

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

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



NEW QUESTION 1

Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

- A. SaaS
- B. DaaS
- C. PaaS
- D. IaaS

Answer: D

NEW QUESTION 2

Which of the following is a service that allows you to control permissions assigned to users in order for them to access and utilize cloud resources?

- A. User-ID
- B. Lightweight Directory Access Protocol (LDAP)
- C. User and Entity Behavior Analytics (UEBA)
- D. Identity and Access Management (IAM)

Answer: D

Explanation:

Identity and access management (IAM) is a software service or framework that allows organizations to define user or group identities within software environments, then associate permissions with them. The identities and permissions are usually spelled out in a text file, which is referred to as an IAM policy.

NEW QUESTION 3

In which situation would a dynamic routing protocol be the quickest way to configure routes on a router?

- A. the network is large
- B. the network is small
- C. the network has low bandwidth requirements
- D. the network needs backup routes

Answer: A

Explanation:

A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can't be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can't be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn't broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

NEW QUESTION 4

In which phase of the cyberattack lifecycle do attackers establish encrypted communication channels back to servers across the internet so that they can modify their attack objectives and methods?

- A. exploitation
- B. actions on the objective
- C. command and control
- D. installation

Answer: C

Explanation:

Command and Control: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

NEW QUESTION 5

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: D

Explanation:

DevOps is not:

A combination of the Dev and Ops teams: There still are two teams; they just operate in a communicative, collaborative way.

Its own separate team: There is no such thing as a "DevOps engineer." Although some companies may appoint a "DevOps team" as a pilot when trying to transition to a DevOps culture, DevOps refers to a culture where developers, testers, and operations personnel cooperate throughout the entire software delivery lifecycle.

A tool or set of tools: Although there are tools that work well with a DevOps model or help promote DevOps culture, DevOps ultimately is a strategy, not a tool.

Automation: Although automation is very important for a DevOps culture, it alone does not define DevOps.

NEW QUESTION 6

A native hypervisor runs:

- A. with extreme demands on network throughput
- B. only on certain platforms
- C. within an operating system's environment
- D. directly on the host computer's hardware

Answer: D

Explanation:

Type 1 (native or bare metal). Runs directly on the host computer's hardware Type 2 (hosted). Runs within an operating system environment

NEW QUESTION 7

Match each description to a Security Operating Platform key capability.

understanding the full context of attacks on a network		detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications		provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack		prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people		reduce the attack surface area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reduce the attack surface: Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility.

Prevent all known threats, fast: A coordinated security platform accounts for the full scope of an attack across the various security controls that compose the security posture, thus enabling organizations to quickly identify and block known threats.

Detect and prevent new, unknown threats with automation: Security that simply detects threats and requires a manual response is too little, too late. Automated creation and

delivery of near-real-time protections against new threats to the various security solutions in the organization's environments enable dynamic policy updates.

These updates are

designed to allow enterprises to scale defenses with technology, rather than people.

NEW QUESTION 8

What is the key to "taking down" a botnet?

- A. prevent bots from communicating with the C2
- B. install openvas software on endpoints
- C. use LDAP as a directory service
- D. block Docker engine software on endpoints

Answer: A

NEW QUESTION 9

In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

- A. weaponization
- B. reconnaissance
- C. exploitation
- D. delivery

Answer: A

Explanation:

"Weaponization: Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message."

NEW QUESTION 10

Which core component is used to implement a Zero Trust architecture?

- A. VPN Concentrator
- B. Content Identification
- C. Segmentation Platform
- D. Web Application Zone

Answer: C

Explanation:

"Remember that a trust zone is not intended to be a "pocket of trust" where systems (and therefore threats) within the zone can communicate freely and directly with each other. For a full Zero Trust implementation, the network would be configured to ensure that all communications traffic, including traffic between devices in the same zone, is intermediated by the corresponding Zero Trust Segmentation Platform."

NEW QUESTION 10

From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

- A. Unit 52
- B. PAN-DB
- C. BrightCloud
- D. MineMeld

Answer: B

Explanation:

When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into about 65 categories.

NEW QUESTION 11

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

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

Answer: C

Explanation:

Application (Layer 7 or L7): This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication.

Presentation (Layer 6 or L6): This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system.

Session (Layer 5 or L5): This layer manages communication sessions (service requests and service responses) between networked systems, including connection establishment, data transfer, and connection release.

Transport (Layer 4 or L4): This layer provides transparent, reliable data transport and end-to-end transmission control.

NEW QUESTION 12

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 16

Which option would be an example of PII that you need to prevent from leaving your enterprise network?

- A. Credit card number
- B. Trade secret
- C. National security information
- D. A symmetric encryption key

Answer: A

NEW QUESTION 18

Systems that allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows are known as what?

- A. XDR
- B. STEP
- C. SOAR
- D. SIEM

Answer: C

NEW QUESTION 23

Which endpoint product from Palo Alto Networks can help with SOC visibility?

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

Answer: B

Explanation:

XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can:

Identify hidden, stealthy, and sophisticated threats proactively and quickly Track threats across any source or location within the organization Increase the productivity of the people operating the technology
Get more out of their security investments Conclude investigations more efficiently

NEW QUESTION 27

Which endpoint tool or agent can enact behavior-based protection?

- A. AutoFocus
- B. Cortex XDR
- C. DNS Security
- D. MineMeld

Answer: B

NEW QUESTION 30

Which type of Software as a Service (SaaS) application provides business benefits, is fast to deploy, requires minimal cost and is infinitely scalable?

- A. Benign
- B. Tolerated
- C. Sanctioned
- D. Secure

Answer: C

NEW QUESTION 35

Which three services are part of Prisma SaaS? (Choose three.)

- A. Data Loss Prevention
- B. DevOps
- C. Denial of Service
- D. Data Exposure Control
- E. Threat Prevention

Answer: ADE

NEW QUESTION 38

Which pillar of Prisma Cloud application security does vulnerability management fall under?

- A. dynamic computing
- B. identity security
- C. compute security
- D. network protection

Answer: C

Explanation:

Prisma Cloud comprises four pillars:

Visibility, governance, and compliance. Gain deep visibility into the security posture of multicloud environments. Track everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.

Compute security. Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your integrated development environment (IDE), software configuration management (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.

Network protection. Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.

Identity security. Monitor and leverage user and entity behavior analytics (UEBA) across your environments to detect and block malicious actions. Gain visibility into and enforce governance p

NEW QUESTION 43

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 46

How does adopting a serverless model impact application development?

- A. costs more to develop application code because it uses more compute resources
- B. slows down the deployment of application code, but it improves the quality of code development
- C. reduces the operational overhead necessary to deploy application code
- D. prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code

Answer: C

Explanation:

List three advantages of serverless computing over

CaaS: - Reduce costs - Increase agility - Reduce operational overhead

NEW QUESTION 50

On an endpoint, which method should you use to secure applications against exploits?

- A. endpoint-based firewall
- B. strong user passwords
- C. full-disk encryption
- D. software patches

Answer: D

Explanation:

New software vulnerabilities and exploits are discovered all the time and thus diligent software patch management is required by system and security administrators in every organization.

NEW QUESTION 55

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 57

Which type of malware takes advantage of a vulnerability on an endpoint or server?

- A. technique
- B. patch
- C. vulnerability
- D. exploit

Answer: A

NEW QUESTION 62

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

Explanation:

In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect.

NEW QUESTION 64

SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)

- A. People
- B. Accessibility

- C. Processes
- D. Understanding
- E. Business

Answer: ACE

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)

All elements must tie back to the business itself and the goals of the security operations

NEW QUESTION 69

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

Explanation:

page 211 "Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment: ... This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus."

NEW QUESTION 71

Which subnet does the host 192.168.19.36/27 belong?

- A. 192.168.19.0
- B. 192.168.19.16
- C. 192.168.19.64
- D. 192.168.19.32

Answer: D

NEW QUESTION 72

Which type of Wi-Fi attack depends on the victim initiating the connection?

- A. Evil twin
- B. Jager
- C. Parager
- D. Mirai

Answer: A

Explanation:

Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with "free Wi-Fi access." The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can't easily target a specific victim, because the attack depends on the victim initiating the connection.

<https://www.paloaltonetworks.com/blog/2013/11/wireless-man-middle/>

NEW QUESTION 73

When signature-based antivirus software detects malware, what three things does it do to provide protection? (Choose three.)

- A. decrypt the infected file using base64
- B. alert system administrators
- C. quarantine the infected file
- D. delete the infected file
- E. remove the infected file's extension

Answer: CDE

NEW QUESTION 75

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:

Short-range wireless:

Adaptive Network Technology+ (ANT+): ANT+ is a proprietary multicast wireless sensor network technology primarily used in personal wearables, such as sports and fitness sensors.

Bluetooth/Bluetooth Low-Energy (BLE): Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. BLE (also known as Bluetooth Smart or Bluetooth 4.0+) devices consume significantly less power than Bluetooth devices and can access the internet directly through 6LoWPAN connectivity.

Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN): 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications that require wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters.

Wi-Fi/802.11: The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. The most common implementations today include:

* 802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54Mbps to 600Mbps

* 802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbps to 3.46 Gbps

* 802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (and all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbps

Z-W ave: Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors.

Zigbee/802.14: Zigbee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. Zigbee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products.

NEW QUESTION 80

What is a key advantage and key risk in using a public cloud environment?

- A. Multi-tenancy
 B. Dedicated Networks
 C. Dedicated Hosts
 D. Multiplexing

Answer: A

Explanation:

Multitenancy is a key characteristic of the public cloud, and an important risk. Although public cloud providers strive to ensure isolation between their various customers, the infrastructure and resources in the public cloud are shared. Inherent risks in a shared environment include misconfigurations, inadequate or ineffective processes and controls, and the “noisy neighbor” problem (excessive network traffic, disk I/O, or processor use can negatively impact other customers sharing the same resource). In hybrid and multicloud environments that connect numerous public and/or private clouds, the delineation becomes blurred, complexity increases, and security risks become more challenging to address.

NEW QUESTION 85

Match the Palo Alto Networks WildFire analysis verdict with its definition.

Answer Area

Benign		malicious in intent and can pose a security threat
Grayware		does not pose a direct security threat
Malware		does not exhibit a malicious behavior

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Benign: Safe and does not exhibit malicious behavior

Grayware: No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects)

Malware: Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits)

Phishing: Malicious attempt to trick the recipient into revealing sensitive data

NEW QUESTION 89

Which NGFW feature is used to provide continuous identification, categorization, and control of known and previously unknown SaaS applications?

- A. User-ID
- B. Device-ID
- C. App-ID
- D. Content-ID

Answer: C

Explanation:

App-ID™ technology leverages the power of the broad global community to provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular.

NEW QUESTION 93

A user is provided access over the internet to an application running on a cloud infrastructure. The servers, databases, and code of that application are hosted and maintained by the vendor.

Which NIST cloud service model is this?

- A. IaaS
- B. SaaS
- C. PaaS
- D. CaaS

Answer: B

Explanation:

SaaS - User responsible for only the data, vendor responsible for rest

NEW QUESTION 98

Which network analysis tool can be used to record packet captures?

- A. Smart IP Scanner
- B. Wireshark
- C. Angry IP Scanner
- D. Netman

Answer: B

NEW QUESTION 103

Which IPsec feature allows device traffic to go directly to the Internet?

- A. Split tunneling
- B. Diffie-Hellman groups
- C. d.Authentication Header (AH)
- D. IKE Security Association

Answer: A

Explanation:

"Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation."

NEW QUESTION 104

Given the graphic, match each stage of the cyber-attack lifecycle to its description.

Unauthorized Access		Unauthorized Use
reconnaissance		attacker will plan the cyber-attack
weaponization		attacker will determine which method to use to compromise an endpoint
delivery		attacker will distribute their weaponized payload to an endpoint
exploitation		attacker will trigger a weaponized payload
installation		escalate privileges on a compromised endpoint
command and control		establish secure communication channel to servers across the internet to reshape attack objectives

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

NEW QUESTION 109

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 113

What is required for a SIEM to operate correctly to ensure a translated flow from the system of interest to the SIEM data lake?

- A. connectors and interfaces
- B. infrastructure and containers
- C. containers and developers
- D. data center and UPS

Answer: A

NEW QUESTION 118

Which activities do local organization security policies cover for a SaaS application?

- A. how the data is backed up in one or more locations
- B. how the application can be used
- C. how the application processes the data
- D. how the application can transit the Internet

Answer: B

NEW QUESTION 123

Which aspect of a SaaS application requires compliance with local organizational security policies?

- A. Types of physical storage media used
- B. Data-at-rest encryption standards
- C. Acceptable use of the SaaS application
- D. Vulnerability scanning and management

Answer: C

NEW QUESTION 125

.....

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