350-701 Q&As

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

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

https://www.passapply.com/350-701.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

A. PaaS

B. XaaS

C. IaaS

D. SaaS

Correct Answer: A

Reference: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide

QUESTION 2

A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling

B. Use MAB with posture assessment.

C. Use 802.1X with posture assessment.

D. Use 802.1X with profiling.

Correct Answer: A

Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design- guide/ta-p/3739456

QUESTION 3

An organization has DHCP servers set up to allocate IP addresses to clients on the LAN.

What must be done to ensure the LAN switches prevent malicious DHCP traffic while also distributing IP addresses to the correct endpoints?

A. Configure Dynamic ARP Inspection and add entries in the DHCP snooping database

B. Configure DHCP snooping and set an untrusted interface for all clients

C. Configure Dynamic ARP Inspection and antispoofing ACLs in the DHCP snooping database

D. Configure DHCP snooping and set a trusted interface for the DHCP server

Correct Answer: D

QUESTION 4

Which Cisco platform onboards the endpoint and can issue a CA signed certificate while also automatically configuring endpoint network settings to use the signed endpoint certificate, allowing the endpoint to gain network access?

A. Cisco ISE

B. Cisco NAC

C. Cisco TACACS+

D. Cisco WSA

Correct Answer: A

QUESTION 5

For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

A. by specifying blocked domains in me policy settings

B. by specifying the websites in a custom blocked category

C. by adding the websites to a blocked type destination list

D. by adding the website IP addresses to the Cisco Umbrella blocklist

Correct Answer: C

QUESTION 6

An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?

A. Cisco FMC

B. CSM

C. Cisco FDM

D. CDO

Correct Answer: A

QUESTION 7

An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?

A. single interface

B. multi-context

C. transparent

D. two-interface

Correct Answer: D

QUESTION 8

In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

A. when there is a need for traditional anti-malware detection

B. when there is no need to have the solution centrally managed

C. when there is no firewall on the network

D. when there is a need to have more advanced detection capabilities

Correct Answer: D

Endpoint protection platforms (EPP) prevent endpoint security threats like known and unknown malware.Endpoint detection and response (EDR) solutions can detect and respond to threats that your EPP and other security tools did not catch.EDR and EPP have similar goals but are designed to fulfill different purposes. EPP is designed to providedevice-level protection by identifying malicious files, detecting potentially malicious activity, and providing tools for incident investigation and response.The preventative nature of EPP complements proactive EDR. EPP acts as the first line of defense, filtering out attacks that can be detected by the organization\\'s deployed security solutions. EDR acts as a second layer of protection, enabling security analysts to perform threat hunting and identify more subtle threats to the endpoint.Effective endpoint defense requires a solution that integrates the capabilities of both EDR and EPP to provide protection against cyber threats without overwhelming an organization\\'s security team.

QUESTION 9

Which Cisco solution extends network visibility, threat detection, and analytics to public cloud environments?

A. Cisco Umbrella

B. Cisco Stealthwatch Cloud

C. Cisco Appdynamics

D. Cisco CloudLock

Correct Answer: B

QUESTION 10

An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

A. Cisco Umbrella

B. Cisco Cloud Email Security

C. Cisco NGFW

D. Cisco Cloudlock

Correct Answer: D

Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web- security/at-a-glance-c45-738565.pdf

QUESTION 11

An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows. What action would allow the attacker to gain access to machine 1 but not machine 2?

A. sniffing the packets between the two hosts

B. sending continuous pings

C. overflowing the buffer\\'s memory

D. inserting malicious commands into the database

Correct Answer: D

QUESTION 12

Which ESA implementation method segregates inbound and outbound email?

A. one listener on a single physical Interface

B. pair of logical listeners on a single physical interface with two unique logical IPv4 addresses and one IPv6 address

C. pair of logical IPv4 listeners and a pair Of IPv6 listeners on two physically separate interfaces

D. one listener on one logical IPv4 address on a single logical interface

Correct Answer: D

QUESTION 13

What are two DDoS attack categories? (Choose two)

A. sequential

B. protocol

C. database

D. volume-based

E. screen-based

Correct Answer: BD

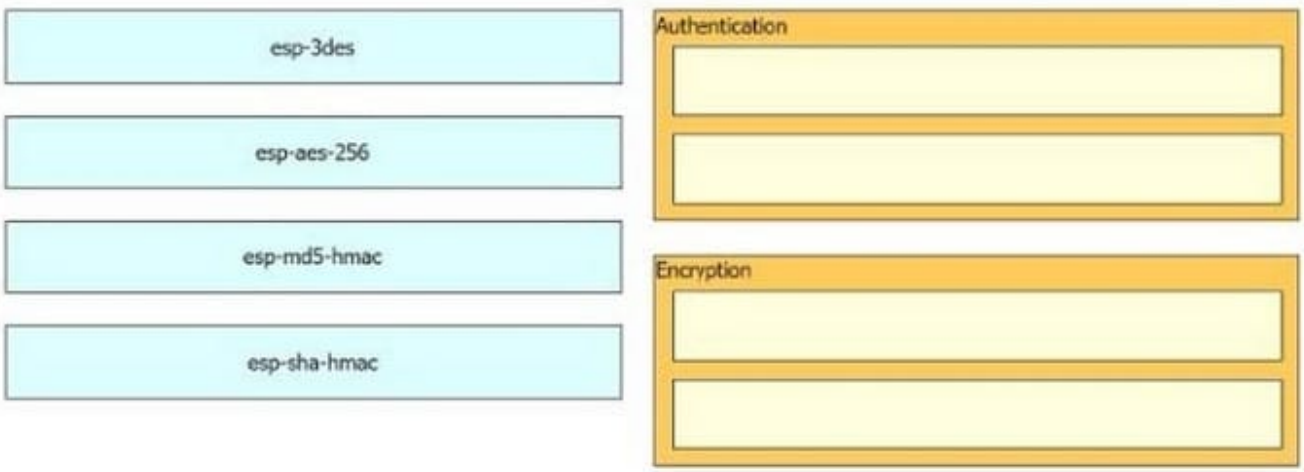
There are three basic categories of attack:+ volume-based attacks, which use high traffic to inundate the network bandwidth+ protocol attacks, which focus on exploiting server resources+ application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks Reference: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/

QUESTION 14

DRAG DROP

Drag and drop the cryptographic algorithms for IPsec from the left onto the cryptographic processes on the right.

Select and Place:



Correct Answer:

QUESTION 15

Refer to the exhibit.

Consider that any feature of DNS requests, such as the length off the domain name and the number of subdomains, can be used to construct models of expected behavior to which observed values can be compared. Which type of malicious attack are these values associated with?

A. Spectre Worm

B. Eternal Blue Windows

C. Heartbleed SSL Bug

D. W32/AutoRun worm

Correct Answer: D