

212-82 Dumps

Certified Cybersecurity Technician(C|CT)

<https://www.certleader.com/212-82-dumps.html>



NEW QUESTION 1

In a security incident, the forensic investigation has isolated a suspicious file named "security_update.exe". You are asked to analyze the file in the Documents folder of the "Attacker Machine-1" to determine whether it is malicious. Analyze the suspicious file and identify the malware signature. (Practical Question)

- A. Stuxnet
- B. KLEZ
- C. ZEUS
- D. Conficker

Answer: A

Explanation:

Stuxnet is the malware signature of the suspicious file in the above scenario. Malware is malicious software that can harm or compromise the security or functionality of a system or network. Malware can include various types, such as viruses, worms, trojans, ransomware, spyware, etc. Malware signature is a unique pattern or characteristic that identifies a specific malware or malware family. Malware signature can be used to detect or analyze malware by comparing it with known malware signatures in databases or repositories. To analyze the suspicious file and identify the malware signature, one has to follow these steps:

- ? Navigate to Documents folder of Attacker Machine-1.
- ? Right-click on security_update.exe file and select Scan with VirusTotal option.
- ? Wait for VirusTotal to scan the file and display the results.
- ? Observe the detection ratio and details.

The detection ratio is 59/70, which means that 59 out of 70 antivirus engines detected the file as malicious. The details show that most antivirus engines detected the file as Stuxnet, which is a malware signature of a worm that targets industrial control systems (ICS). Stuxnet can be used to sabotage or damage ICS by modifying their code or behavior. Therefore, Stuxnet is the malware signature of the suspicious file. KLEZ is a malware signature of a worm that spreads via email and network shares. KLEZ can be used to infect or overwrite files, disable antivirus software, or display fake messages. ZEUS is a malware signature of a trojan that targets banking and financial systems. ZEUS can be used to steal or modify banking credentials, perform fraudulent transactions, or install other malware. Conficker is a malware signature of a worm that exploits a vulnerability in Windows operating systems. Conficker can be used to create a botnet, disable security services, or download other malware

NEW QUESTION 2

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 3

Zayn, a network specialist at an organization, used Wireshark to perform network analysis. He selected a Wireshark menu that provided a summary of captured packets, IO graphs, and flow graphs. Identify the Wireshark menu selected by Zayn in this scenario.

- A. Status bar
- B. Analyze
- C. Statistics
- D. Packet list panel

Answer: C

Explanation:

Statistics is the Wireshark menu selected by Zayn in this scenario. Statistics is a Wireshark menu that provides a summary of captured packets, IO graphs, and flow graphs. Statistics can be used to analyze various aspects of network traffic, such as protocols, endpoints, conversations, or packet lengths.

References: Wireshark Statistics Menu

NEW QUESTION 4

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

Answer: C

Explanation:

The correct answer is C, as it identifies the designation of Zion. A guard is a person who is responsible for implementing and managing the physical security equipment installed around the facility. A guard typically performs tasks such as:

- ? Checking the functionality of equipment related to physical security
- ? Monitoring the surveillance cameras and alarms
- ? Controlling the access to restricted areas
- ? Responding to emergencies or incidents

In the above scenario, Zion belongs to this category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. Option A is incorrect, as it does not identify the designation of Zion. A supervisor is a person who is responsible for overseeing and directing the work of other employees. A supervisor typically performs tasks such as:

- ? Assigning tasks and responsibilities to employees
- ? Evaluating the performance and productivity of employees
- ? Providing feedback and guidance to employees
- ? Resolving conflicts or issues among employees

In the above scenario, Zion does not belong to this category of employees who are responsible for overseeing and directing the work of other employees. Option B is incorrect, as it does not identify the designation of Zion. A chief information security officer (CISO) is a person who is responsible for establishing and maintaining the security vision, strategy, and program for an organization. A CISO typically performs tasks such as:

- ? Developing and implementing security policies and standards
- ? Managing security risks and compliance
- ? Leading security teams and projects
- ? Communicating with senior management and stakeholders

In the above scenario, Zion does not belong to this category of employees who are responsible for establishing and maintaining the security vision, strategy, and program for

an organization. Option D is incorrect, as it does not identify the designation of Zion. A safety officer is a person who is responsible for ensuring that health and safety regulations are followed in an organization. A safety officer typically performs tasks such as:

- ? Conducting safety inspections and audits
- ? Identifying and eliminating hazards and risks
- ? Providing safety training and awareness
- ? Reporting and investigating accidents or incidents

In the above scenario, Zion does not belong to this category of employees who are responsible for ensuring that health and safety regulations are followed in an organization. References: Section 7.1

NEW QUESTION 5

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 6

Finley, a security professional at an organization, was tasked with monitoring the organizational network behavior through the SIEM dashboard. While monitoring, Finley noticed suspicious activities in the network; thus, he captured and analyzed a single network packet to determine whether the signature included malicious patterns. Identify the attack signature analysis technique employed by Finley in this 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 attack signature analysis technique employed by Finley in this scenario. Content-based signature analysis is a technique that captures and analyzes a single network packet to determine whether the signature included malicious patterns. Content-based signature analysis can be used to detect known attacks, such as buffer overflows, SQL injections, or cross-site scripting². References: Content-Based Signature Analysis

NEW QUESTION 7

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 media. 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

Answer: D

Explanation:

Recovery is the IH&R step performed by Edwin 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. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Recovery can include reinstating lost data from the backup media, applying patches or updates, reconfiguring settings, testing functionality, etc. Recovery also involves ensuring that the backup does not have any traces of malware or compromise. 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 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. Notification is the IH&R step that involves informing relevant stakeholders, authorities, or customers about the incident and its impact.

NEW QUESTION 8

Gideon, a forensic officer, was examining a victim's Linux system suspected to be involved in online criminal activities. Gideon navigated to a directory containing a log file that recorded information related to user login/logout. This information helped Gideon to determine the current login state of cyber criminals in the victim system, identify the Linux log file accessed by Gideon in this scenario.

- A. /var/log/mysqld
- B. log
- C. /var/log/wtmp
- D. /var/log/boot.log
- E. /var/log/httpd/

Answer: B

Explanation:

/var/log/wtmp is the Linux log file accessed by Gideon in this scenario.

/var/log/wtmp is a log file that records information related to user login/logout, such as username, terminal, IP address, and login time. /var/log/wtmp can be used to determine the current login state of users in a Linux system. /var/log/wtmp can be viewed using commands such as last, lastb, or utmpdump1. References: Linux Log Files

NEW QUESTION 9

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 10

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 10

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

Answer: B

Explanation:

Investigation objectives is the section of the forensic investigation report where Arabella recorded the “nature of the claim and information provided to the officers” in the above scenario. A forensic investigation report is a document that summarizes the findings and conclusions of a forensic investigation. A forensic investigation report typically follows a standard template that contains different sections covering all the details of the crime and the investigation process. Investigation objectives is the section of the forensic investigation report that describes the purpose and scope of the investigation, the nature of the claim and information provided to the officers, and the questions or issues to be addressed by the investigation. Investigation process is the section of the forensic investigation report that describes the steps and methods followed by the investigators, such as evidence collection, preservation, analysis, etc. Evidence information is the section of the forensic investigation report that lists and describes the evidence obtained from various sources, such as devices, media, witnesses, etc. Evaluation and analysis process is the section of the forensic investigation report that explains how the evidence was evaluated and analyzed using various tools and techniques, such as software, hardware, etc.

NEW QUESTION 12

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

Answer: D

Explanation:

4 is the UID that is mapped to user john in the database table in the above scenario. SQL injection is a type of web application attack that exploits a vulnerability in a web application that allows an attacker to inject malicious SQL statements into an input field, such as a username or password field, and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web application and fetch the user credentials, one has to follow these steps:

- ? Open a web browser and type www.movieabc.com
- ? Press Enter key to access the web application.
- ? Enter sam as username and test as password.
- ? Click on Login button.
- ? Observe that a welcome message with username sam is displayed.
- ? Click on Logout button.
- ? Enter sam' or '1'=1 as username and test as password.
- ? Click on Login button.
- ? Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.
- ? Click on Logout button.
- ? Enter sam'; SELECT * FROM users; – as username and test as password.
- ? Click on Login button.
- ? Observe that an error message with user credentials from users table is displayed. The user credentials from users table are:
The UID that is mapped to user john is 4.

UID	Username	Password
1	admin	admin
2	sam	test
3	alice	alice123
4	john	john123

NEW QUESTION 16

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 19

Martin, a network administrator at an organization, received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. In which of the following threat-modeling steps did Martin evaluate the severity level of the threat?

- A. Identify vulnerabilities
- B. Application overview
- C. Risk and impact analysis
- D. Decompose the application

Answer: C

Explanation:

Risk and impact analysis is the threat-modeling step in which Martin evaluated the severity level of the threat in the above scenario. Threat modeling is a process that involves identifying, analyzing, and mitigating threats and risks to a system or network. Threat modeling can be used to improve the security and resilience of a system or network by applying various methods or techniques, such as STRIDE, DREAD, PASTA, etc. Threat modeling consists of various steps or phases that perform different tasks or roles. Risk and impact analysis is a threat-modeling step that involves assessing the likelihood and consequences of threats and risks to a system or network. Risk and impact analysis can be used to evaluate the severity level of threats and risks and prioritize them for mitigation. In the scenario, Martin received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. This means that he performed risk and impact analysis for this purpose. Identify vulnerabilities is a threat-modeling step that involves finding and documenting the weaknesses or flaws in a system or network that can be exploited by threats or risks. Application overview is a threat-modeling step that involves defining and understanding the scope, architecture, components, and functionality of a system or network. Decompose the application is a threat-modeling step that involves breaking down a system or network into smaller and simpler elements, such as data flows, processes, assets, etc.

NEW QUESTION 23

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 26

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 31

A startup firm contains various devices connected to a wireless network across the floor. An AP with Internet connectivity is placed in a corner to allow wireless communication between devices. To support new devices connected to the network beyond the APS range, an administrator used a network device that extended the signals of the wireless AP and transmitted it to uncovered area, identify the network component employed by the administrator to extend signals in this scenario.

- A. Wireless repeater
- B. Wireless bridge
- C. wireless modem
- D. Wireless router

Answer: A

Explanation:

Wireless repeater is the network component employed by the administrator to extend signals in this scenario. A wireless network is a type of network that uses radio waves or infrared signals to transmit data between devices without using cables or wires. A wireless network can consist of various components, such as

wireless access points (APs), wireless routers, wireless adapters, wireless bridges, wireless repeaters, etc. A wireless repeater is a network component that extends the range or coverage of a wireless signal by receiving it from an AP or another repeater and retransmitting it to another area. A wireless repeater can be used to support new devices connected to the network beyond the AP's range. In the scenario, a startup firm contains various devices connected to a wireless network across the floor. An AP with internet connectivity is placed in a corner to allow wireless communication between devices. To support new devices connected to the network beyond the AP's range, an administrator used a network component that extended the signals of the wireless AP and transmitted it to the uncovered area. This means that he used a wireless repeater for this purpose. A wireless bridge is a network component that connects two or more wired or wireless networks or segments together. A wireless bridge can be used to expand the network or share resources between networks. A wireless modem is a network component that modulates and demodulates wireless signals to enable data transmission over a network. A wireless modem can be used to provide internet access to devices via a cellular network or a satellite network. A wireless router is a network component that performs the functions of both a wireless AP and a router. A wireless router can be used to create a wireless network and connect it to another network, such as the internet.

NEW QUESTION 34

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 data. 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

Answer: B

Explanation:

WPA3 encryption is the type of wireless encryption used by the security solution employed by Matias in the above scenario. WPA3 encryption is the latest and most secure version of Wi-Fi Protected Access, a protocol that provides authentication and encryption for wireless networks. WPA3 encryption uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data. WPA3 encryption also provides enhanced protection against offline dictionary attacks, forward secrecy, and secure public Wi-Fi access. WPA2 encryption is the previous version of Wi-Fi Protected Access, which uses Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) for data encryption. WEP encryption is an outdated and insecure version of Wi-Fi security, which uses RC4 stream cipher for data encryption. WPA encryption is an intermediate version of Wi-Fi security, which uses TKIP for data encryption.

NEW QUESTION 37

Jordan, a network administrator in an organization, was instructed to identify network-related issues and improve network performance. While troubleshooting the network, he received a message indicating that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host, which of the following network issues did Jordan find in this scenario?

- A. Time exceeded message
- B. Destination unreachable message
- C. Unreachable networks
- D. Network cable is unplugged

Answer: B

Explanation:

Destination unreachable message is the network issue that Jordan found in this scenario. Destination unreachable message is a type of ICMP message that indicates that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host. Destination unreachable message can be caused by various reasons, such as incorrect routing, firewall blocking, or host configuration problems.

References: Destination Unreachable Message

NEW 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

Answer: BCD

Explanation:

Turn the device ON if it is OFF, do not leave the device as it is if it is ON, and make sure that the device is charged are some of the points that Shawn must follow while preserving the digital evidence in the above scenario. Digital evidence is any information or data stored or transmitted in digital form that can be used in a legal proceeding or investigation. Digital evidence can be found on various devices, such as computers, mobile phones, tablets, etc. Preserving digital evidence is a crucial step in forensic investigation that involves protecting and maintaining the integrity and authenticity of digital evidence from any alteration or damage. Some of the points that Shawn must follow while preserving digital evidence are:

? Turn the device ON if it is OFF: If the device is OFF, Shawn must turn it ON to prevent any data loss or encryption that may occur when the device is powered off. Shawn must also document any password or PIN required to unlock or access the device.

? Do not leave the device as it is if it is ON: If the device is ON, Shawn must not leave it as it is or use it for any purpose other than preserving digital evidence. Shawn must also disable any network connections or communication features on the device, such as Wi-Fi, Bluetooth, cellular data, etc., to prevent any remote access or deletion of data by unauthorized parties.

? Make sure that the device is charged: Shawn must ensure that the device has enough battery power to prevent any data loss or corruption that may occur due to sudden shutdown or low battery. Shawn must also use a write blocker or a Faraday bag to isolate the device from any external interference or signals.

Never record the screen display of the device is not a point that Shawn must follow while preserving digital evidence. On contrary, Shawn should record or photograph the screen display of the device to capture any relevant information or messages that may appear on the screen. Recording or photographing the screen display of the device can also help document any changes or actions performed on the device during preservation.

NEW QUESTION 46

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

Answer: A

Explanation:

Quantum cryptography is the encryption mechanism demonstrated in the above scenario. Quantum cryptography is a branch of cryptography that uses quantum physics to secure data transmission and communication. Quantum cryptography encrypts data by using a sequence of photons that have a spinning trait, called polarization, while traveling from one end to another. These photons keep changing their shapes, called states, during their course through filters: vertical, horizontal, forward slash, and backslash. Quantum cryptography ensures that any attempt to intercept or tamper with the data will alter the quantum states of the photons and be detected by the sender and receiver. Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without decrypting it first. Rivest Shamir Adleman (RSA) encryption is a type of asymmetric encryption that uses two keys, public and private, to encrypt and decrypt data. Elliptic curve cryptography (ECC) is a type of asymmetric encryption that uses mathematical curves to generate keys and perform encryption and decryption.

NEW QUESTION 48

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

Answer: A

Explanation:

A cloud auditor is a role played by Walker in the above scenario. A cloud auditor is a third party who examines controls of cloud computing service providers. Cloud auditor performs an audit to verify compliance with the standards and expressed his opinion through a report⁸⁹. A cloud provider is an entity that provides cloud services, such as infrastructure, platform, or software, to cloud consumers¹⁰. A cloud carrier is an entity that provides connectivity and transport of cloud services between cloud providers and cloud consumers¹⁰. A cloud consumer is an entity that uses cloud services for its own purposes or on behalf of another entity

NEW QUESTION 49

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 51

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 54

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 data. Which of the following regulations is mostly violated?

- A. HIPPA/PHI
- B. PII
- C. PCIDSS
- D. ISO 2002

Answer: A

Explanation:

HIPPA/PHI is the regulation that is mostly violated in the above scenario. HIPPA (Health Insurance Portability and Accountability Act) is a US federal law that sets standards for protecting the privacy and security of health information. PHI (Protected Health Information) is any information that relates to the health or health care of an individual and that can identify the individual, such as name, address, medical records, etc. HIPPA/PHI requires covered entities, such as health care providers, health plans, or health care clearinghouses, and their business associates, to safeguard PHI from unauthorized access, use, or disclosure. In the scenario, the medical company experienced a major cyber security breach that exposed the personal medical records of many patients on the internet, which violates HIPPA/PHI regulations. PII (Personally Identifiable Information) is any information that can be used to identify a specific individual, such as name, address, social security number, etc. PII is not specific to health information and can be regulated by various laws, such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), etc. 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. ISO 2002 (International Organization for Standardization 2002) is not a regulation, but a standard for information security management systems that provides guidelines and best practices for organizations to manage their information security risks.

NEW QUESTION 57

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

Answer: A

Explanation:

Hardware-assisted virtualization is 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. Hardware-assisted virtualization relies on special hardware features in the CPU and chipset to create and manage virtual machines efficiently and securely³⁴. Full virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment, but the VMM will run in software and emulate all the hardware resources for each virtual machine⁵. Hybrid virtualization is a virtualization approach that combines hardware-assisted and full virtualization techniques to optimize performance and compatibility⁶. OS-assisted virtualization is a virtualization approach in which the guest OS will be modified to run in a virtualized environment and cooperate with the VMM to access the hardware resources

NEW QUESTION 60

A disgruntled employee has set up a RAT (Remote Access Trojan) server in one of the machines in the target network to steal sensitive corporate documents. The IP address of the target machine where the RAT is installed is 20.20.10.26. Initiate a remote connection to the target machine from the "Attacker Machine-1" using the Thief client. Locate the "Sensitive Corporate Documents" folder in the target machine's Documents directory and determine the number of files. Mint: Thief folder is located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef of the Attacker Machine1.

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

Answer: B

Explanation:

The number of files in the "Sensitive Corporate Documents" folder is 4. This can be verified by initiating a remote connection to the target machine from the "Attacker Machine-1" using Thief client. Thief is a Remote Access Trojan (RAT) that allows an attacker to remotely control a victim's machine and perform various malicious activities. To connect to the target machine using Thief client, one can follow these steps:

Launch Thief client from Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef on the "Attacker Machine-1".

Enter the IP address of the target machine (20.20.10.26) and click on Connect.

Wait for a few seconds until a connection is established and a message box appears saying "Connection Successful".

Click on OK to close the message box and access the remote desktop of the target machine.

Navigate to the Documents directory and locate the "Sensitive Corporate Documents" folder.

Open the folder and count the number of files in it. The screenshot below shows an example of performing these steps: References: [Theef Client Tutorial], [Screenshot of Thief client showing remote desktop and folder]

NEW QUESTION 63

Brielle, a security professional, was instructed to secure her organization's network from malicious activities. To achieve this, she started monitoring network activities on a control system that collected event data from various sources. During this process, Brielle observed that a malicious actor had logged in to access a network device connected to the organizational network. Which of the following types of events did Brielle identify in the above scenario?

- A. Failure audit
- B. Error
- C. Success audit
- D. Warning

Answer: C

Explanation:

Success audit is the type of event that Brielle identified in the above scenario. Success audit is a type of event that records successful attempts to access a network device or resource. Success audit can be used to monitor authorized activities on a network, but it can also indicate unauthorized activities by malicious actors who have compromised credentials or bypassed security controls.

References: Success Audit Event

NEW QUESTION 68

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

Answer: A

Explanation:

Type = 12 is the type of ICMP error message received by Jaden in the above scenario. ICMP (Internet Control Message Protocol) is a protocol that sends error and control messages between network devices. ICMP error messages are categorized by types and codes, which indicate the cause and nature of the error. Type = 12 is the type of ICMP error message that indicates an IP parameter problem, which means that the IP header field contains invalid information. Type = 8 is the type of ICMP message that indicates an echo request, which is used to test the connectivity and reachability of a destination host. Type = 5 is the type of ICMP error message that indicates a redirect, which means that a better route to the destination host is available. Type = 3 is the type of ICMP error message that indicates a destination unreachable, which means that the destination host or network cannot be reached.

NEW QUESTION 73

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 76

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 hijacking¹. The vulnerability report provides more details about this vulnerability, such as its description, impact, solution, references, and CVSS score². References: Screenshot of OpenVAS showing TCP Timestamps vulnerability, TCP Timestamps Vulnerability, Vulnerability Report

NEW QUESTION 81

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

Answer: B

Explanation:

RFID (Radio Frequency Identification) is the wireless technology that the software company has implemented in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects¹¹¹². WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology that provides high-speed broadband access over long distances¹³. Bluetooth is a wireless technology that enables short-range data communication between devices, such as phones, laptops, printers, etc.¹⁴. Wi-Fi (Wireless Fidelity) is a wireless technology that allows devices to connect to a local area network or the internet using radio waves

NEW QUESTION 85

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 88

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. dnsenum
- 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. Dnsenum 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 93

Identify a machine in the network with 5SH service enabled. Initiate an SSH Connection to the machine, find the file, ttag.txt. in the machine, and enter the tile's content as the answer. The credentials for SSH login are sam/adm(admin@123. {Practical Question)

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

Answer: D

Explanation:

bob1@sam is the file's content as the answer. To find the machine with SSH service enabled, one can use a network scanning tool such as Nmap to scan the network for port 22, which is the default port for SSH. For example, the command `nmap -p 22 192.168.0.0/24` will scan the network range 192.168.0.0/24 for port 22 and display the results2. To initiate an SSH connection to the machine, one can use a command-line tool such as ssh or an SSH client such as PuTTY to connect to the machine using the credentials sam/admin@123. For example, the command `ssh sam@192.168.0.10` will connect to the machine with IP address 192.168.0.10 using the username sam and prompt for the password admin@1233. To find the file flag.txt in the machine, one can use a file searching tool such as find or locate to search for the file name in the machine's file system. For example, the command `find / -name flag.txt` will search for the file flag.txt from the root directory (/) and display its location4. To enter the file's content as the answer, one can use a file viewing tool such as cat or less to display the content of the file flag.txt. For example, the command `cat /home/sam/flag.txt` will display the content of the file flag.txt located in /home/sam/ directory5. The screenshot below shows an example of performing these steps: ![Screenshot of performing these steps] References: Nmap Tutorial, SSH Tutorial, Find Command Tutorial, Cat Command Tutorial, [Screenshot of performing these steps]

NEW QUESTION 94

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

Answer: B

Explanation:

Capture is the Wireshark menu that Leilani has navigated in the above scenario. Wireshark is a network analysis tool that captures and displays network traffic in real-time or from saved files. Wireshark has various menus that contain different items and options for manipulating, displaying, and analyzing network data. Capture is the Wireshark menu that contains items to start, stop, restart, or save a live capture of network traffic. Capture also contains items to configure capture filters, interfaces, options, and preferences. Statistics is the Wireshark menu that contains items to display various statistics and graphs of network traffic, such as packet lengths, protocols, endpoints, conversations, etc. Main toolbar is the Wireshark toolbar that contains icons for quick access to common functions, such as opening or saving files, starting or stopping a capture, applying display filters, etc. Analyze is the Wireshark menu that contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, and configure user-specified decodes.

NEW QUESTION 95

Grace, an online shopping enthusiast, purchased a smart TV using her debit card. During online payment. Grace's browser redirected her from the e-commerce website to a third- party payment gateway, where she provided her debit card details and the OTP received on her registered mobile phone. After completing the transaction, Grace logged into her online bank account and verified the current balance in her savings account, identify the state of data being processed between the e-commerce website and payment gateway in the above scenario.

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

Answer: B

Explanation:

Data in transit is the state of data being processed between the e-commerce website and payment gateway in the above scenario. Data in transit is the data that is moving from one location to another over a network, such as the internet. Data in transit can be vulnerable to interception, modification, or theft by unauthorized parties. Therefore, data in transit should be protected using encryption, authentication, and secure protocols2. References: Data in Transit

NEW QUESTION 100

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 105

An organization divided its IT infrastructure into multiple departments to ensure secure connections for data access. To provide high-speed data access, the administrator implemented a PAID level that broke data into sections and stored them across multiple drives. The storage capacity of this RAID level was equal to the sum of disk capacities in the set. which of the following RAID levels was implemented by the administrator in the above scenario?

- A. RAID Level 0
- B. RAID Level 3
- C. RAID Level 5
- D. RAID Level 1

Answer: A

Explanation:

RAID Level 0 is the RAID level that was implemented by the administrator in the above scenario. RAID Level 0 is also known as striping, which breaks data into sections and stores them across multiple drives. RAID Level 0 provides high-speed data access and increases performance, but it does not provide any redundancy or fault tolerance. The storage capacity of RAID Level 0 is equal to the sum of disk capacities in the set. References: RAID Level 0

NEW QUESTION 110

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 112

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 115

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 118

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 121

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 125

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 212-82 Exam with Our Prep Materials Via below:

<https://www.certleader.com/212-82-dumps.html>