PCCSA Q&As

Palo Alto Networks Certified Cybersecurity Associate

Pass Palo Alto Networks PCCSA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/pccsa.html

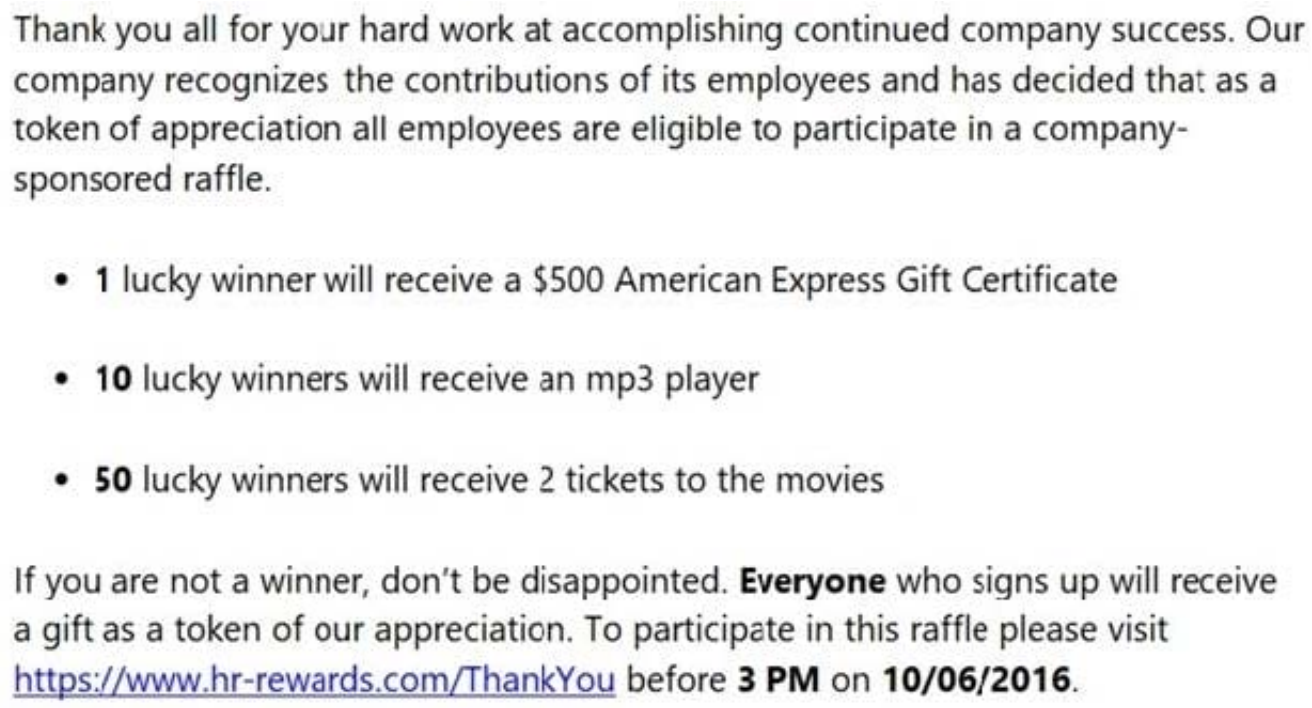
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

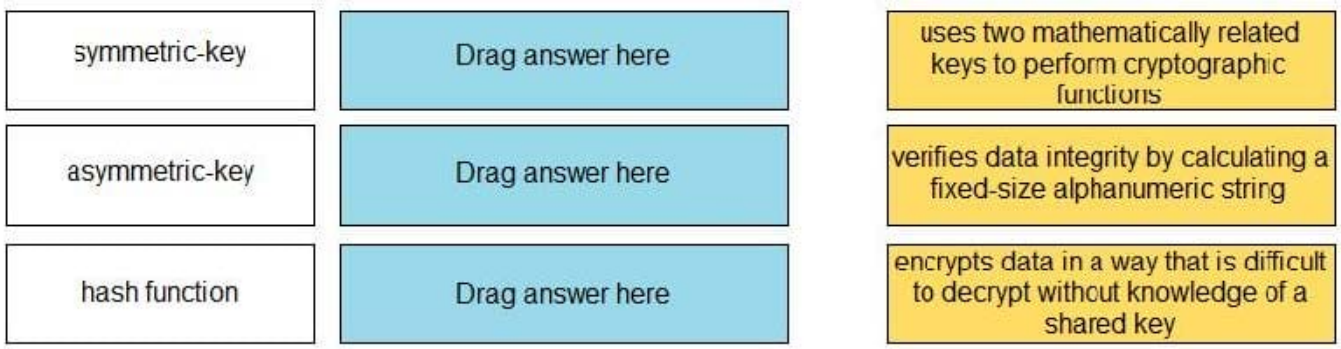
Correct Answer: C

QUESTION 2

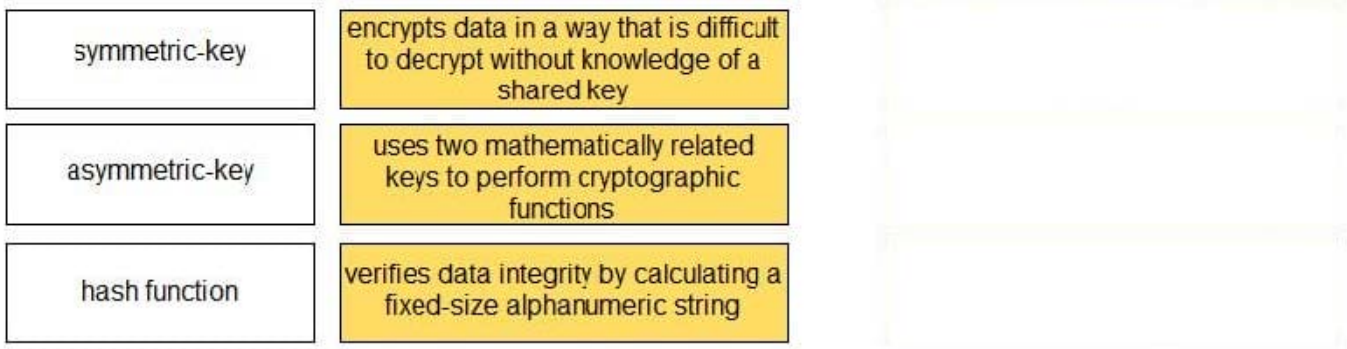
DRAG DROP

Match each cryptographic method with its description.

Select and Place:



Correct Answer:



QUESTION 3

A firewall located on an organization\\'s network perimeter can be used to protect against which type of attack?

A. a malicious SaaS application file accessed from an unmanaged mobile phone

B. ransomware installed from an infected USB drive

C. malware installed on the laptop by a disgruntled employee

D. a malicious PDF file located on an internet website

Correct Answer: D

QUESTION 4

Which type of attack floods a target with TCP SYN requests?

A. route table poisoning

B. reconaissance

C. denial-of-service

D. IP spoofing

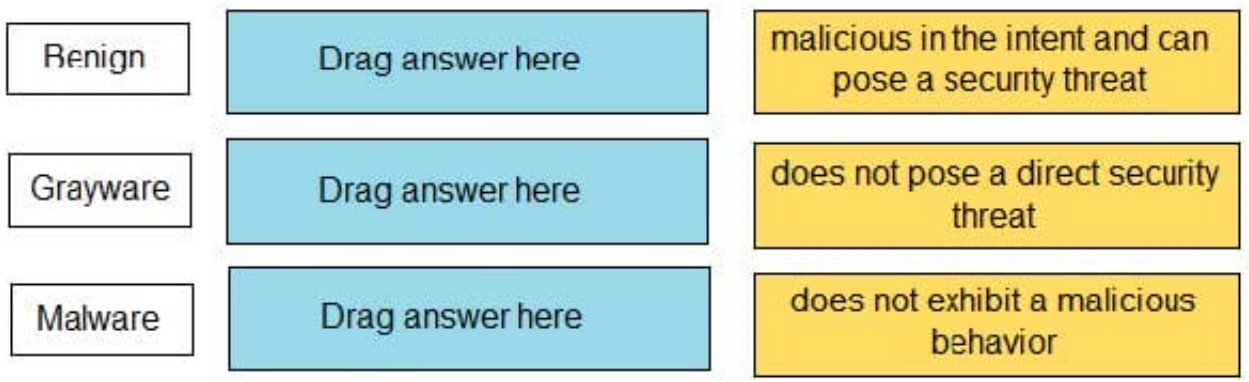
Correct Answer: C

QUESTION 5

DRAG DROP

Match the Palo Alto Networks Wild Fire analysis verdict with its definition.

Select and Place:



Correct Answer:

QUESTION 6

Which type of SaaS application is allowed and provided by an IT department?

A. tolerated

B. certified

C. sanctioned

D. unsanctioned

Correct Answer: C

Reference: https://www.paloaltonetworks.com/cyberpedia/saas-security

QUESTION 7

From which resource can a Palo Alto Networks firewall get URL category information for URLs whose categories cannot be found on the firewall?

A. App-ID database

B. WildFire

C. PDF file

D. PAN-DB database

Correct Answer: D

QUESTION 8

You discover an infected email attachment that contains software code that attacks a known vulnerability in a popular social networking application. This type of software code belongs to which type of malware category?

A. social engineering

B. virus

C. pharming

D. exploit

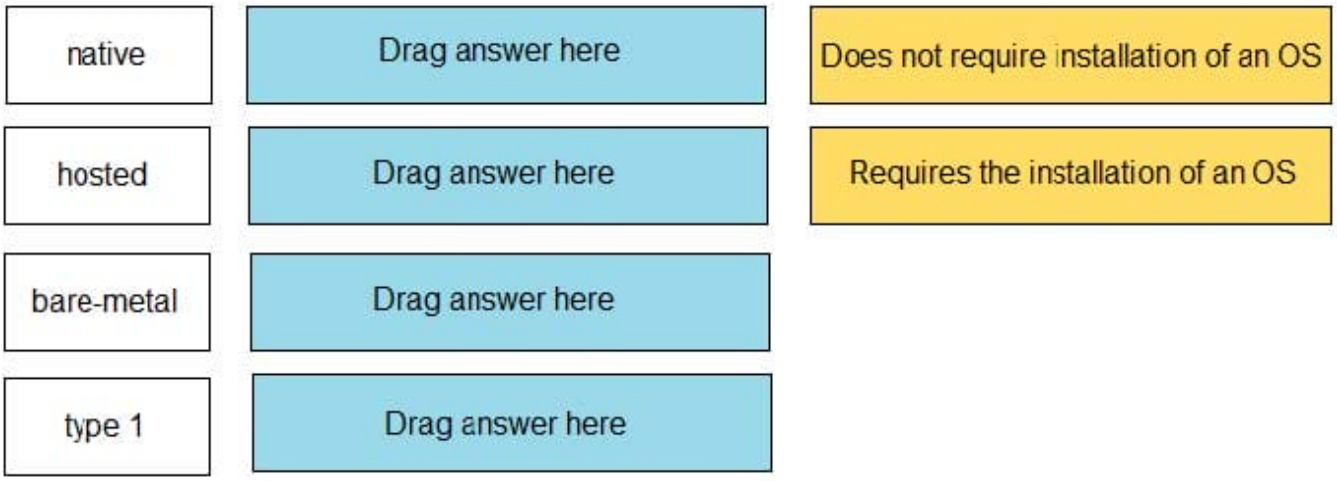
Correct Answer: D

QUESTION 9

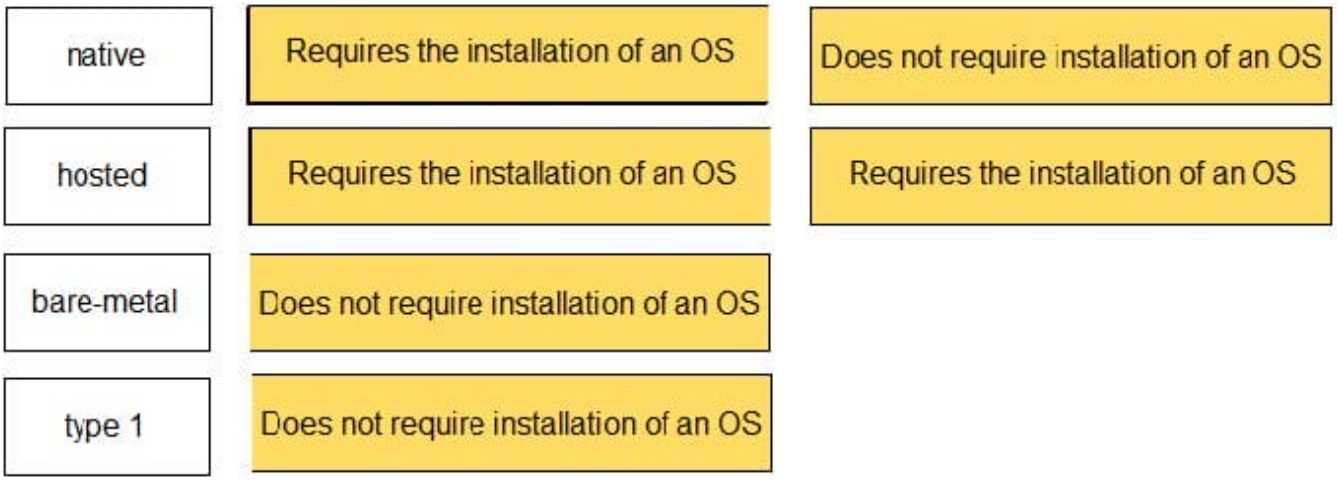
DRAG DROP

Match the task for server settings in group mapping with its order in the process.

Select and Place:



Correct Answer:



QUESTION 10

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

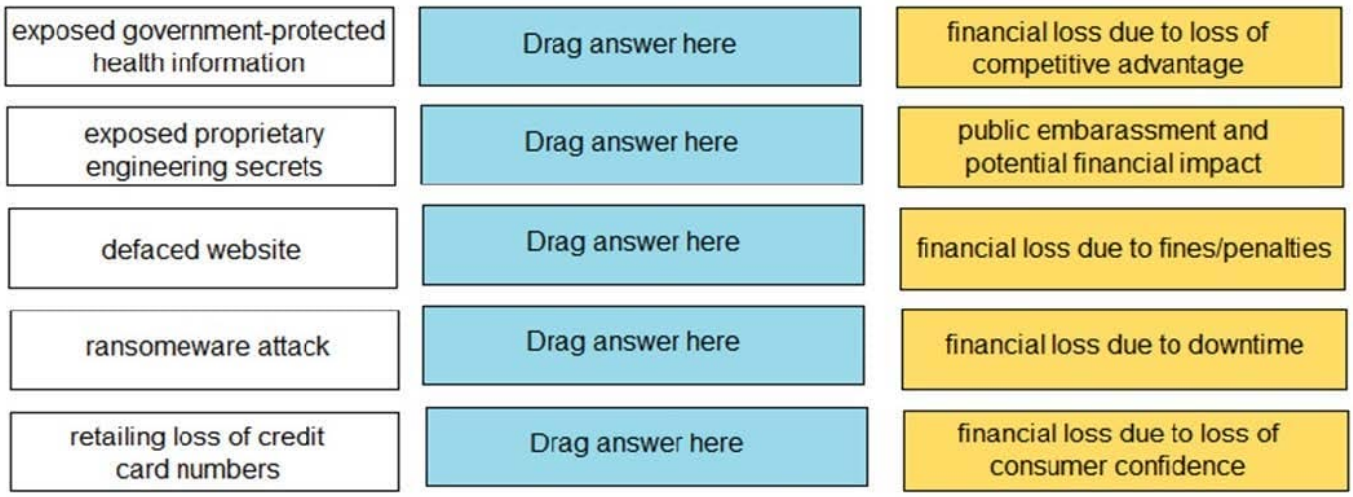
Correct Answer: B

QUESTION 11

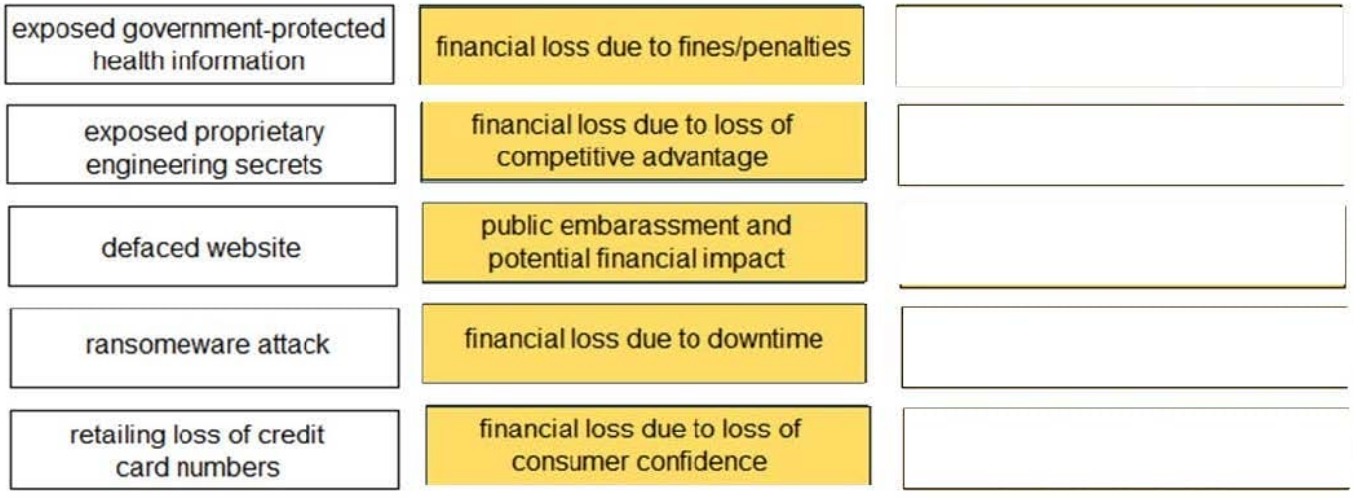
DRAG DROP

Match each type of breach to its consequence.

Select and Place:



Correct Answer:



QUESTION 12

Which type of firewall monitors traffic streams from beginning to end?

A. circuit-level gateway

B. stateless

C. stateful

D. packet filter

Correct Answer: C

QUESTION 13

You discover malware has corrupted the BIOS on your laptop. Which type of malware is this?

A. bootkit

B. exploit

C. rootkit

D. vulnerability

Correct Answer: A

QUESTION 14

Which mobile device management feature prevents jailbreaking or rooting?

A. software distribution

B. malware protection

C. policy enforcement

D. data loss prevention

Correct Answer: C

QUESTION 15

Which type of security device uses a single-pass, parallel processor hardware architecture to accelerate content inspection?

A. unified threat management

B. stateless firewalls

C. next-generation firewall

D. PoS-based firewall

Correct Answer: C