed by Lorenzo in the above scenario.

A. SNMPv3
B. RADIUS
C. POP3S
D. IMAPS

Correct Answer: B
Section:

QUESTION 9
Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate.
Identify the firewall technology implemented by Malachi in the above scenario.

A. Next generation firewall (NGFW)
B. Circuit-level gateways
C. Network address translation (NAT)
D. Packet filtering

Correct Answer: B
Section:

QUESTION 10
Rhett, a security professional at an organization, was instructed to deploy an IDS solution on their corporate network to defend against evolving threats. For this purpose, Rhett selected an IDS solution that first creates models for possible intrusions and then compares these models with incoming events to make detection decisions.
Identify the detection method employed by the IDS solution in the above scenario.

A. Not-use detection
B. Protocol anomaly detection
C. Anomaly detection
D. Signature recognition

Correct Answer: C
Section:

QUESTION 11
Richards, a security specialist at an organization, was monitoring an IDS system. While monitoring, he suddenly received an alert of an ongoing intrusion attempt on the organization's network. He immediately averted the malicious actions by implementing the necessary measures.
Identify the type of alert generated by the IDS system in the above scenario.

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

D. False positive

Correct Answer: A
Section:

QUESTION 12
Karter, a security professional, deployed a honeypot on the organization's network for luring attackers who attempt to breach the network. For this purpose, he configured a type of honeypot that simulates a real OS as well as applications and services of a target network. Furthermore, the honeypot deployed by Karter only responds to preconfigured commands.
Identify the type of Honeypot deployed by Karter in the above scenario.

A. Low-interaction honeypot
B. Pure honeypot
C. Medium-interaction honeypot
D. High-interaction honeypot

Correct Answer: A
Section:

QUESTION 13
An MNC hired Brandon, a network defender, to establish secured VPN communication between the company's remote offices. For this purpose, Brandon employed a VPN topology where all the remote offices communicate with the corporate office but communication between the remote offices is denied.
Identify the VPN topology employed by Brandon in the above scenario.

A. Point-to-Point VPN topology
B. Star topology
C. Hub-and-Spoke VPN topology
D. Full-mesh VPN topology

Correct Answer: C
Section:

QUESTION 14
Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat hunting process using existing data collected from DNS and proxy logs.
Identify the type of threat hunting method employed by Mark in the above scenario.

A. Entity-driven hunting
B. TTP-driven hunting
C. Data-driven hunting
D. Hybrid hunting

Correct Answer: C
Section:

QUESTION 15
An organization hired a network operations center (NOC) team to protect its IT infrastructure from external attacks. The organization utilized a type of threat intelligence to protect its resources from evolving threats. The threat intelligence helped the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors.
Identify the type of threat intelligence consumed by the organization in the above scenario.

A. Operational threat intelligence
B. Strategic threat intelligence
C. Technical threat intelligence
D. Tactical threat intelligence

Correct Answer: C
Section:

QUESTION 16
Tristan, a professional penetration tester, was recruited by an organization to test its network infrastructure. The organization wanted to understand its current security posture and its strength in defending against external threats.
For this purpose, the organization did not provide any information about their IT infrastructure to Tristan. Thus, Tristan initiated zero-knowledge attacks, with no information or assistance from the organization.
Which of the following types of penetration testing has Tristan initiated in the above scenario?

A. Black-box testing
B. White-box testing
C. Gray-box testing
D. Translucent-box testing

Correct Answer: A
Section:

QUESTION 17
Miguel, a professional hacker, targeted an organization to gain illegitimate access to its critical information. He identified a flaw in the end-point communication that can disclose the target application's dat a.Which of the following secure application design principles was not met by the application in the above scenario?

A. Secure the weakest link
B. Do not trust user input
C. Exception handling
D. Fault tolerance

Correct Answer: C
Section:

QUESTION 18
A software company is developing a new software product by following the best practices for secure application development. Dawson, a software analyst, is checking the performance of the application on the client's network to determine whether end users are facing any issues in accessing the application.
Which of the following tiers of a secure application development lifecycle involves checking the performance of the application?

A. Development
B. Testing
C. Quality assurance (QA)
D. Staging

Correct Answer: B
Section:

QUESTION 19
Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment.
The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.
Which of the following virtualization approaches has Nicolas adopted in the above scenario?

A. Hardware-assisted virtualization
B. Full virtualization
C. Hybrid virtualization
D. OS-assisted virtualization

Correct Answer: B
Section:

QUESTION 20
Walker, a security team member at an organization, was instructed to check if a deployed cloud service is working as expected. He performed an independent examination of cloud service controls to verify adherence to standards through a review of objective evidence. Further, Walker evaluated the services provided by the CSP regarding security controls, privacy impact, and performance.
Identify the role played by Walker in the above scenario.

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

Correct Answer: A
Section:

QUESTION 21
A software company has implemented a wireless technology to track the employees' attendance by recording their in and out timings. Each employee in the company will have an entry card that is embedded with a tag. Whenever an employee enters the office premises, he/she is required to swipe the card at the entrance. The wireless technology uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects.
Which of the following technologies has the software company implemented in the above scenario?

A. WiMAX
B. RFID
C. Bluetooth
D. Wi-Fi

Correct Answer: B
Section:

QUESTION 22
Matias, a network security administrator at an organization, was tasked with the implementation of secure wireless network encryption for their network. For this purpose, Matias employed a security solution that uses 256-bit
Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of dat a.
Identify the type of wireless encryption used by the security solution employed by Matias in the above scenario.

A. WPA2 encryption

B. WPA3 encryption
C. WEP encryption
D. WPA encryption

Correct Answer: B
Section:

QUESTION 23
Rickson, a security professional at an organization, was instructed to establish short-range communication between devices within a range of 10 cm. For this purpose, he used a mobile connection method that employs electromagnetic induction to enable communication between devices. The mobile connection method selected by Rickson can also read RFID tags and establish Bluetooth connections with nearby devices to exchange information such as images and contact lists.
Which of the following mobile connection methods has Rickson used in above scenario?

A. NFC
B. Satcom
C. Cellular communication
D. ANT

Correct Answer: A
Section:

QUESTION 24
Stephen, a security professional at an organization, was instructed to implement security measures that prevent corporate data leakage on employees' mobile devices. For this purpose, he employed a technique using which all personal and corporate data are isolated on an employee's mobile device.
Using this technique, corporate applications do not have any control of or communication with the private applications or data of the employees.
Which of the following techniques has Stephen implemented in the above scenario?

A. Full device encryption
B. Geofencing
C. Containerization
D. OTA updates

Correct Answer: C
Section:

QUESTION 25
Leo has walked to the nearest supermarket to purchase grocery. At the billing section, the billing executive scanned each product's machine-readable tag against a readable machine that automatically reads the product details, displays the prices of the individual product on the computer, and calculates the sum of those scanned items. Upon completion of scanning all the products, Leo has to pay the bill.
Identify the type of short-range wireless communication technology that the billing executive has used in the above scenario.

A. Radio-frequency identification (RFID)
B. Near-field communication (NFC)
C. QUIC
D. QR codes and barcodes

Correct Answer: A
Section:

QUESTION 26
Hayes, a security professional, was tasked with the implementation of security controls for an industrial network at the Purdue level 3.5 (IDMZ). Hayes verified all the possible attack vectors on the IDMZ level and deployed a security control that fortifies the IDMZ against cyber-attacks.
Identify the security control implemented by Hayes in the above scenario.

A. Point-to-point communication
B. MAC authentication
C. Anti-DoS solution
D. Use of authorized RTU and PLC commands

Correct Answer: D
Section:

QUESTION 27
Paul, a computer user, has shared information with his colleague using an online application. The online application used by Paul has been incorporated with the latest encryption mechanism. This mechanism encrypts data by using a sequence of photons that have a spinning trait while traveling from one end to another, and these photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash.
Identify the encryption mechanism demonstrated in the above scenario.

A. Quantum cryptography
B. Homomorphic encryption
C. Rivest Shamir Adleman encryption
D. Elliptic curve cryptography

Correct Answer: A
Section:

QUESTION 28
Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit.
Which of the following keys did Louis use to verify the digital signature in the above scenario?

A. Riley's public key
B. Louis's public key
C. Riley's private key
D. Louis's private key

Correct Answer: A
Section:

QUESTION 29
Grace, an online shopping freak, has purchased a smart TV using her debit card. During online payment, Grace's browser redirected her from ecommerce website to a third-party payment gateway, where she provided her debit card details and OTP received on her registered mobile phone. After completing the transaction, Grace navigated to her online bank account and verified the current balance in her savings account.
Identify the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario.

A. Data at rest
B. Data in inactive

C. Data in transit
D. Data in use

Correct Answer: C
Section:

QUESTION 30
Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).
Which of the following techniques was employed by Andre in the above scenario?

A. Tokenization
B. Masking
C. Hashing
D. Bucketing

Correct Answer: B
Section:

QUESTION 31
Ryleigh, a system administrator, was instructed to perform a full back up of organizational data on a regular basis. For this purpose, she used a backup technique on a fixed date when the employees are not accessing the system i.e., when a service-level down time is allowed a full backup is taken.
Identify the backup technique utilized by Ryleigh in the above scenario.

A. Nearline backup
B. Cold backup
C. Hot backup
D. Warm backup

Correct Answer: B
Section:

QUESTION 32
Jaden, a network administrator at an organization, used the ping command to check the status of a system connected to the organization's network. He received an ICMP error message stating that the IP header field contains invalid information. Jaden examined the ICMP packet and identified that it is an IP parameter problem.
Identify the type of ICMP error message received by Jaden in the above scenario.

A. Type =12
B. Type = 8
C. Type = 5
D. Type = 3

Correct Answer: C
Section:

QUESTION 33
Steve, a network engineer, was tasked with troubleshooting a network issue that is causing unexpected packet drops. For this purpose, he employed a network troubleshooting utility to capture the ICMP echo request packets sent to the server. He identified that certain packets are dropped at the gateway due to poor network connection.

Identify the network troubleshooting utility employed by Steve in the above scenario.

A. dnsenurn
B. arp
C. traceroute
D. ipconfig

Correct Answer: C
Section:

QUESTION 34
Anderson, a security engineer, was Instructed to monitor all incoming and outgoing traffic on the organization's network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.
Identify the type of attack signature analysis performed by Anderson in the above scenario.

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

Correct Answer: D
Section:

QUESTION 35
Leilani, a network specialist at an organization, employed Wireshark for observing network traffic.
Leilani navigated to the Wireshark menu icon that contains items to manipulate, display and apply filters, enable, or disable the dissection of protocols, and configure user-specified decodes.
Identify the Wireshark menu Leilani has navigated in the above scenario.

A. Statistics
B. Capture
C. Main toolbar
D. Analyze

Correct Answer: B
Section:

QUESTION 36
Tenda, a network specialist at an organization, was examining logged data using Windows Event Viewer to identify attempted or successful unauthorized activities. The logs analyzed by Tenda include events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies.
Identify the type of event logs analyzed by Tenda in the above scenario.

A. Application event log
B. Setup event log
C. Security event log
D. System event log

Correct Answer: C

Section:

QUESTION 37
Nancy, a security specialist, was instructed to identify issues related to unexpected shutdown and restarts on a Linux machine. To identify the incident cause, Nancy navigated to a directory on the Linux system and accessed a log file to troubleshoot problems related to improper shutdowns and unplanned restarts.
Identify the Linux log file accessed by Nancy in the above scenario.

A. /var/log/secure
B. /var/log/kern.log
C. /var/log/boot.log
D. /var/log/lighttpd/

Correct Answer: C
Section:

QUESTION 38
Warren, a member of IH&R team at an organization, was tasked with handling a malware attack launched on one of servers connected to the organization's network. He immediately implemented appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization.
Identify the IH&R step performed by Warren in the above scenario.

A. Containment
B. Recovery
C. Eradication
D. Incident triage

Correct Answer: A
Section:

QUESTION 39
The IH&R team in an organization was handling a recent malware attack on one of the hosts connected to the organization's network. Edwin, a member of the IH&R team, was involved in reinstating lost data from the backup medi a.
Before performing this step, Edwin ensured that the backup does not have any traces of malware.
Identify the IH&R step performed by Edwin in the above scenario.

A. Eradication
B. Incident containment
C. Notification
D. Recovery

Correct Answer: D
Section:

QUESTION 40
Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.
Which of the following rules of evidence was discussed in the above scenario?

A. Authentic

B. Understandable
C. Reliable
D. Admissible

Correct Answer: D
Section:

QUESTION 41
Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.
In which of the following sections of the forensic investigation report did Arabella record the "nature of the claim and information provided to the officers"?

A. Investigation process
B. Investigation objectives
C. Evidence information
D. Evaluation and analysis process

Correct Answer: C
Section:

QUESTION 42
Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.
Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

A. Never record the screen display of the device
B. Turn the device ON if it is OFF
C. Do not leave the device as it is if it is ON
D. Make sure that the device is charged

Correct Answer: B, C, D
Section:

QUESTION 43
Ruben, a crime investigator, wants to retrieve all the deleted files and folders in the suspected media without affecting the original files. For this purpose, he uses a method that involves the creation of a cloned copy of the entire media and prevents the contamination of the original medi a.
Identify the method utilized by Ruben in the above scenario.

A. Sparse acquisition
B. Bit-stream imaging
C. Drive decryption
D. Logical acquisition

Correct Answer: B
Section:

QUESTION 44

Kasen, a cybersecurity specialist at an organization, was working with the business continuity and disaster recovery team. The team initiated various business continuity and discovery activities in the organization. In this process, Kasen established a program to restore both the disaster site and the damaged materials to the pre-disaster levels during an incident.
Which of the following business continuity and disaster recovery activities did Kasen perform in the above scenario?

A. Prevention
B. Resumption
C. Response
D. Recovery

Correct Answer: D
Section:

QUESTION 45
Cassius, a security professional, works for the risk management team in an organization. The team is responsible for performing various activities involved in the risk management process. In this process, Cassius was instructed to select and implement appropriate controls on the identified risks in order to address the risks based on their severity level.
Which of the following risk management phases was Cassius instructed to perform in the above scenario?

A. Risk analysis
B. Risk treatment
C. Risk prioritization
D. Risk identification

Correct Answer: B
Section:

QUESTION 46
RAT has been setup in one of the machines connected to the network to steal the important Sensitive corporate docs located on Desktop of the server, further investigation revealed the IP address of the server 20.20.10.26. Initiate a remote connection using thief client and determine the number of files present in the folder.
Hint: Thief folder is located at: Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

A. 2
B. 4
C. 3
D. 5

Correct Answer: C
Section:

QUESTION 47
An FTP server has been hosted in one of the machines in the network. Using Cain and Abel the attacker was able to poison the machine and fetch the FTP credentials used by the admin. You're given a task to validate the credentials that were stolen using Cain and Abel and read the file flag.txt

A. white@hat
B. red@hat
C. hat@red
D. blue@hat

Correct Answer: C
Section:

QUESTION 48
An attacker with malicious intent used SYN flooding technique to disrupt the network and gain advantage over the network to bypass the Firewall. You are working with a security architect to design security standards and plan for your organization. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Study the Synflood.pcapng file and determine the source IP address.
Note: Synflood.pcapng file is present in the Documents folder of Attacker-1 machine.

A. 20.20.10.180
B. 20.20.10.19
C. 20.20.10.60
D. 20.20.10.59

Correct Answer: B
Section:

QUESTION 49
A web application www.movieabc.com was found to be prone to SQL injection attack. You are given a task to exploit the web application and fetch the user credentials. Select the UID which is mapped to user john in the database table.
Note:
Username: sam
Pass: test

A. 5
B. 3
C. 2
D. 4

Correct Answer: D
Section:

QUESTION 50
A pfSense firewall has been configured to block a web application www.abchacker.com. Perform an analysis on the rules set by the admin and select the protocol which has been used to apply the rule.
Hint: Firewall login credentials are given below:
Username: admin
Password: admin@l23

A. POP3
B. TCP/UDP
C. FTP
D. ARP

Correct Answer: B
Section:

QUESTION 51
You are Harris working for a web development company. You have been assigned to perform a task for vulnerability assessment on the given IP address 20.20.10.26. Select the vulnerability that may affect the website according to the severity factor.
Hint: Greenbone web credentials: admin/password

A. TCP timestamps
B. Anonymous FTP Login Reporting
C. FTP Unencrypted Cleartext Login
D. UDP timestamps

Correct Answer: C
Section:

QUESTION 52
A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with http://securityabc.s21sec.com.

A. 5.9.200.200
B. 5.9.200.150
C. 5.9.110.120
D. 5.9.188.148

Correct Answer: D
Section:

QUESTION 53
An IoT device that has been placed in a hospital for safety measures, it has sent an alert command to the server. The network traffic has been captured and stored in the Documents folder of the Attacker Machine-1. Analyze the loTdeviceTraffic.pcapng file and select the appropriate command that was sent by the loT device over the network.

A. Tempe_Low
B. Low_Tempe
C. Temp_High
D. High_Tempe

Correct Answer: C
Section:

QUESTION 54
A text file containing sensitive information about the organization has been leaked and modified to bring down the reputation of the organization. As a safety measure, the organization did contain the MD5 hash of the original file. The file which has been leaked is retained for examining the integrity. A file named "Sensitiveinfo.txt" along with OriginalFileHash.txt has been stored in a folder named Hash in Documents of Attacker Machine-1. Compare the hash value of the original file with the leaked file and state whether the file has been modified or not by selecting yes or no.

A. No
B. Yes

Correct Answer: B
Section:

QUESTION 55
Initiate an SSH Connection to a machine that has SSH enabled in the network. After connecting to the machine find the file flag.txt and choose the content hidden in the file. Credentials for SSH login are provided below:
Hint:
Username: sam

Password: admin@l23

A. sam@bob
B. bob2@sam
C. bob@sam
D. sam2@bob

Correct Answer: C
Section:

QUESTION 56
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

A. Quid pro quo
B. Diversion theft
C. Elicitation
D. Phishing

Correct Answer: A
Section:

QUESTION 57
You are a penetration tester working to test the user awareness of the employees of the client xyz.
You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

A. Reconnaissance
B. Command and control
C. Weaponization
D. Exploitation

Correct Answer: C
Section:

QUESTION 58
Bob was recently hired by a medical company after it experienced a major cyber security breach.
Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those dat a.
Which of the following regulations is mostly violated?

A. HIPPA/PHl
B. Pll
C. PCIDSS
D. ISO 2002

Correct Answer: A

Section:

QUESTION 59
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64
B. 128
C. 255
D. 138

Correct Answer: B
Section:

QUESTION 60
Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Desynchronization
B. Obfuscating
C. Session splicing
D. Urgency flag

Correct Answer: B
Section:
Explanation: