



## **EC-Council**

### **Exam Questions 212-82**

Certified Cybersecurity Technician(C|CT)

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

A software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client's network to determine any issue faced by end users while accessing the application. Which of the following tiers of the secure application development lifecycle involves checking the application performance?

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

**Answer: C**

#### Explanation:

Testing is the tier of the secure application development lifecycle that involves checking the application performance in the above scenario. Secure application development is a process that involves designing, developing, deploying, and maintaining software applications that are secure and resilient to threats and attacks. Secure application development can be based on various models or frameworks, such as SDLC (Software Development Life Cycle), OWASP (Open Web Application Security Project), etc. Secure application development consists of various tiers or stages that perform different tasks or roles. Testing is a tier of the secure application development lifecycle that involves verifying and validating the functionality and security of software applications before releasing them to end users. Testing can include various types of tests, such as unit testing, integration testing, system testing, performance testing, security testing, etc. Testing can be used to check the application performance and identify any errors, bugs, or vulnerabilities in the software applications. In the scenario, a software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client's network to determine any issue faced by end users while accessing the application. This means that he performs testing for this purpose. Development is a tier of the secure application development lifecycle that involves creating and coding software applications according to the design and specifications. Staging is a tier of the secure application development lifecycle that involves deploying software applications to a simulated or pre-production environment for testing or evaluation purposes. Quality assurance (QA) is a tier of the secure application development lifecycle that involves ensuring that software applications meet the quality standards and expectations of end users and stakeholders.

#### NEW QUESTION 2

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

**Answer: D**

#### Explanation:

Content-based signature analysis is the type of attack signature analysis performed by Anderson in the above scenario. Content-based signature analysis is a technique that analyzes packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit. Content-based signature analysis can help detect attacks that manipulate packet headers to evade detection or exploit vulnerabilities. Context-based signature analysis is a technique that analyzes packet payloads such as application data or commands to check whether they match any known attack patterns or signatures. Atomic-signature-based analysis is a technique that analyzes individual packets to check whether they match any known attack patterns or signatures. Composite-signature-based analysis is a technique that analyzes multiple packets or sessions to check whether they match any known attack patterns or signatures.

#### NEW QUESTION 3

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

**Answer: B**

#### Explanation:

Cold backup is the backup technique utilized by Ryleigh in the above scenario. Cold backup is a backup technique that involves taking a full backup of data when the system or database is offline or shut down. Cold backup ensures that the data is consistent and not corrupted by any ongoing transactions or operations. Cold backup is usually performed on a fixed date or time when the service-level downtime is allowed or scheduled. Nearline backup is a backup technique that involves storing data on a medium that is not immediately accessible, but can be retrieved within a short time. Hot backup is a backup technique that involves taking a backup of data while the system or database is online or running. Warm backup is a backup technique that involves taking a backup of data while the system or database is partially online or running.

#### NEW QUESTION 4

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

**Answer:** C

**Explanation:**

Anomaly detection is a type of IDS detection method that involves first creating models for possible intrusions and then comparing these models with incoming events to make a detection decision. It can detect unknown or zero-day attacks by looking for deviations from normal or expected behavior

**NEW QUESTION 5**

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

**Answer:** C

**Explanation:**

Data in transit is the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario. Data in transit is data that is moving from one location to another over a network, such as the internet, a LAN, or a WAN. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties, so it needs to be protected by encryption, authentication, and other security measures. Data at rest is data that is stored on a device or a media, such as a hard drive, a flash drive, or a cloud storage. Data in active is data that is currently being accessed or modified by an application or a user. Data in use is data that is loaded into the memory of a device or a system for processing or computation.

**NEW QUESTION 6**

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

**Answer:** C

**Explanation:**

Security event log is the type of event log analyzed by Tenda in the above scenario. Windows Event Viewer is a tool that displays logged data about various events that occur on a Windows system or network. Windows Event Viewer categorizes event logs into different types based on their source and purpose. Security event log is the type of event log that records events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies. Security event log can help identify attempted or successful unauthorized activities on a Windows system or network. Application event log is the type of event log that records events related to applications running on a Windows system, such as errors, warnings, or information messages. Setup event log is the type of event log that records events related to the installation or removal of software or hardware components on a Windows system. System event log is the type of event log that records events related to the operation of a Windows system or its components, such as drivers, services, processes, etc.

**NEW QUESTION 7**

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 IoTdeviceTraffic.pcapng file and select the appropriate command that was sent by the IoT device over the network.

- A. Tempe\_Low
- B. Low\_Tempe
- C. Temp\_High
- D. High\_Tempe

**Answer:** C

**Explanation:**

Temp\_High is the command that was sent by the IoT device over the network in the above scenario. An IoT (Internet of Things) device is a device that can connect to the internet and communicate with other devices or systems over a network. An IoT device can send or receive commands or data for various purposes, such as monitoring, controlling, or automating processes. To analyze the IoT device traffic file and determine the command that was sent by the IoT device over the network, one has to follow these steps:

- ? Navigate to the Documents folder of Attacker-1 machine.
- ? Double-click on IoTdeviceTraffic.pcapng file to open it with Wireshark.
- ? Click on Analyze menu and select Display Filters option.
- ? Enter `udp.port == 5000` as filter expression and click on Apply button.
- ? Observe the packets filtered by the expression.
- ? Click on packet number 4 and expand User Datagram Protocol section in packet details pane.
- ? Observe the data field under User Datagram Protocol section.

The data field under User Datagram Protocol section is `54:65:6d:70:5f:48:69:67:68`, which is hexadecimal representation of Temp\_High, which is the command that was sent by the IoT device over the network.

#### NEW QUESTION 8

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

**Answer: B**

#### Explanation:

128 is the TTL value that Henry obtained, which indicates that the target OS is Windows. TTL (Time to Live) is a field in the IP (Internet Protocol) header that specifies how long a packet can remain in a network before it is discarded or dropped. TTL is usually expressed in seconds or hops (the number of routers or gateways that a packet passes through). TTL is used to prevent packets from looping endlessly in a network or consuming network resources. Different operating systems have different default TTL values for their packets. By observing the TTL value of a packet from a target system or network, one can infer the operating system of the target. Some common TTL values and their corresponding operating systems are:

? 64: Linux, Unix, Android

? 128: Windows

? 255: Cisco IOS

? 60: Mac OS

In the scenario, Henry used Nmap tool to discover the OS of the target system. Nmap (Network Mapper) is a tool that can perform various network scanning and enumeration tasks, such as port scanning, OS detection, service identification, etc. Nmap can use various techniques to detect the OS of a target system, such as TCP/IP fingerprinting, which involves analyzing various TCP/IP characteristics of packets from the target system, such as TTL value. In the scenario, Henry obtained a TTL value of 128, which indicates that the target OS is Windows.

#### NEW QUESTION 9

Juan, a safety officer at an organization, installed a physical lock at the entrance of each floor. All employees in the organization were allotted a smart card embedded in their ID cards, which had to be swiped to unlock doors and Access any floor. Which of the following types of physical locks did Juan install In this scenario?

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

**Answer: B**

#### Explanation:

Digital locks are the types of physical locks that Juan installed in this scenario. A physical lock is a device that prevents or restricts access to a physical location or environment, such as a door, a cabinet, a drawer, etc. A physical lock can have different types based on its mechanism or technology. A digital lock is a type of physical lock that uses electronic or digital components, such as a keypad, a card reader, a fingerprint scanner, etc., to unlock or lock. A digital lock can be used to provide enhanced security and convenience to users, but it can also be vulnerable to hacking or tampering. In the scenario, Juan installed a physical lock at the entrance of each floor. All employees in the organization were allotted a smart card embedded in their ID cards, which had to be swiped to unlock doors and access any floor. This means that he installed digital locks for those doors. A mechanical lock is a type of physical lock that uses mechanical components, such as a key, a bolt, a latch, etc., to unlock or lock. A combination lock is a type of physical lock that uses a sequence of numbers or symbols, such as a dial, a wheel, or a keypad, to unlock or lock. An electromagnetic lock is a type of physical lock that uses an electromagnet and an armature plate to unlock or lock.

#### NEW QUESTION 10

The incident handling and response (IH&R) team of an organization was handling a recent cyberattack on the organization's web server. Fernando, a member of the IH&P team, was tasked with eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. For this purpose, Fernando applied the latest patches to the web server and installed the latest security mechanisms on it. Identify the IH&R step performed by Fernando in this scenario.

- A. Notification
- B. Containment
- C. Recovery
- D. Eradication

**Answer: D**

#### Explanation:

Eradication is the IH&R step performed by Fernando in this scenario. Eradication is a step in IH&R that involves eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. Eradication can include applying patches, installing security mechanisms, removing malware, restoring backups, or reformatting systems.

References: [Eradication Step in IH&R]

#### NEW QUESTION 10

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

**Answer: D**

**Explanation:**

The use of authorized RTU and PLC commands is the security control implemented by Hayes in the above scenario. RTU (Remote Terminal Unit) and PLC (Programmable Logic Controller) are devices that control and monitor industrial processes, such as power generation, water treatment, oil and gas production, etc. RTU and PLC commands are instructions that are sent from a master station to a slave station to perform certain actions or request certain data. The use of authorized RTU and PLC commands is a security control that fortifies the IDMZ (Industrial Demilitarized Zone) against cyber-attacks by ensuring that only valid and authenticated commands are executed by the RTU and PLC devices. Point-to-point communication is a communication method that establishes a direct connection between two endpoints. MAC authentication is an authentication method that verifies the MAC (Media Access Control) address of a device before granting access to a network. Anti-DoS solution is a security solution that protects a network from DoS (Denial-of-Service) attacks by filtering or blocking malicious traffic.

**NEW QUESTION 14**

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/

**Answer: C**

**Explanation:**

/var/log/boot.log is the Linux log file accessed by Nancy in the above scenario. Linux is an open-source operating system that logs various events and activities on the system or network. Linux log files are stored in the /var/log directory, which contains different types of log files for different purposes. /var/log/boot.log is the type of log file that records events related to the booting process of the Linux system, such as loading drivers, services, modules, etc. /var/log/boot.log can help identify issues related to unexpected shutdowns and restarts on a Linux machine. /var/log/secure is the type of log file that records events related to security and authentication, such as logins, logouts, password changes, sudo commands, etc. /var/log/kern.log is the type of log file that records events related to the kernel, such as kernel messages, errors, warnings, etc. /var/log/lighttpd/ is the directory that contains log files related to the lighttpd web server, such as access logs, error logs, etc.

**NEW QUESTION 17**

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

**Answer: C**

**Explanation:**

Weaponization is the stage of the cyber kill chain that you are at in the above scenario. The cyber kill chain is a model that describes the phases of a cyberattack from the perspective of the attacker. The cyber kill chain consists of seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Reconnaissance is the stage of the cyber kill chain that involves gathering information about the target, such as IP addresses, domain names, vulnerabilities, etc. Weaponization is the stage of the cyber kill chain that involves creating a malicious payload or tool that can exploit the target's vulnerabilities. Weaponization can include creating a client-side backdoor to send it to the employees via email. Delivery is the stage of the cyber kill chain that involves transmitting or delivering the weaponized payload or tool to the target's system or network. Exploitation is the stage of the cyber kill chain that involves executing or triggering the weaponized payload or tool on the target's system or network.

**NEW QUESTION 20**

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

**Answer: A**

**Explanation:**

Radio-frequency identification (RFID) is the type of short-range wireless communication technology that the billing executive has used in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. RFID tags are machine-readable tags that store information about the products, such as name, price, expiry date, etc. RFID readers are readable machines that scan the RFID tags and display the product details on the computer. RFID technology is widely used in supermarkets, warehouses, libraries, and other places where inventory management and tracking are required.

**NEW QUESTION 24**

Kayden successfully cracked the final round of interviews at an organization. After a 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 an 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 the company's message, and the 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

**Answer:** B

**Explanation:**

The correct answer is B, as it describes the information security element that was described in the above scenario. Non-repudiation is an information security element that ensures that a party cannot deny sending or receiving a message or performing an action. In the above scenario, non-repudiation was described, as Kayden could not deny company's message, and company could not deny Kayden's signature. Option A is incorrect, as it does not describe the information security element that was described in the above scenario. Availability is an information security element that ensures that authorized users can access and use information and resources when needed. In the above scenario, availability was not described, as there was no mention of access or use of information and resources. Option C is incorrect, as it does not describe the information security element that was described in the above scenario. Integrity is an information security element that ensures that information and resources are accurate and complete and have not been modified by unauthorized parties. In the above scenario, integrity was not described, as there was no mention of accuracy or completeness of information and resources. Option D is incorrect, as it does not describe the information security element that was described in the above scenario. Confidentiality is an information security element that ensures that information and resources are protected from unauthorized access and disclosure. In the above scenario, confidentiality was not described, as there was no mention of protection or disclosure of information and resources.

References: , Section 3.1

**NEW QUESTION 28**

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

**Answer:** B

**Explanation:**

A circuit-level gateway is a type of 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. It does not inspect the contents of each packet, but rather relies on the session information to filter traffic

**NEW QUESTION 32**

Desmond, a forensic officer, was investigating a compromised machine involved in various online attacks. For this purpose. Desmond employed a forensic tool to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine. Identify the computer-created evidence retrieved by Desmond in this scenario.

- A. Cookies
- B. Documents
- C. Address books
- D. Compressed files

**Answer:** A

**Explanation:**

Cookies are the computer-created evidence retrieved by Desmond in this scenario. Cookies are small files that are stored on a user's computer by a web browser when the user visits a website. Cookies can contain information such as user preferences, login details, browsing history, or tracking data. Cookies can be used to extract and analyze computer-based evidence to retrieve information related to websites accessed from the victim machine<sup>2</sup>. References: Cookies

**NEW QUESTION 36**

Wilson, a security specialist in an organization, was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. Identify the method used by Wilson to achieve cloud network security in this scenario.

- A. Virtual private cloud (VPC)
- B. Public and private subnets
- C. Transit gateways
- D. VPC endpoint

**Answer:** C

**Explanation:**

Transit gateways are the method used by Wilson to achieve cloud network security in this scenario. Cloud network security is a branch of cybersecurity that focuses on protecting and securing the network infrastructure and traffic in a cloud environment. Cloud network security can involve various methods or techniques, such as encryption, firewall, VPN, IDS/IPS, etc. Transit gateways are a method of cloud network security that provide a network routing solution that establishes and manages communication between on-premises consumer networks and VPCs (Virtual Private Clouds) via a centralized unit . Transit gateways can be used to simplify and secure the connectivity between different networks or VPCs in a cloud environment . In the scenario, Wilson was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. This means that he used transit gateways for this purpose. A virtual private cloud (VPC) is not a method of cloud network security, but a term that describes an isolated and private section of a public cloud that provides exclusive access to cloud resources to a single organization or entity . A VPC can be used to create and configure virtual networks in a cloud environment . Public and private subnets are not methods of cloud network security, but terms that describe segments of a VPC that have different levels of accessibility or visibility . A public subnet is a segment of a VPC that can be accessed from the internet or other networks . A private subnet is a segment of a VPC that cannot be accessed from the internet or other networks . A VPC endpoint is not a method of cloud network security, but a term that describes an interface that allows private connectivity between a VPC and other AWS (Amazon Web Services) services or resources.

#### NEW QUESTION 38

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

**Answer:** C

#### Explanation:

Technical threat intelligence is a type of threat intelligence that provides information about the technical details of specific attacks, such as indicators of compromise (IOCs), malware signatures, attack vectors, and vulnerabilities. Technical threat intelligence helps 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. Technical threat intelligence is often consumed by security analysts, incident responders, and penetration testers who need to analyze and respond to active or potential threats.

#### NEW QUESTION 39

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

**Answer:** A

#### Explanation:

A true positive alert is generated by an IDS system when it correctly identifies an ongoing intrusion attempt on the network and sends an alert to the security professional. This is the desired outcome of an IDS system, as it indicates that the system is working effectively and accurately.

#### NEW QUESTION 40

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

**Answer:** B

#### Explanation:

Risk treatment is the risk management phase that Cassius was instructed to perform in the above scenario. Risk management is a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that can affect an organization's objectives, assets, or operations. Risk management phases can be summarized as follows: risk identification, risk analysis, risk prioritization, risk treatment, and risk monitoring. Risk identification is the risk management phase that involves identifying and documenting potential sources, causes, events, and impacts of risks. Risk analysis is the risk management phase that involves assessing and quantifying the likelihood and consequences of risks. Risk prioritization is the risk management phase that involves ranking risks based on their severity level and determining which risks need immediate attention or action. Risk treatment is the risk management phase that involves selecting and implementing appropriate controls or strategies to address risks based on their severity level. Risk treatment can include avoiding, transferring, reducing, or accepting risks. Risk monitoring is the risk management phase that involves tracking and reviewing the performance and effectiveness of risk controls or strategies over time.

#### NEW QUESTION 44

Giovanni, a system administrator, was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. Identify the type of account created by Giovanni in this scenario.

- A. Third-party account
- B. Group-based account
- C. Shared account
- D. Application account

**Answer:** B

#### Explanation:

Group-based account is the type of account created by Giovanni in this scenario. An account is a set of credentials, such as a username and a password, that allows a user to access a system or network. An account can have different types based on its purpose or usage. A group-based account is a type of account that allows multiple users to access a system or network with the same credentials and permissions. A group-based account can be used to simplify the management of users and resources by assigning them to groups based on their roles or functions. In the scenario, Giovanni was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. This means that he created a group-based account for those employees. A third-party account is a type of account that allows an external entity or service to access a system or network with limited permissions or scope. A shared account is a type of account that allows multiple users to access a system or network with the same credentials but different permissions. An application account is

a type of account that allows an application or software to access a system or network with specific permissions or functions.

#### NEW QUESTION 45

You have been assigned to perform a vulnerability assessment of a web server located at IP address 20.20.10.26. Identify the vulnerability with a severity score of 8.0. You can use the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password for this challenge. (Practical Question)

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

**Answer:** A

#### Explanation:

TCP Timestamps is the vulnerability with a severity score of 8.0. This can be verified by performing a vulnerability assessment of the web server located at IP address 20.20.10.26 using the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password. To perform the vulnerability assessment, one can follow these steps:

Launch the Parrot Security machine and open a terminal.

Enter the command `sudo openvas-start` to start the OpenVAS service and wait for a few minutes until it is ready.

Open a web browser and navigate to `https://127.0.0.1:9392` to access the OpenVAS web interface.

Enter the credentials admin/password to log in to OpenVAS.

Click on Scans -> Tasks from the left menu and then click on the blue icon with a star to create a new task.

Enter a name and a comment for the task, such as "Web Server Scan". Select "Full and fast" as the scan config from the drop-down menu. Click on the icon with a star next to Target to create a new target. Enter a name and a comment for the target, such as "Web Server". Enter 20.20.10.26 as the host in the text box and click on Save.

Select "Web Server" as the target from the drop-down menu and click on Save.

Click on the green icon with a play button next to the task name to start the scan and wait for it to finish.

Click on the task name to view the scan report and click on Results from the left menu to see the list of vulnerabilities found.

Sort the list by Severity in descending order and look for the vulnerability with a severity score of 8.0. The screenshot below shows an example of performing these steps: The vulnerability with a severity score of 8.0 is TCP Timestamps, which is an option in TCP packets that can be used to measure round-trip time and improve performance, but it can also reveal information about the system's uptime, clock skew, or TCP sequence numbers, which can be used by attackers to launch various attacks, such as idle scanning, OS fingerprinting, or TCP hijacking<sup>1</sup>. The vulnerability report provides more details about this vulnerability, such as its description, impact, solution, references, and CVSS score<sup>2</sup>. References: Screenshot of OpenVAS showing TCP Timestamps vulnerability, TCP Timestamps Vulnerability, Vulnerability Report

#### NEW QUESTION 48

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

**Answer:** C

#### Explanation:

FTP Unencrypted Cleartext Login is the vulnerability that may affect the website according to the severity factor in the above scenario. A vulnerability is a weakness or flaw in a system or network that can be exploited by an attacker to compromise its security or functionality. A vulnerability assessment is a process that involves identifying, analyzing, and evaluating vulnerabilities in a system or network using various tools and techniques. Greenbone is a tool that can perform vulnerability assessment on various targets using various tests and scans. To perform a vulnerability assessment on the given IP address 20.20.10.26, one has to follow these steps:

? Open a web browser and type 20.20.10.26:9392

? Press Enter key to access the Greenbone web interface.

? Enter admin as username and password as password.

? Click on Login button.

? Click on Scans menu and select Tasks option.

? Click on Start Scan icon next to IP Address Scan task.

? Wait for the scan to complete and click on Report icon next to IP Address Scan task.

? Observe the vulnerabilities found by the scan.

The vulnerabilities found by the scan are:

| Name                            | Severity |
|---------------------------------|----------|
| TCP timestamps                  | Low      |
| Anonymous FTP Login Reporting   | Low      |
| FTP Unencrypted Cleartext Login | Medium   |
| UDP timestamps                  | Low      |

The vulnerability that may affect the website according to the severity factor is FTP Unencrypted Cleartext Login, which has a medium severity level. FTP Unencrypted Cleartext Login is a vulnerability that allows an attacker to intercept or sniff FTP login credentials that are sent in cleartext over an unencrypted connection. An attacker can use these credentials to access or modify files or data on the FTP server. TCP timestamps and UDP timestamps are vulnerabilities that allow an attacker to estimate the uptime of a system or network by analyzing the timestamp values in TCP or UDP packets. Anonymous FTP Login Reporting is a vulnerability that allows an attacker to access an FTP server anonymously without providing any username or password.

#### NEW QUESTION 51

Alex, a certified security professional, works for both aggressor and defender teams. His team's main responsibility involves enhancing protection and boosting the

security standards of the organization. Identify Alex's team in this scenario.

- A. White team
- B. Purple team
- C. Blue team
- D. Red team

**Answer: B**

**Explanation:**

Purple team is the team that Alex works for in this scenario. A team is a group of people that work together to achieve a common goal or objective. A team can have different types based on its role or function in an organization or a project. A purple team is a type of team that works for both aggressor and defender teams. A purple team can be used to enhance protection and boost the security standards of an organization by performing various tasks, such as testing, evaluating, improving, or integrating the security measures implemented by the defender team or exploited by the aggressor team. In the scenario, Alex is a certified security professional who works for both aggressor and defender teams. His team's main responsibility involves enhancing protection and boosting the security standards of the organization. This means that he works for a purple team. A white team is a type of team that acts as an observer or an arbitrator between the aggressor and defender teams. A white team can be used to monitor, evaluate, or adjudicate the performance or outcome of the aggressor and defender teams by providing feedback, guidance, or rules. A blue team is a type of team that acts as a defender or a protector of an organization's network or system. A blue team can be used to prevent, detect, or respond to attacks from external or internal threats by implementing various security measures, such as firewalls, antivirus, encryption, etc. A red team is a type of team that acts as an attacker or an adversary of an organization's network or system. A red team can be used to simulate realistic attacks from external or internal threats by exploiting various vulnerabilities, weaknesses, or gaps in the organization's security posture.

**NEW QUESTION 52**

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. dnstenum
- B. arp
- C. traceroute
- D. ipconfig

**Answer: C**

**Explanation:**

Traceroute is the network troubleshooting utility employed by Steve in the above scenario. Traceroute is a utility that traces the route of packets from a source host to a destination host over a network. Traceroute sends ICMP echo request packets with increasing TTL (Time to Live) values and records the ICMP echo reply packets from each intermediate router or gateway along the path. Traceroute can help identify the network hops, latency, and packet loss between the source and destination hosts. Dnenum is a utility that enumerates DNS information from a domain name or an IP address. Arp is a utility that displays and modifies the ARP (Address Resolution Protocol) cache of a host. Ipconfig is a utility that displays and configures the IP (Internet Protocol) settings of a host.

**NEW QUESTION 56**

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

**Answer: B**

**Explanation:**

Masking is the technique that Andre employed in the above scenario. Masking is a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (\*) and hashes (#). Masking can help protect sensitive data from unauthorized access or disclosure, while preserving the format and structure of the original data. Tokenization is a deidentification technique that can replace the critical information in database fields with random tokens that have no meaning or relation to the original data. Hashing is a deidentification technique that can transform the critical information in database fields into fixed-length strings using a mathematical function. Bucketing is a deidentification technique that can group the critical information in database fields into ranges or categories based on certain criteria.

**NEW QUESTION 59**

An IoT device placed in a hospital for safety measures has sent an alert to the server. The network traffic has been captured and stored in the Documents folder of the "Attacker Machine-1". Analyze the IoTdeviceTraffic.pcapng file and identify the command the IoT device sent over the network. (Practical Question)

- A. Tempe\_Low
- B. Low\_Tempe
- C. High\_Tcmpe
- D. Temp\_High

**Answer: D**

**Explanation:**

The IoT device sent the command Temp\_High over the network, which indicates that the temperature in the hospital was above the threshold level. This can be verified by analyzing the IoTdeviceTraffic.pcapng file using a network protocol analyzer tool such as Wireshark4. The command Temp\_High can be seen in the data field of the UDP packet sent from the IoT device (192.168.0.10) to the server (192.168.0.1) at 12:00:03. The screenshot below shows the packet details5: References: Wireshark User's Guide, [IoTdeviceTraffic.pcapng]

### NEW QUESTION 63

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

**Answer: D**

#### Explanation:

Recovery is the business continuity and disaster recovery activity that Kasen performed in the above scenario. Business continuity and disaster recovery (BCDR) is a process that involves planning, preparing, and implementing various activities to ensure the continuity of critical business functions and the recovery of essential resources in the event of a disaster or disruption. BCDR activities can be categorized into four phases: prevention, response, resumption, and recovery. Prevention is the BCDR phase that involves identifying and mitigating potential risks and threats that can cause a disaster or disruption. Response is the BCDR phase that involves activating the BCDR plan and executing the immediate actions to protect people, assets, and operations during a disaster or disruption. Resumption is the BCDR phase that involves restoring the minimum level of services and functions required to resume normal business operations after a disaster or disruption. Recovery is the BCDR phase that involves restoring both the disaster site and the damaged materials to the pre-disaster levels during an incident.

### NEW QUESTION 64

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

**Answer: B**

#### Explanation:

Obfuscating is the technique used by Kevin to evade the IDS system in the above scenario. Obfuscating is a technique that involves encoding or modifying packets or data with various methods or characters to make them unreadable or unrecognizable by an IDS (Intrusion Detection System). Obfuscating can be used to bypass or evade an IDS system that relies on signatures or patterns to detect malicious activities. Obfuscating can include encoding packets with Unicode characters, which are characters that can represent various languages and symbols. The IDS system cannot recognize the packet, but the target web server can decode them and execute them normally. Desynchronization is a technique that involves creating discrepancies or inconsistencies between the state of a connection as seen by an IDS system and the state of a connection as seen by the end hosts. Desynchronization can be used to bypass or evade an IDS system that relies on stateful inspection to track and analyze connections. Desynchronization can include sending packets with invalid sequence numbers, which are numbers that indicate the order of packets in a connection. Session splicing is a technique that involves splitting or dividing packets or data into smaller fragments or segments to make them harder to detect by an IDS system. Session splicing can be used to bypass or evade an IDS system that relies on packet size or content to detect malicious activities. Session splicing can include sending packets with small MTU (Maximum Transmission Unit) values, which are values that indicate the maximum size of packets that can be transmitted over a network. An urgency flag is a flag in the TCP (Transmission Control Protocol) header that indicates that the data in the packet is urgent and should be processed immediately by the receiver. An urgency flag is not a technique to evade an IDS system, but it can be used to trigger an IDS system to generate an alert or a response.

### NEW QUESTION 66

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 media.

Identify the method utilized by Ruben in the above scenario.

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

**Answer: B**

#### Explanation:

Bit-stream imaging is the method utilized by Ruben in the above scenario.

Bit-stream imaging is a method that involves creating a cloned copy of the entire media and prevents the contamination of the original media. Bit-stream imaging copies all the data on the media, including deleted files and folders, hidden partitions, slack space, etc., at a bit level. Bit-stream imaging preserves the integrity and authenticity of the digital evidence and allows further analysis without affecting the original media. Sparse acquisition is a method that involves creating a partial copy of the media by skipping empty sectors or blocks. Drive decryption is a method that involves decrypting an encrypted drive or partition using a password or a key. Logical acquisition is a method that involves creating a copy of the logical files and folders on the media using file system commands.

### NEW QUESTION 67

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

**Answer:** D

**Explanation:**

5.9.188.148 is the IP address linked with <http://securityabc.s21sec.com> in the above scenario. A threat intelligence feed is a source of data that provides information about current or potential threats and attacks that can affect an organization's network or system. A threat intelligence feed can include indicators of compromise (IoCs), such as IP addresses, domain names, URLs, hashes, etc., that can be used to detect or prevent malicious activities. To analyze the threat intelligence feed data file and determine the IP address linked with <http://securityabc.s21sec.com>, one has to follow these steps:

? Navigate to the Documents folder of Attacker-1 machine.

? Open Threatfeed.txt file with a text editor.

? Search for <http://securityabc.s21sec.com> in the file.

? Observe the IP address associated with the URL.

The IP address associated with the URL is 5.9.188.148, which is the IP address linked with <http://securityabc.s21sec.com>.

**NEW QUESTION 72**

Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN. To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. Identify the type of wireless encryption employed by Charlie in the above scenario.

- A. TKIP
- B. WEP
- C. AES
- D. CCMP

**Answer:** B

**Explanation:**

WEP is the type of wireless encryption employed by Charlie in the above scenario. Wireless encryption is a technique that involves encoding or scrambling the data transmitted over a wireless network to prevent unauthorized access or interception. Wireless encryption can use various algorithms or protocols to encrypt and decrypt the data, such as WEP, WPA, WPA2, etc. WEP (Wired Equivalent Privacy) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer

. WEP can be used to provide basic security and privacy for wireless networks, but it can also be easily cracked or compromised by various attacks . In the scenario, Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN (Wireless Local Area Network). To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. This means that he employed WEP for this purpose. TKIP (Temporal Key Integrity Protocol) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer with dynamic keys . TKIP can be used to provide enhanced security and compatibility for wireless networks, but it can also be vulnerable to certain attacks . AES (Advanced Encryption Standard) is a type of wireless encryption that uses the Rijndael algorithm to encrypt information in the data link layer with fixed keys . AES can be used to provide strong security and performance for wireless networks, but it can also require more processing power and resources . CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is a type of wireless encryption that uses the AES algorithm to encrypt information in the data link layer with dynamic keys .

CCMP can be used to provide robust security and reliability for wireless networks, but it can also require more processing power and resources

**NEW QUESTION 76**

An organization's risk management team identified the risk of natural disasters in the organization's current location. Because natural disasters cannot be prevented using security controls, the team suggested to build a new office in another location to eliminate the identified risk. Identify the risk treatment option suggested by the risk management team in this scenario.

- A. Risk modification
- B. Risk avoidance
- C. Risk sharing
- D. Risk retention

**Answer:** B

**Explanation:**

Risk avoidance is the risk treatment option suggested by the risk management team in this scenario. Risk avoidance is a risk treatment option that involves eliminating the identified risk by changing the scope, requirements, or objectives of the project or activity. Risk avoidance can be used when the risk cannot be prevented using security controls or when the risk outweighs the benefits. References: Risk Avoidance

**NEW QUESTION 81**

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

**Answer:** C

**Explanation:**

A data-driven hunting method is a type of threat hunting method that employs existing data collected from various sources, such as DNS and proxy logs, to generate and test hypotheses about potential threats. This method relies on data analysis and machine learning techniques to identify patterns and anomalies that indicate malicious activity. A data-driven hunting method can help discover unknown or emerging threats that may evade traditional detection methods. An entity-driven hunting method is a type of threat hunting method that focuses on specific entities, such as users, devices, or domains, that are suspected or known to be involved in malicious activity. A TTP-driven hunting method is a type of threat hunting method that leverages threat intelligence and knowledge of adversary tactics, techniques, and procedures (TTPs) to formulate and test hypotheses about potential threats. A hybrid hunting method is a type of threat hunting method that combines different approaches, such as data-driven, entity-driven, and TTP-driven methods, to achieve more comprehensive and effective results.

#### NEW QUESTION 85

Ayden works from home on his company's laptop. During working hours, he received an antivirus software update notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel. Which of the following PCI-DSS requirements is demonstrated in this scenario?

- A. PCI-DSS requirement no 5.3
- B. PCI-DSS requirement no 1.3.1
- C. PCI-DSS requirement no 5.1
- D. PCI-DSS requirement no 1.3.2

**Answer:** A

#### Explanation:

PCI-DSS requirement no 5.3 is the PCI-DSS requirement that is demonstrated in this scenario. PCI-DSS (Payment Card Industry Data Security Standard) is a set of standards that applies to entities that store, process, or transmit payment card information, such as merchants, service providers, or payment processors. PCI-DSS requires them to protect cardholder data from unauthorized access, use, or disclosure. PCI-DSS consists of 12 requirements that are grouped into six categories: build and maintain a secure network and systems, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy. PCI-DSS requirement no 5.3 is part of the category "maintain a vulnerability management program" and states that antivirus mechanisms must be actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. In the scenario, Ayden works from home on his company's laptop. During working hours, he received an antivirus software update notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel. This means that his company's laptop has an antivirus mechanism that is actively running and cannot be disabled or altered by users, which demonstrates PCI-DSS requirement no 5.3.

#### NEW QUESTION 90

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@I23

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

**Answer:** C

#### Explanation:

Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Social engineering is a technique that involves manipulating or deceiving people into performing actions or revealing information that can be used for malicious purposes. Social engineering can be performed through various methods, such as phone calls, emails, websites, etc. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy. In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact 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. Diversion theft is a social engineering method that involves diverting the delivery or shipment of goods or assets to a different location or destination. Elicitation is a social engineering method that involves extracting information from a target by engaging them in a conversation or an interaction. Phishing is a social engineering method that involves sending fraudulent emails or messages that appear to come from a trusted source, such as a bank, a company, or a person, and asking the recipient to click on a link, open an attachment, or provide personal or financial information.

#### NEW QUESTION 94

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

**Answer:** C

#### Explanation:

A hub-and-spoke VPN topology is a type of VPN topology where all the remote offices communicate with the corporate office, but communication between the remote offices is denied. The corporate office acts as the hub, and the remote offices act as the spokes. This topology reduces the number of VPN tunnels required and simplifies the management of VPN policies. A point-to-point VPN topology is a type of VPN topology where two endpoints establish a direct VPN connection. A star topology is a type of VPN topology where one endpoint acts as the central node and connects to multiple other endpoints. A full-mesh VPN topology is a type of VPN topology where every endpoint connects to every other endpoint.

#### NEW QUESTION 96

George, a security professional at an MNC, implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. Identify the type of Internet access policy implemented by George in this scenario.

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

**Answer:** A

**Explanation:**

Permissive policy is the type of Internet access policy implemented by George in this scenario. An Internet access policy is a policy that defines the rules and guidelines for accessing the Internet from a system or network. An Internet access policy can be based on various factors, such as security, productivity, bandwidth, etc. An Internet access policy can have different types based on its level of restriction or control. A permissive policy is a type of Internet access policy that allows users to access any site, download any application, and access any computer or network without any restrictions. A permissive policy can be used to provide maximum flexibility and freedom to users, but it can also pose significant security risks and challenges. In the scenario, George implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. This means that he implemented a permissive policy for those employees. A paranoid policy is a type of Internet access policy that blocks or denies all Internet access by default and only allows specific sites, applications, or computers that are explicitly authorized. A prudent policy is a type of Internet access policy that allows most Internet access but blocks or restricts some sites, applications, or computers that are deemed inappropriate, malicious, or unnecessary. A promiscuous policy is not a type of Internet access policy, but a term that describes a network mode that allows a network interface card (NIC) to capture all packets on a network segment, regardless of their destination address.

**NEW QUESTION 101**

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

**Answer:** A

**Explanation:**

The correct answer is A, as it identifies the type of Internet access policy implemented by Ashton in the above scenario. An Internet access policy is a set of rules and guidelines that defines how an organization's employees or members can use the Internet and what types of websites or services they can access. There are different types of Internet access policies, such as:

? Paranoid policy: This type of policy forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage. This policy is suitable for organizations that deal with highly sensitive or classified information and have a high level of security and compliance requirements.

? Prudent policy: This type of policy allows some things and blocks others and imposes moderate restrictions on company computers, depending on the role and responsibility of the user. This policy is suitable for organizations that deal with confidential or proprietary information and have a medium level of security and compliance requirements.

? Permissive policy: This type of policy allows most things and blocks few and imposes minimal restrictions on company computers, as long as the user does not violate any laws or regulations. This policy is suitable for organizations that deal with public or general information and have a low level of security and compliance requirements.

? Promiscuous policy: This type of policy allows everything and blocks nothing and imposes no restrictions on company computers, regardless of the user's role or responsibility. This policy is suitable for organizations that have no security or compliance requirements and trust their employees or members to use the Internet responsibly.

In the above scenario, Ashton implemented a paranoid policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage. Option B is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A prudent policy allows some things and blocks others and imposes moderate restrictions on company computers, depending on the role and responsibility of the user. In the above scenario, Ashton did not implement a prudent policy, but a paranoid policy. Option C is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A permissive policy allows most things and blocks few and imposes minimal restrictions on company computers, as long as the user does not violate any laws or regulations. In the above scenario, Ashton did not implement a permissive policy, but a paranoid policy. Option D is incorrect, as it does not identify the type of Internet access policy implemented by Ashton in the above scenario. A promiscuous policy allows everything and blocks nothing and imposes no restrictions on company computers, regardless of the user's role or responsibility. In the above scenario, Ashton did not implement a promiscuous policy, but a paranoid policy.

References: , Section 6.2

**NEW QUESTION 103**

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

**Answer:** A

**Explanation:**

Containment is the IH&R step performed by Warren in the above scenario. IH&R (Incident Handling and Response) is a process that involves identifying, analyzing, containing, eradicating, recovering from, and reporting on security incidents that affect an organization's network or system. Containment is the IH&R step that involves implementing appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization. Containment can be done by isolating the affected system or network, blocking malicious traffic or communication, disabling or removing malicious accounts or processes, etc. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Eradication is the IH&R step that involves removing all traces of the incident from the system or network, such as malware, backdoors, compromised files, etc. Incident triage is the IH&R step that involves prioritizing incidents based on their severity, impact, and urgency.

**NEW QUESTION 104**

As a cybersecurity technician, you were assigned to analyze the file system of a Linux image captured from a device that has been attacked recently. Study the forensic image "Evidenced.img" in the Documents folder of the "Attacker Machine-1" and identify a user from the image file. (Practical Question)

- A. smith

- B. attacker
- C. roger
- D. john

**Answer:** B

**Explanation:**

The attacker is a user from the image file in the above scenario. A file system is a method or structure that organizes and stores files and data on a storage device, such as a hard disk, a flash drive, etc. A file system can have different types based on its format or features, such as FAT, NTFS, ext4, etc. A file system can be analyzed to extract various information, such as file names, sizes, dates, contents, etc. A Linux image is an image file that contains a copy or a snapshot of a Linux-based file system. A Linux image can be analyzed to extract various information about a Linux-based system or device. To analyze the file system of a Linux image captured from a device that has been attacked recently and identify a user from the image file, one has to follow these steps:

? Navigate to Documents folder of Attacker Machine-1.

? Right-click on Evidenced.img file and select Mount option.

? Wait for the image file to be mounted and assigned a drive letter.

? Open File Explorer and navigate to the mounted drive.

? Open etc folder and open passwd file with a text editor.

? Observe the user accounts listed in the file. The user accounts listed in the file are:

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www- data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
timesync:x:100: systemd-network:x: systemd-resolve:x: systemd-bus-proxy:x: syslog:x: _apt:x: messagebus:x: uidd:x: lightdm:x: whoopsie:x: avahi-autoipd:x:
avahi:x: dnsmasq:x: colord:x: speech-dispatcher:x: hplip:x: kernoops:x: saned:x: nm-openvpn:x: nm- openconnect:x: pulse:x: rtkit:x: sshd:x: attacker::1000
```

The user account that is not a system or service account is attacker, which is a user from the image file.

**NEW QUESTION 106**

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

**Answer:** C

**Explanation:**

Containerization is the technique that Stephen has implemented in the above scenario. Containerization is a technique that isolates personal and corporate data on an employee's mobile device. Containerization creates separate encrypted containers or partitions on the device, where corporate applications and data are stored and managed. Containerization prevents corporate data leakage on employees' mobile devices by restricting access, sharing, copying, or transferring of data between containers. Containerization also allows remote wiping of corporate data in case of device loss or theft

. Full device encryption is a technique that encrypts all the data on a mobile device using a password or a key. Geofencing is a technique that uses GPS or RFID to define geographical boundaries and trigger actions based on the location of a mobile device. OTA (Over-the-Air) updates are updates that are delivered wirelessly to mobile devices without requiring physical connection to a computer.

**NEW QUESTION 107**

.....

## Relate Links

**100% Pass Your 212-82 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/212-82-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>