Cisco 210-260 Exam

Volume: 226 Questions

Question No: 1
Which two services define cloud networks? (Choose two.)

A. Infrastructure as a Service

B. Platform as a Service

C. Security as a Service

D. Compute as a Service

E. Tenancy as a Service

Answer: A,B

Question No: 2
In which two situations should you use out-of-band management? (Choose two.)

A. when a network device fails to forward packets

B. when you require ROMMON access

C. when management applications need concurrent access to the device

D. when you require administrator access from multiple locations

E. when the control plane fails to respond

Answer: A,B

Question No: 3
In which three ways does the TACACS protocol differ from RADIUS? (Choose three.)

A. TACACS uses TCP to communicate with the NAS.

B. TACACS can encrypt the entire packet that is sent to the NAS.

C. TACACS supports per-command authorization.

D. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.

E. TACACS uses UDP to communicate with the NAS.

F. TACACS encrypts only the password field in an authentication packet.

Answer: A,B,C

Question No: 4
According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

A. BOOTP

B. TFTP

C. DNS

D. MAB

E. HTTP

F. 802.1x

Answer: A,B,C

Question No: 5
Which two next-generation encryption algorithms does Cisco recommend? (Choose two.)

A.AES

B. 3DES

C. DES

D. MDS

E. DH-1024

F. SHA-384

Answer: A,F

Question No: 6
Which three ESP fields can be encrypted during transmission? (Choose three.)

A. Security Parameter Index

B. Sequence Number

C. MAC Address

D. Padding

E. Pad Length

F. Next Header

Answer: D,E,F

Question No: 7
What are two default Cisco IOS privilege levels? (Choose two.)

A. 0

B. 1

C. 5

D. 7

E. 10

F. 15

Answer: B,F

Question No: 8
Which two authentication types does OSPF support? (Choose two.)

A. plaintext

B. MD5

C. HMAC

D. AES 256

E. SHA-1

F. DES

Answer: A,B

Question No: 9
Which two features do CoPP and CPPr use to protect the control plane? (Choose two.)

A. QoS

B. traffic classification

C. access lists

D. policy maps

E. class maps

F. Cisco Express Forwarding

Answer: A,B

Question No: 10
Which two statements about stateless firewalls are true? (Choose two.)

A. They compare the 5-tuple of each incoming packet against configurable rules.

B. They cannot track connections.

C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.

D. Cisco IOS cannot implement them because the platform is stateful by nature.

E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

Answer: A,B

Question No: 11
Which three statements about host-based IPS are true? (Choose three.)

A. It can view encrypted files.

B. It can have more restrictive policies than network-based IPS.

C. It can generate alerts based on behavior at the desktop level.

D. It can be deployed at the perimeter.

E. It uses signature-based policies.

F. It works with deployed firewalls.

Answer: A,B,C

Question No: 12
What three actions are limitations when running IPS in promiscuous mode? (Choose three.)

A. deny attacker

B. deny packet

C. modify packet

D. request block connection

E. request block host

F. reset TCP connection

Answer: A,B,C

Question No: 13
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Deny the connection inline.

B. Perform a Layer 6 reset.

C. Deploy an antimalware system.

D. Enable bypass mode.

Answer: A

Question No: 14
What is an advantage of implementing a Trusted Platform Module for disk encryption?

A. It provides hardware authentication.

B. It allows the hard disk to be transferred to another device without requiring re-encryption.dis

C. It supports a more complex encryption algorithm than other disk-encryption technologies.

D. It can protect against single points of failure.

Answer: A

Question No: 15
What is the purpose of the Integrity component of the CIA triad?

A. to ensure that only authorized parties can modify data

B. to determine whether data is relevant

C. to create a process for accessing data

D. to ensure that only authorized parties can view data

Answer: A

Question No: 16
In a security context, which action can you take to address compliance?

A. Implement rules to prevent a vulnerability.

B. Correct or counteract a vulnerability.

C. Reduce the severity of a vulnerability.

D. Follow directions from the security appliance manufacturer to remediate a vulnerability.

Answer: A

Question No: 17
Which type of secure connectivity does an extranet provide?

A. other company networks to your company network

B. remote branch offices to your company network

C. your company network to the Internet

D. new networks to your company network

Answer: A

Question No: 18
Which tool can an attacker use to attempt a DDoS attack?

A. botnet

B. Trojan horse

C. virus

D. adware

Answer: A

Question No: 19
What type of security support is provided by the Open Web Application Security Project?

A. Education about common Web site vulnerabilities.

B. A Web site security framework.

C. A security discussion forum for Web site developers.

D. Scoring of common vulnerabilities and exposures.

Answer: A

Question No: 20
What type of attack was the Stuxnet virus?

A. cyber warfare

B. hacktivism

C. botnet

D. social engineering

Answer: A

Question No: 21
What type of algorithm uses the same key to encrypt and decrypt data?

A. a symmetric algorithm

B. an asymmetric algorithm

C. a Public Key Infrastructure algorithm

D. an IP security algorithm

Answer: A

Question No: 22
Refer to the exhibit.

```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
   6 Bad SNMP version errors
   3 Unknown community name
   9 Illegal operation for community name supplied
   4 Encoding errors
   2 Number of requested variables
   0 Number of altered variables
   98 Get-request PDUs
   12 Get-next PDUs
   2 Set-request PDUs
   0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   0 No such name errors
   0 Bad values errors
   0 General errors
   31 Response PDUs
   1 Trap PDUs
```

How many times was a read-only string used to attempt a write operation?

A. 9

B. 6

C. 4

D. 3

E. 2

Answer: A

Question No: 23
Refer to the exhibit.

```
R1> show clock detail
.22:22:35.123 UTC Tue Feb 26 2013
Time source is NTP
```

Which statement about the device time is true?

A. The time is authoritative, but the NTP process has lost contact with its servers.

B. The time is authoritative because the clock is in sync.

C. The clock is out of sync.

D. NTP is configured incorrectly.

E. The time is not authoritative.

Answer: A

Question No: 24
How does the Cisco ASA use Active Directory to authorize VPN users?

A. It queries the Active Directory server for a specific attribute for the specified user.

B. It sends the username and password to retrieve an ACCEPT or REJECT message from the Active Directory server.

C. It downloads and stores the Active Directory database to query for future authorization requests.

D. It redirects requests to the Active Directory server defined for the VPN group.

Answer: A

Question No: 25
Which statement about Cisco ACS authentication and authorization is true?

A. ACS servers can be clustered to provide scalability.

B. ACS can query multiple Active Directory domains.

C. ACS uses TACACS to proxy other authentication servers.

D. ACS can use only one authorization profile to allow or deny requests.

Answer: A

Question No: 26
Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dotlx webauth
authentication priority dotlx mab
authentication port-control auto
dotlx pae authenticator
```