

- **Vendor: Palo Alto Networks**
- **Exam Code: PCCSA**
- **Exam Name: Palo Alto Networks Certified Cybersecurity Associate**
- **New Updated Questions from [Braindump2go](#) (Updated in [May/2020](#))**

Visit Braindump2go and Download Full Version PCCSA Exam Dumps

QUESTION 1

In the context of a mobile device management solution, what is a function of the "policy enforcement" feature?

- A. controls which websites can be accessed when connected to Wi-Fi
- B. controls which Wi-Fi networks can be accessed
- C. controls which phone numbers can be dialed
- D. controls which password/passcode settings are allowed

Answer: A

QUESTION 2

Review the exhibit and identify the type of vulnerability or attack.

Thank you all for your hard work at accomplishing continued company success. Our company recognizes the contributions of its employees and has decided that as a token of appreciation all employees are eligible to participate in a company-sponsored raffle.

- **1** lucky winner will receive a \$500 American Express Gift Certificate
- **10** lucky winners will receive an mp3 player
- **50** lucky winners will receive 2 tickets to the movies

If you are not a winner, don't be disappointed. **Everyone** who signs up will receive a gift as a token of our appreciation. To participate in this raffle please visit <https://www.hr-rewards.com/ThankYou> before **3 PM** on **10/06/2016**.

Thank you for your great work!

Human Resources

- A. botnet
- B. man-in-the-middle

- C. spear phishing
- D. buffer overflow

Answer: C

QUESTION 3

Which two reconnaissance tools might an attacker use to scan for vulnerable network services and settings? (Choose two.)

- A. bandwidth analyzer
- B. intrusion detection
- C. port scanner
- D. password cracker

Answer: CD

QUESTION 4

Drag and Drop Question

Match the OSI network model Layer 3 function to the correct description.

routing	Drag answer here	provides service to direct packets to their destination host
encapsulation	Drag answer here	wraps transport layer data in IP packets
decapsulation	Drag answer here	provides segments or datagrams to the transport layer
addressing	Drag answer here	provides a mechanism for identifying end devices

Answer:

routing	provides service to direct packets to their destination host
encapsulation	wraps transport layer data in IP packets
decapsulation	provides segments or datagrams to the transport layer
addressing	provides a mechanism for identifying end devices

QUESTION 5

During which step of the cyber-attack lifecycle is a user's web browser redirected to a webpage that automatically downloads malware to the endpoint?

- A. delivery

- B. weaponization
- C. reconnaissance
- D. command-and-control

Answer: A

QUESTION 6

How does machine learning enhance WildFire operation?

- A. analyzes file sample characteristics during static analysis
- B. determines which file samples should be forwarded to WildFire
- C. determines the optimum OS WildFire uses to analyze file samples
- D. analyzes file sample characteristics during dynamic analysis

Answer: D

QUESTION 7

Palo Alto Networks App-ID uses information from which source to help identify an application in network traffic?

- A. PAN-DB URL database
- B. traffic behavioral analysis
- C. source port in packet header
- D. destination IP address in packet header

Answer: B

QUESTION 8

Which capability is required for a next-generation firewall to protect your network against malware threats?

- A. can access/read Windows and Linux file systems
- B. can scan all endpoint devices
- C. can interpret file permissions
- D. can perform SSL decryption

Answer: D

QUESTION 9

Which Palo Alto Networks technology safely enables business use of mobile devices by providing a unique solution to manage the device, protect the device, and control the data?

- A. AutoFocus
- B. WildFire
- C. GlobalProtect
- D. Traps

Answer: C

QUESTION 10

Which option describes a characteristic of a next-generation firewall but not a UTM device?

- A. Content inspection engines operate in individual silos.
- B. Content inspection engines use tightly integrated operation.
- C. Content inspection engines process traffic serially, not in parallel.
- D. Content inspection engines run on the same hardware and memory resources.

Answer: B

QUESTION 11

Which type of cloud computing service provides access to email and word processing applications running in a cloud infrastructure?

- A. software as a service
- B. computing as a service
- C. platform as a service
- D. infrastructure as a service

Answer: A

QUESTION 12

What is the result of deploying virtualization in your data center?

- A. reduced security threat
- B. reduced operational costs
- C. increased hardware capital costs
- D. increased host provisioning

Answer: B

QUESTION 13

Which two remote access methods are secure because they encrypt traffic? (Choose two.)

- A. IPsec-AH
- B. SSH
- C. VPN
- D. Telnet
- E. rlogin

Answer: BC

QUESTION 14

Which action must be taken prior to a successful ransomware attack to enable recovery from the attack?

- A. create a data snapshot on your IDS device
- B. back up all hosts that contain critical data
- C. update all firewall malware signatures
- D. limit external exposure of internal DNS resource records

Answer: B

QUESTION 15

Which network security architecture feature is designed to purposely expose some of an organization's services to untrusted networks?

- A. network zone
- B. security zone
- C. demilitarized zone
- D. military zone

Answer: C