



Free Questions for PCCET by actualtestdumps

Shared by Bond on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two statements describe the Jasager attack? (Choose two.)

Options:

- A- The victim must manually choose the attacker's access point
- B- It actively responds to beacon requests.
- C- It tries to get victims to connect at random.
- D- The attacker needs to be within close proximity of the victim.

Answer:

B, D

Explanation:

A Jasager attack is a type of wireless man-in-the-middle attack that exploits the way mobile devices search for known wireless networks. A Jasager device will respond to any beacon request from a mobile device by saying "Yes, I'm here", pretending to be one of the preferred networks. This way, the Jasager device can trick the mobile device into connecting to it, without the user's knowledge or

consent. The Jigsaw device can then intercept, modify, or redirect the traffic of the victim. For this attack to work, the attacker needs to be within close proximity of the victim, and the victim must have at least one known network in their preferred list. The victim does not need to manually choose the attacker's access point, nor does the attacker try to get victims to connect at random. Reference: Wireless Man in the Middle - Palo Alto Networks, Man-in-the-middle attacks with malicious & rogue Wi-Fi access points - Privacy Guides

Question 2

Question Type: MultipleChoice

Which VM-Series virtual firewall cloud deployment use case reduces your environment's attack surface?

Options:

- A- O Multicloud
- B- O 5G -
- C- Micro-segmentation
- D- DevOps

Answer:

C

Explanation:

Micro-segmentation is a VM-Series virtual firewall cloud deployment use case that reduces your environment's attack surface. Micro-segmentation is the process of dividing a network into smaller segments, each with its own security policies and controls. This helps to isolate and protect workloads from lateral movement and unauthorized access, as well as to enforce granular trust zones and application dependencies. Micro-segmentation can be applied to virtualized data centers, private clouds, and public clouds, using software-defined solutions such as VMware NSX, Cisco ACI, and Azure Virtual WAN. Reference: Micro-Segmentation - Palo Alto Networks, VM-Series Deployment Guide - Palo Alto Networks, VM-Series on VMware NSX - Palo Alto Networks, VM-Series on Cisco ACI - Palo Alto Networks, VM-Series on Azure Virtual WAN - Palo Alto Networks

Question 3

Question Type: MultipleChoice

How does Cortex XSOAR Threat Intelligence Management (TIM) provide relevant threat data to analysts?

Options:

- A-** It creates an encrypted connection to the company's data center.
- B-** It performs SSL decryption to give visibility into user traffic.
- C-** It prevents sensitive data from leaving the network.
- D-** It automates the ingestion and aggregation of indicators.

Answer:

D

Explanation:

Cortex XSOAR Threat Intelligence Management (TIM) is a platform that enables security teams to manage the lifecycle of threat intelligence, from aggregation to action. One of the key features of Cortex XSOAR TIM is that it automates the ingestion and aggregation of indicators from various sources, such as threat feeds, open-source intelligence, internal data, and third-party integrations 1. Indicators are pieces of information that can be used to identify malicious activity, such as IP addresses, domains, URLs, hashes, etc. By automating the ingestion and aggregation of indicators, Cortex XSOAR TIM reduces the manual effort and time required to collect, validate, and prioritize threat data. It also enables analysts to have a unified view of the global threat landscape and the impact of threats on their network 1. Reference: 1: Threat Intelligence Management - Palo Alto Networks 2

Question 4

Question Type: MultipleChoice

What protocol requires all routers in the same domain to maintain a map of the network?

Options:

- A- EIGRP
- B- Static
- C- RIP
- D- OSPF

Answer:

D

Explanation:

OSPF is a link-state routing protocol that requires all routers in the same domain to maintain a map of the network. This map is called the link-state database (LSDB) and it contains information about the topology and the state of each link. Each router independently calculates the shortest path to every destination in the network using the Dijkstra algorithm. OSPF routers exchange routing information by flooding link-state advertisements (LSAs) to their neighbors. LSAs are acknowledged by the receivers to ensure reliable delivery¹². Reference:

Question 5

Question Type: MultipleChoice

On which security principle does virtualization have positive effects?

Options:

A- integrity

B- confidentiality

C- availability

D- non-repudiation

Answer:

C

Explanation:

Virtualization improves the availability of IT systems and resources by enabling features such as:

Resource optimization: Virtualization allows multiple virtual instances to share the same physical infrastructure, reducing hardware costs and increasing resource utilization.

Scalability: Virtualization enables rapid provisioning and deprovisioning of virtual instances, allowing organizations to scale up or down their IT capacity according to demand.

Disaster recovery: Virtualization facilitates backup and replication of virtual instances, allowing organizations to restore their IT systems and data in the event of a disaster or outage.

Fault tolerance: Virtualization supports high availability and load balancing of virtual instances, ensuring that IT systems and services remain operational even if one or more virtual instances fail.
Reference: [Virtualization Benefits: How Virtualization Improves Efficiency and Security | VMware](#), [Virtualization Security - A Complete Guide - CyberExperts.com](#)

Question 6

Question Type: MultipleChoice

What differentiates Docker from a bare metal hypervisor?

Options:

- A- Docker lets the user boot up one or more instances of an operating system on the same host whereas hypervisors do not
- B- Docker uses more resources than a bare metal hypervisor
- C- Docker is more efficient at allocating resources for legacy systems
- D- Docker uses OS-level virtualization, whereas a bare metal hypervisor runs independently from the OS

Answer:

D

Explanation:

Docker and bare metal hypervisor are two different types of virtualization technologies that have different functioning mechanisms, architectures, and use cases. Docker is a containerization technology that allows users to create, deploy, and run applications using containers. Containers are isolated environments that share the same host operating system kernel, but have their own libraries, dependencies, and resources. Docker can run multiple containers on the same host, without requiring a separate operating system for each container¹². Bare metal hypervisor, also known as type 1 hypervisor, is a software that runs directly on the hardware and creates virtual machines. Virtual machines are complete operating systems that have their own kernel, drivers, and resources. Bare metal hypervisor can run multiple virtual machines on the same host, each with a different operating system and dedicated resources³.

The main difference between Docker and bare metal hypervisor is the level of abstraction they provide. Docker uses OS-level virtualization, which means it creates containers on top of the host operating system. Bare metal hypervisor uses hardware virtualization, which means it runs independently from the host operating system and creates virtual machines on the hardware layer. This difference has implications for the performance, efficiency, and portability of the virtualized environments. Docker containers are generally faster, lighter, and more scalable than virtual machines, as they do not have the overhead of running a separate operating system for each container. However, Docker containers are more limited and can run only on Linux, certain Windows servers and IBM mainframes if hosted on bare metal. Virtual machines, on the other hand, are more flexible and secure, as they can run any operating system and isolate the guest operating system from the host operating system. However, virtual machines are more resource-intensive and slower than containers, as they have to emulate the hardware and run a full operating system for each virtual machine¹².

[Docker vs VMWare: How Do They Stack Up? | UpGuard](#)

[Hypervisor vs. Docker: Complete Comparison of the Two - HitechNectar](#)

[Beginners Track - Docker On Bare Metal | dockerlabs](#)

[\[Getting Started: Layer 3 Subinterfaces - Palo Alto Networks Knowledge Base\]](#)

Question 7

Question Type: MultipleChoice

Based on how much is managed by the vendor, where can CaaS be situated in the spread of cloud computing services?

Options:

- A- between PaaS and FaaS
- B- between IaaS and PaaS
- C- between On-Prem and IaaS
- D- between FaaS and Serverless

Answer:

B

Explanation:

CaaS, or Containers-as-a-Service, is a cloud service that allows users to manage and deploy applications using containers and clusters. CaaS can be situated between IaaS and PaaS in the spread of cloud computing services, based on how much is managed by the vendor. IaaS, or Infrastructure-as-a-Service, provides the lowest level of abstraction, where users have to manage the servers, storage, network, and operating system. PaaS, or Platform-as-a-Service, provides a higher level of abstraction, where users only have to manage the application code and data. FaaS, or Function-as-a-Service, provides the highest level of abstraction, where users only have to manage the functions or logic of the application. CaaS falls in between IaaS and PaaS, as it provides users with more control over the container orchestration and configuration than PaaS, but also simplifies the infrastructure management and scaling than IaaS.¹²³Reference:

[What is CaaS?from Red Hat](#)

[Containers as a Servicefrom Atlassian](#)

[Container as a Service \(CaaS\)from GeeksforGeeks](#)

Question 8

Question Type: MultipleChoice

Which element of the security operations process is concerned with using external functions to help achieve goals?

Options:

A- interfaces

B- business

C- technology

D- people

Answer:

A

Explanation:

The six pillars include:

1. Business (goals and outcomes)
2. People (who will perform the work)
3. Interfaces (external functions to help achieve goals)
4. Visibility (information needed to accomplish goals)
5. Technology (capabilities needed to provide visibility and enable people)
6. Processes (tactical steps required to execute on goals)

Question 9

Question Type: MultipleChoice

What is a characteristic of the National Institute Standards and Technology (NIST) defined cloud computing model?

Options:

- A- requires the use of only one cloud service provider
- B- enables on-demand network services
- C- requires the use of two or more cloud service providers
- D- defines any network service

Answer:

B

Explanation:

According to the NIST definition, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction¹. One of the essential characteristics of cloud computing is on-demand self-service, which means that users can request and obtain computing resources as needed, without requiring human intervention from the service provider². On-demand network services are an example of this characteristic, as they allow users to access network resources such as bandwidth, routing, firewall, or load balancing, on demand and in a scalable manner³. Reference:

[The NIST definition of cloud computing](#)

[SP 800-145, The NIST Definition of Cloud Computing | CSRC](#)

[On-Demand Network Services - Palo Alto Networks](#)

To Get Premium Files for PCCET Visit

<https://www.p2pexams.com/products/pccet>

For More Free Questions Visit

<https://www.p2pexams.com/palo-alto-networks/pdf/pccet>

