

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

<https://www.2passeasy.com/dumps/PCCET/>



NEW QUESTION 1

Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

- A. Dynamic
- B. Pre-exploit protection
- C. Bare-metal
- D. Static

Answer: A

NEW QUESTION 2

Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

- A. North-South traffic
- B. Intrazone traffic
- C. East-West traffic
- D. Interzone traffic

Answer: A

NEW QUESTION 3

Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

- A. MineMeld
- B. AutoFocus
- C. WildFire
- D. Cortex XDR

Answer: D

NEW QUESTION 4

Which technique changes protocols at random during a session?

- A. use of non-standard ports
- B. port hopping
- C. hiding within SSL encryption
- D. tunneling within commonly used services

Answer: B

NEW QUESTION 5

What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

- A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
- B. control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)
- C. control and protect inter-host traffic by using IPv4 addressing
- D. control and protect inter-host traffic using physical network security appliances

Answer: D

NEW QUESTION 6

Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?

- A. Global Protect
- B. WildFire
- C. AutoFocus
- D. STIX

Answer: C

NEW QUESTION 7

Which key component is used to configure a static route?

- A. router ID
- B. enable setting
- C. routing protocol
- D. next hop IP address

Answer: D

NEW QUESTION 8

Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to

websites and to protect your organization from websites hosting malware and phishing pages?

- A. Threat Prevention
- B. DNS Security
- C. WildFire
- D. URL Filtering

Answer: D

NEW QUESTION 9

Which Palo Alto Networks tool is used to prevent endpoint systems from running malware executables such as viruses, trojans, and rootkits?

- A. Expedition
- B. Cortex XDR
- C. AutoFocus
- D. App-ID

Answer: B

NEW QUESTION 10

What does SIEM stand for?

- A. Security Infosec and Event Management
- B. Security Information and Event Management
- C. Standard Installation and Event Media
- D. Secure Infrastructure and Event Monitoring

Answer: B

NEW QUESTION 10

DRAG DROP

Match the IoT connectivity description with the technology.

a proprietary multicast wireless sensor network technology primarily used in personal wearables		Bluetooth (BLE)
a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology		802.11
a wireless protocol defined by the Institute of Electrical and Electronics Engineers (IEEE)		Adaptive Network Technology (ANT+)
a low-energy wireless mesh network protocol primarily used for home automation applications		Z-Wave

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

a proprietary multicast wireless sensor network technology primarily used in personal wearables	a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology	Bluetooth (BLE)
a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology	a wireless protocol defined by the Institute of Electrical and Electronics Engineers (IEEE)	802.11
a wireless protocol defined by the Institute of Electrical and Electronics Engineers (IEEE)	a proprietary multicast wireless sensor network technology primarily used in personal wearables	Adaptive Network Technology (ANT+)
a low-energy wireless mesh network protocol primarily used for home automation applications	a low-energy wireless mesh network protocol primarily used for home automation applications	Z-Wave

NEW QUESTION 12

Which option is an example of a North-South traffic flow?

- A. Lateral movement within a cloud or data center
- B. An internal three-tier application
- C. Client-server interactions that cross the edge perimeter
- D. Traffic between an internal server and internal user

Answer: C

NEW QUESTION 14

Which option describes the “selective network security virtualization” phase of incrementally transforming data centers?

- A. during the selective network security virtualization phase, all intra-host communication paths are strictly controlled
- B. during the selective network security virtualization phase, all intra-host traffic is forwarded to a Web proxy server
- C. during the selective network security virtualization phase, all intra-host traffic is encapsulated and encrypted using the IPSEC protocol
- D. during the selective network security virtualization phase, all intra-host traffic is load balanced

Answer: A

NEW QUESTION 18

Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?

- A. UDP
- B. MAC
- C. SNMP
- D. NFS

Answer: C

NEW QUESTION 19

Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of its servers. The infiltration by hackers was attributed to which type of vulnerability?

- A. an intranet-accessed contractor’s system that was compromised
- B. exploitation of an unpatched security vulnerability
- C. access by using a third-party vendor’s password
- D. a phishing scheme that captured a database administrator’s password

Answer: D

NEW QUESTION 24

In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?

- A. Cortex XDR
- B. AutoFocus
- C. MineMild
- D. Cortex XSOAR

Answer: A

NEW QUESTION 29

On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

- A. operating system patches
- B. full-disk encryption
- C. periodic data backups
- D. endpoint-based firewall

Answer: B

NEW QUESTION 34

Which option is a Prisma Access security service?

- A. Compute Security
- B. Firewall as a Service (FWaaS)
- C. Virtual Private Networks (VPNs)
- D. Software-defined wide-area networks (SD-WANs)

Answer: B

NEW QUESTION 35

Which item accurately describes a security weakness that is caused by implementing a “ports first” data security solution in a traditional data center?

- A. You may have to use port numbers greater than 1024 for your business-critical applications.
- B. You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter.
- C. You may not be able to assign the correct port to your business-critical applications.
- D. You may not be able to open up enough ports for your business-critical applications which will increase the attack surface area.

Answer: B

NEW QUESTION 39

Which statement describes DevOps?

- A. DevOps is its own separate team
- B. DevOps is a set of tools that assists the Development and Operations teams throughout the software delivery process
- C. DevOps is a combination of the Development and Operations teams
- D. DevOps is a culture that unites the Development and Operations teams throughout the software delivery process

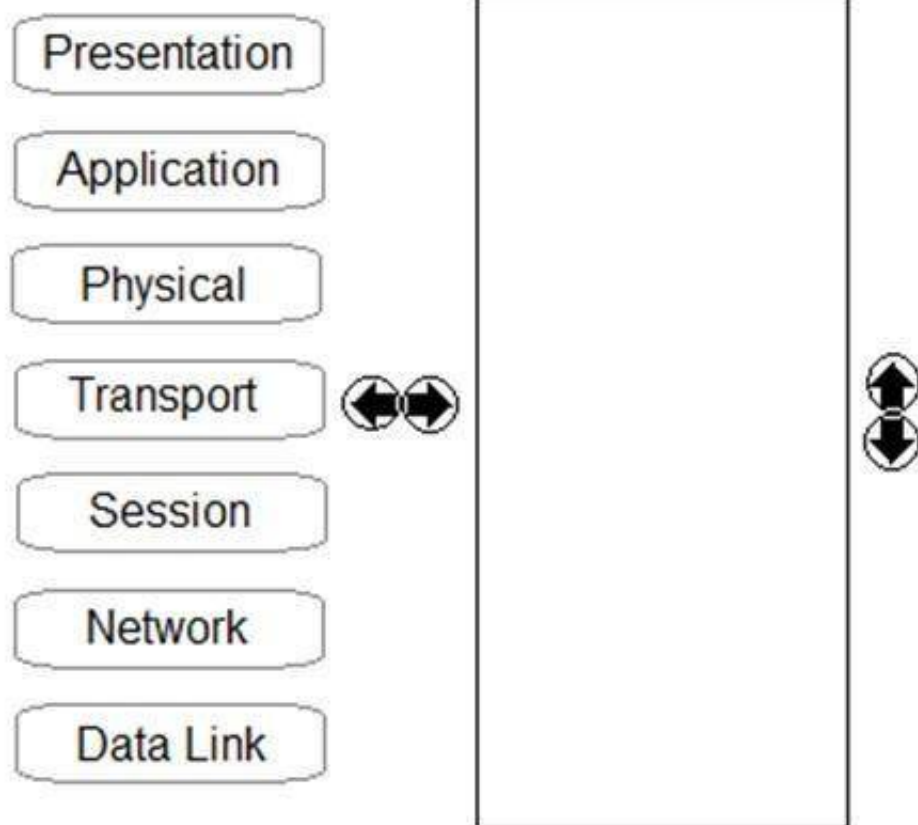
Answer: B

NEW QUESTION 43

DRAG DROP

Order the OSI model with Layer7 at the top and Layer1 at the bottom.

Unordered Options Ordered Options

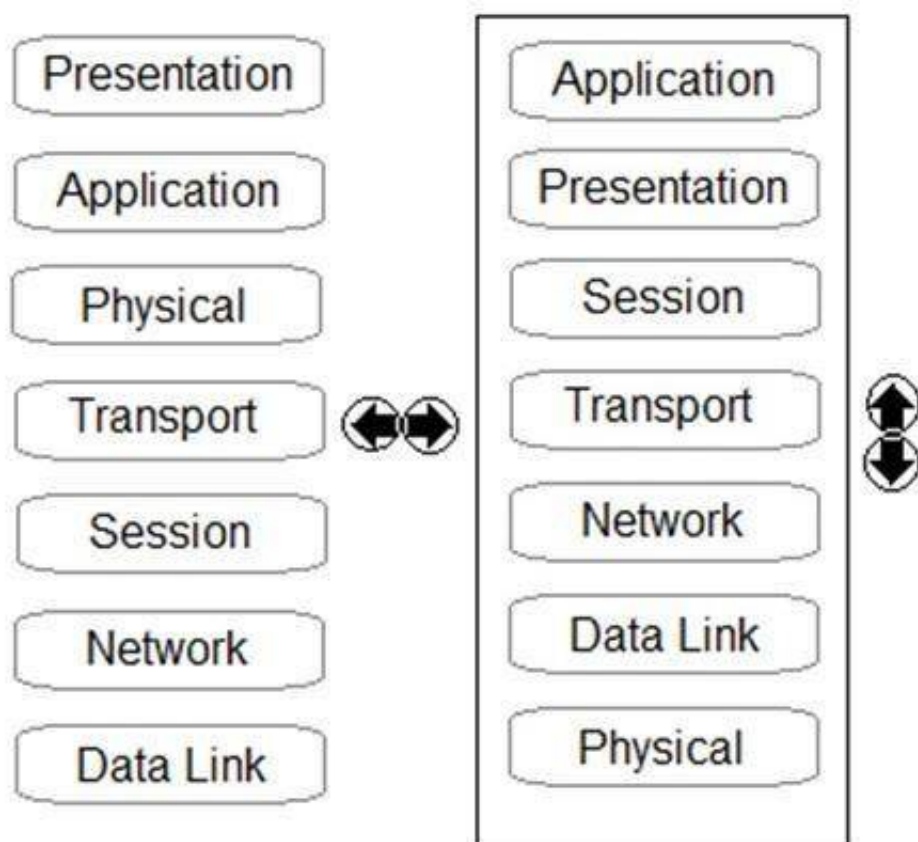


- A. Mastered
- B. Not Mastered

Answer: A

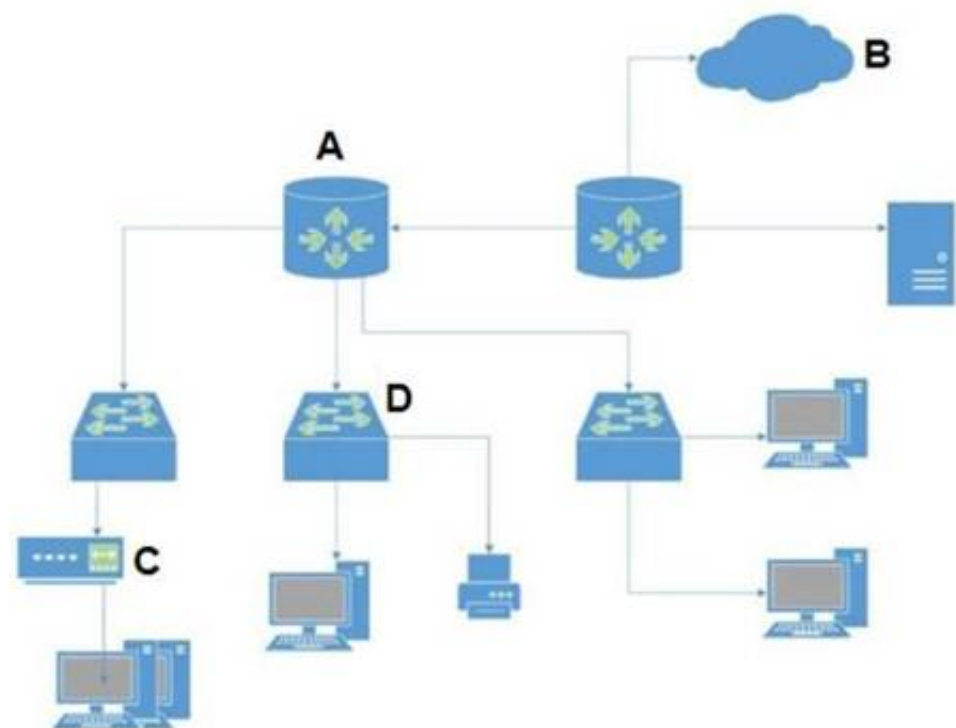
Explanation:

Unordered Options Ordered Options



NEW QUESTION 47

In the attached network diagram, which device is the switch?



- A. A
- B. B
- C. C
- D. D

Answer: D

NEW QUESTION 48

In SecOps, what are two of the components included in the identify stage? (Choose two.)

- A. Initial Research
- B. Change Control
- C. Content Engineering
- D. Breach Response

Answer: AC

NEW QUESTION 53

Which IoT connectivity technology is provided by satellites?

- A. 4G/LTE
- B. VLF
- C. L-band
- D. 2G/2.5G

Answer: C

NEW QUESTION 55

What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?

- A. run a static analysis
- B. check its execution policy
- C. send the executable to WildFire
- D. run a dynamic analysis

Answer: B

NEW QUESTION 57

An Administrator wants to maximize the use of a network address. The network is 192.168.6.0/24 and there are three subnets that need to be created that can not overlap. Which subnet would you use for the network with 120 hosts?

Requirements for the three subnets:

Subnet 1: 3 host addresses

Subnet 2: 25 host addresses

Subnet 3: 120 host addresses

- A. 192.168.6.168/30
- B. 192.168.6.0/25
- C. 192.168.6.160/29
- D. 192.168.6.128/27

Answer: B

NEW QUESTION 60

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCCET Exam Questions With Answers.

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

<https://www.2passeasy.com/dumps/PCCET/>

Money Back Guarantee

PCCET Practice Exam Features:

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