Free Questions for PCCET by braindumpscollection

Shared by Deleon on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Organizations that transmit, process, or store payment-card information must comply with what standard?

Options:

A- HIPAA

B- CISA

C- GDPR

D- PCI DSS

Answer:

D

Explanation:

PCI DSS stands for Payment Card Industry Data Security Standard, which is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment1. The standard is administered by the Payment Card Industry Security Standards Council, and its use is mandated by the major card brands2. PCI DSS covers 12

requirements for compliance, organized into six control objectives, such as building and maintaining a secure network and systems, protecting cardholder data, and implementing strong access control measures3. Reference: Payment Card Industry Security Standards, PCI Security Standards Council -- Protect Payment Data with Industry-driven Security Standards, Training, and Programs, What is PCI Compliance? 12 Requirements & More - Digital Guardian

Question 2

Question Type: MultipleChoice

At which layer of the OSI model are routing protocols defined?

Options:

A- Network

B- Physical

C- Transport

D- Data Link

Answer:

A

Explanation:

Routing protocols are defined at the network layer (Layer 3) of the OSI model. The network layer is responsible for routing packets across different networks using logical addresses (IP addresses). Routing protocols are used to exchange routing information between routers and to determine the best path for data delivery. Some examples of routing protocols are BGP, OSPF, RIP, and EIGRP. Palo Alto Networks devices support advanced routing features using the Advanced Routing Engine1. Reference: Advanced Routing - Palo Alto Networks | TechDocs, What Is Layer 7? - Palo Alto Networks, How to Configure Routing Information Protocol (RIP)

Question 3

Question Type: **MultipleChoice**

What are two disadvantages of Static Rout ng? (Choose two.)

Options:

A- Manual reconfiguration

B- Requirement for additional computational resources

C- Single point of failure

D- Less security

Answer:

A, C

Explanation:

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic 1. Static routing has some advantages, such as simplicity, low overhead, and full control, but it also has some disadvantages, such as:

* Manual reconfiguration: Static routes require manual effort to configure and maintain. This can be time-consuming and error-prone, especially in large networks with many routes. If there is a change in the network topology or a link failure, the static routes need to be updated manually by the network administrator 23.

* Single point of failure: Static routing is not fault tolerant. This means that if the path used by the static route stops working, the traffic will not be rerouted automatically. The network will be unreachable until the failure is repaired or the static route is changed manually. Dynamic routing, on the other hand, can adapt to network changes and find alternative paths 23.

Question 4

Question Type: MultipleChoice

Layer 4 of the TCP/IP Model corresponds to which three Layer(s) of the OSI Model? (Choose three.)

Options:

A- Network

B- Application

C- Session

D- Transport

E- Presentation

Answer:

C, D, E

Explanation:

Layer 4 of the TCP/IP model is the transport layer, which is responsible for providing reliable and efficient data transmission between hosts. The transport layer can use different protocols, such as TCP or UDP, depending on the requirements of the application. The

transport layer also performs functions such as segmentation, acknowledgement, flow control, and error recovery. 1

The transport layer of the TCP/IP model corresponds to three layers of the OSI model: the transport layer, the session layer, and the presentation layer. The session layer of the OSI model manages the establishment, maintenance, and termination of sessions between applications. The session layer also provides services such as synchronization, dialogue control, and security. The presentation layer of the OSI model handles the representation, encoding, and formatting of data for the application layer. The presentation layer also performs functions such as compression, encryption, and translation. 23

* 1: TCP/IP Model - GeeksforGeeks

* 2: Transport Layer | Layer 4 | The OSI-Model

* 3: Transport Layer Explanation -- Layer 4 of the OSI Model

Question 5

Question Type: **MultipleChoice**

Which internet of things (loT) connectivity technology operates on the 2.4GHz and 5GHz bands, as well as all bands between 1 and 6GHz when they become available for 802.11 use. at ranges up to 11 Gbit/s?

Options:

A- 3G

B- Z-wave

C- 802.11ax

D- C-band

Answer:

C

Explanation:

802.11ax, also known as Wi-Fi 6, is an internet of things (IoT) connectivity technology that operates on the 2.4GHz and 5GHz bands, as well as all bands between 1 and 6GHz when they become available for 802.11 use, at ranges up to 11 Gbit/s. 802.11ax is designed to improve the performance, efficiency, and capacity of wireless networks, especially in high-density environments such as smart homes, smart cities, and industrial IoT. 802.11ax uses various techniques such as orthogonal frequency division multiple access (OFDMA), multi-user multiple input multiple output (MU-MIMO), target wake time (TWT), and 1024 quadrature amplitude modulation (QAM) to achieve higher data rates, lower latency, longer battery life, and reduced interference for IoT devices. Reference:

* Wi-Fi 6 (802.11ax) - Palo Alto Networks

* What is Wi-Fi 6? | Wi-Fi 6 Features and Benefits | Cisco

* What is Wi-Fi 6 (802.11ax)? - Definition from WhatIs.com

Question 6

Question Type: MultipleChoice

Which of these ports is normally associated with HTTPS?

Options:

A- 443

B- 5050

C- 25

D- 80

Answer:

A

Explanation:

HTTPS is a protocol that encrypts and secures the communication between web browsers and servers. HTTPS uses SSL or TLS certificates to establish a secure connection and prevent unauthorized access or tampering of data. HTTPS typically uses port 443, which is the default port for HTTPS connections. Port 443 is different from port 80, which is the default port for HTTP connections. HTTP is an unencrypted and insecure protocol that can expose sensitive information or allow malicious attacks. Port 443 is also different from port 5050, which is a common port for some applications or services, such as Yahoo Messenger or SIP. Port 5050 is not associated with HTTPS and does not provide any encryption or security. Port 443 is also different from port 25, which is the default port for SMTP, the protocol used for sending and receiving emails. Port 25 is not associated with HTTPS and does not encrypt the email content or headers. Reference:

* Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) - Palo Alto Networks

* HTTPS Protocol: What is the Default Port for SSL & Common TCP Ports

* What is HTTPS? | Cloudflare

* Can I use another port other than 443 for HTTPS/SSL communication?

Question 7

Question Type: **MultipleChoice**

Which action must Secunty Operations take when dealing with a known attack?

Options:

A- Document, monitor, and track the incident.

B- Limit the scope of who knows about the incident.

C- Increase the granularity of the application firewall.

D- Disclose details of lhe attack in accordance with regulatory standards.

Answer:

A

Explanation:

Security Operations (SecOps) is the process of coordinating and aligning security teams and IT teams to improve the security posture of an organization. SecOps involves implementing and maintaining security controls, technologies, policies, and procedures to protect the organization from cyber threats and incidents. When dealing with a known attack, SecOps must take the following action: document, monitor, and track the incident. This action is important because it helps SecOps to:

* Record the details of the attack, such as the source, target, impact, timeline, and response actions.

* Monitor the status and progress of the incident response and recovery efforts, as well as the ongoing threat activity and indicators of compromise.

* Track the performance and effectiveness of the security controls and technologies, as well as the lessons learned and improvement opportunities. Reference:

* Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)

* 6 Incident Response Steps to Take After a Security Event - Exabeam

* Dealing with Cyber Attacks--Steps You Need to Know | NIST

Question 8

Question Type: MultipleChoice

What type of address translation does a NAT perform?

Options:

A- Private to public

B- Logical to physical

C- Physical Io logical

D- Public to private

Answer:

A

Explanation:

NAT stands for Network Address Translation, which is a process that allows devices on a private network to communicate with devices on a public network, such as the Internet. NAT translates the private IP addresses of the devices on the private network to public IP addresses that can be routed on the public network. This way, multiple devices on the private network can share a single public IP address and access the Internet. NAT also provides security benefits, as it hides the internal network structure and IP addresses from the outside world. Reference: Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET), Fundamentals of Network Security, Network Address Translation (NAT)

Question 9

Question Type: **MultipleChoice**

The seventy of an attack needs to be escalated.

What needs to be in place in order for the security operations team to properly inform various units within the enterprise of the issue?

Options:

A- Interface Agreement

B- FAO Incident Site ---

C- Corporate Executive Listserv

D- Security Breach Blog

Answer:

A

Question 10

Question Type: **MultipleChoice**

What is the ptrpose of automation in SOAR?

Options:

A- To provide consistency in response to security issues

B- To give only administrators the ability to view logs

C- To allow easy manual entry of changes to security templates

D- To complicate programming for system administration -

Answer:

A

Explanation:

Automation in SOAR (Security Orchestration, Automation, and Response) is the process of programming tasks, alerts, and responses to security incidents so that they can be executed without human intervention. Automation in SOAR helps security teams to handle the huge amount of information generated by various security tools, analyze it through machine learning processes, and take appropriate actions based on predefined rules and workflows. Automation in SOAR also reduces the manual effort and time required for security operations, improves the accuracy and efficiency of threat detection and response, and provides consistency in handling security issues across different environments and scenarios. Reference: What is SOAR (security orchestration, automation and response)? | IBM, What Is SOAR? Technology and Solutions | Microsoft Security, Security orchestration - Wikipedia.