

Exam Questions 212-82

Certified Cybersecurity Technician(C|CT)

<https://www.2passeasy.com/dumps/212-82/>



NEW QUESTION 1

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 2

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

- A. No
- B. Yes

Answer: B

Explanation:

Yes is the answer to whether the file has been modified or not in the above scenario. A hash is a fixed-length string that is generated by applying a mathematical function, called a hash function, to a piece of data, such as a file or a message. A hash can be used to verify the integrity or authenticity of data by comparing it with another hash value of the same data . A hash value is unique and any change in the data will result in a different hash value . To compare the hash value of the original file with the leaked file and state whether the file has been modified or not, one has to follow these steps:

- ? Navigate to Hash folder in Documents of Attacker-1 machine.
 - ? Open OriginalFileHash.txt file with a text editor.
 - ? Note down the MD5 hash value of the original file as 8f14e45fceeaa167a5a36dedd4bea2543
 - ? Open Command Prompt and change directory to Hash folder using cd command.
 - ? Type certutil -hashfile Sensitiveinfo.txt MD5 and press Enter key to generate MD5 hash value of leaked file.
 - ? Note down the MD5 hash value of leaked file as 9f14e45fceeaa167a5a36dedd4bea2543
 - ? Compare both MD5 hash values.
- The MD5 hash values are different , which means that the file has been modified.

NEW QUESTION 3

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 Unknornscan 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 4

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

Identify the PCI-DSS requirement followed by Myles in the above scenario.

- A. PCI-DSS requirement no 1.3.2
- B. PCI-DSS requirement no 1.3.5

- C. PCI-DSS requirement no 5.1
- D. PCI-DSS requirement no 1.3.1

Answer: C

Explanation:

The correct answer is C, as it identifies the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS is a set of standards that aims to protect cardholder data and ensure secure payment transactions. PCI-DSS has 12 requirements that cover various aspects of security such as network configuration, data encryption, access control, vulnerability management, monitoring, and testing. PCI-DSS requirement no 5.1 states that "Protect all systems against malware and regularly update anti-virus software or programs". In the above scenario, Myles followed this requirement by installing antivirus software on each laptop to detect and protect the machines from external malicious events over the Internet. Option A is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.2 states that "Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet". In the above scenario, Myles did not follow this requirement, as there was no mention of outbound traffic or cardholder data environment. Option B is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.5 states that "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment". In the above scenario, Myles did not follow this requirement, as there was no mention of inbound or outbound traffic or cardholder data environment. Option D is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.1 states that "Implement a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data". In the above scenario, Myles did not follow this requirement, as there was no mention of firewall configuration or publicly accessible servers or system components storing cardholder data.

References: Section 5.2

NEW QUESTION 5

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 lengths³.

References: Wireshark Statistics Menu

NEW QUESTION 6

Cairo, an incident responder, was handling an incident observed in an organizational network. After performing all IH&R steps, Cairo initiated post-incident activities. He determined all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Identify the post-incident activity performed by Cairo in this scenario.

- A. Incident impact assessment
- B. Close the investigation
- C. Review and revise policies
- D. Incident disclosure

Answer: A

Explanation:

Incident impact assessment is the post-incident activity performed by Cairo in this scenario. Incident impact assessment is a post-incident activity that involves determining all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Incident impact assessment can include measuring financial losses, reputational damages, operational disruptions, legal liabilities, or regulatory penalties¹. References: Incident Impact Assessment

NEW QUESTION 7

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

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

Answer: B

Explanation:

The testing tier of a secure application development lifecycle involves checking the performance of the application on the client's network to determine whether end users are facing any issues in accessing the application. Testing is a crucial phase of software development that ensures the quality, functionality, reliability, and security of the application. Testing can be done manually or automatically using various tools and techniques, such as unit testing, integration testing, system testing, regression testing, performance testing, usability testing, security testing, and acceptance testing

NEW QUESTION 8

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 9

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 10

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 10

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 14

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 machine². References: Cookies

NEW QUESTION 15

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 problems¹.

References: Destination Unreachable Message

NEW QUESTION 20

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

Identify the type of Honeypot deployed by Karter in the above scenario.

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

Answer: A

Explanation:

A low-interaction honeypot is a type of honeypot that simulates a real OS as well as the applications and services of a target network, but only responds to pre-configured commands. It is designed to capture basic information about the attacker, such as their IP address, tools, and techniques. A low-interaction honeypot is easier to deploy and maintain than a high-interaction honeypot, which fully emulates a real system and allows the attacker to interact with it. A pure honeypot is a real system that is intentionally vulnerable and exposed to attackers. A medium-interaction honeypot is a type of honeypot that offers more functionality and interactivity than a low-interaction honeypot, but less than a high-interaction honeypot.

NEW QUESTION 25

A web application, www.moviescope.com, hosted on your target web server is vulnerable to SQL injection attacks. Exploit the web application and extract the user credentials from the moviescope database. Identify the UID (user ID) of a user, John, in the database. Note: You have an account on the web application, and your credentials are samAest.

(Practical Question)

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

Answer: B

Explanation:

4 is the UID (user ID) of a user, John, in the database in the above scenario. A web application is a software application that runs on a web server and can be accessed by users through a web browser. A web application can be vulnerable to SQL injection attacks, which are a type of web application attack that exploit 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 extract the user credentials from the moviescope database, one has to follow these steps:

? Open a web browser and type www.moviescope.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 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 30

Kaison, a forensic officer, was investigating a compromised system used for various online attacks. Kaison initiated the data acquisition process and extracted the data from the systems DVD-ROM. Which of the following types of data did Kaison acquire in the above scenario?

- A. Archival media
- B. Kernel statistics
- C. ARP cache
- D. Processor cache

Answer: A

Explanation:

Archival media is the type of data that Kaison acquired in the above scenario. Archival media is a type of data that is stored on removable media such as DVD-ROMs, CD-ROMs, tapes, or flash drives. Archival media can be used to backup or transfer data from one system to another. Archival media can be acquired using forensic tools that can read and copy the data from the media. References: Archival Media

NEW QUESTION 33

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 Theef client showing remote desktop and folder]

NEW QUESTION 37

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 controls⁴.

References: Success Audit Event

NEW QUESTION 38

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 39

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 41

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

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

Answer: A

Explanation:

NFC (Near Field Communication) is the mobile connection method that Rickson has used in the above scenario. NFC is a short-range wireless communication technology that enables devices to exchange data within a range of 10 cm. NFC employs electromagnetic induction to create a radio frequency field between two devices. NFC can also read RFID tags and establish Bluetooth connections with nearby devices to exchange information such as images and contact lists . Satcom (Satellite Communication) is a mobile connection method that uses satellites orbiting the earth to provide communication services over long distances. Cellular communication is a mobile connection method that uses cellular networks to provide voice and data services over wireless devices. ANT is a low-power wireless communication technology that enables devices to create personal area networks and exchange data over short distances.

NEW QUESTION 43

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_Tem p e
- 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 44

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 47

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 48

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 set³. References: RAID Level 0

NEW QUESTION 50

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 benefits². References: Risk Avoidance

NEW QUESTION 52

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 53

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 58

A software team at an MNC was involved in a project aimed at developing software that could detect the oxygen levels of a person without physical contact, a helpful solution for pandemic situations. For this purpose, the team used a wireless technology that could digitally transfer data between two devices within a short range of up to 5 m and only worked in the absence of physical blockage or obstacle between the two devices, identify the technology employed by the software team in the above scenario.

- A. Infrared
- B. USB
- C. CPS
- D. Satcom

Answer: A

Explanation:

Infrared is a wireless technology that can digitally transfer data between two devices within a short range of up to 5 m and only works in the absence of physical blockage or obstacle between the two devices. Infrared is commonly used for remote controls, wireless keyboards, and medical devices.

References: Infrared Technology

NEW QUESTION 62

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 65

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 212-82 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 212-82 Product From:

<https://www.2passeasy.com/dumps/212-82/>

Money Back Guarantee

212-82 Practice Exam Features:

- * 212-82 Questions and Answers Updated Frequently
- * 212-82 Practice Questions Verified by Expert Senior Certified Staff
- * 212-82 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 212-82 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year