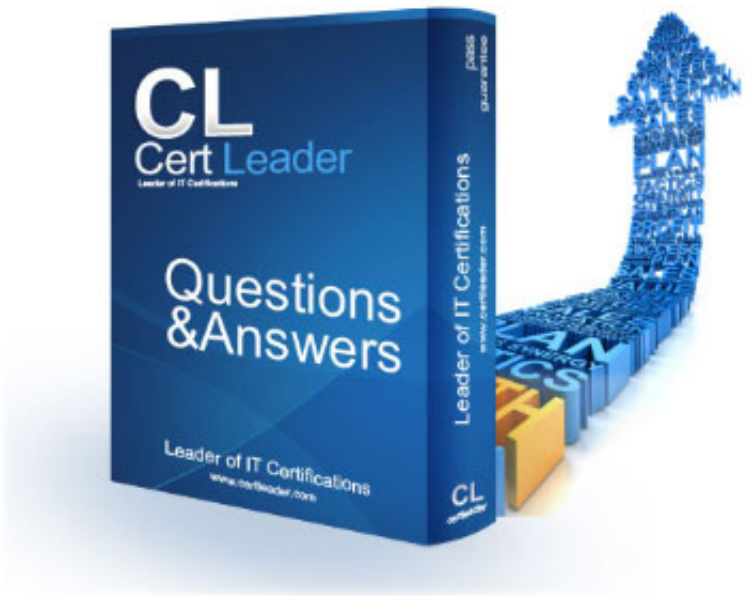
210-260 - IINS Implementing Cisco Network Security

http://www.certleader.com/210-260-dumps.html



1. Which FirePOWER preprocessor engine is used to prevent SYN attacks?

A. Rate-Based Prevention

B. Portscan Detection

C. IP Defragmentation

D. Inline Normalization

Answer: A

2. Which statement about college campus is true?

A. College campus has geographical position.

B. College campus Hasn`t got internet access.

C. College campus Has multiple subdomains.

Answer: A

3. An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.

B. The switch could become the root bridge.

C. The switch could be allowed to join the VTP domain.

D. The switch could become a transparent bridge.

Answer: B

4. Refer to the exhibit.

```
UDP outside  209.165.201.225:53 inside  10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

What type of firewall would use the given configuration line?

A. a stateful firewall

B. a personal firewall

C. a proxy firewall

D. an application firewall

E. a stateless firewall

Answer: A

5. Which three statements describe DHCP spoofing attacks? (Choose three.)

A. They can modify traffic in transit.

B. They are used to perform man-in-the-middle attacks.

C. They use ARP poisoning.

D. They can access most network devices.

E. They protect the identity of the attacker by masking the DHCP address.

F. They are can physically modify the network gateway.

Answer: A,B,C

6. Which port should (or would) be open if VPN NAT-T was enabled

A. port 500

B. port 500 outside interface

C. port 4500 outside interface

D. port 4500 ipsec

Answer: D

7. If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

A. The ASA will apply the actions from only the first matching class map it finds for the feature type.

B. The ASA will apply the actions from only the most specific matching class map it finds for the feature type.

C. The ASA will apply the actions from all matching class maps it finds for the feature type.

D. The ASA will apply the actions from only the last matching class map it finds for the feature type.

Answer: A

8. Which of the following pairs of statements is true in terms of configuring MD authentication?

A. Interface statements (OSPF, EIGRP) must be configured; use of key chain in OSPF

B. Router process (OSPF, EIGRP) must be configured; key chain in EIGRP

C. Router process (only for OSPF) must be configured; key chain in EIGRP

D. Router process (only for OSPF) must be configured; key chain in OSPF

Answer: C

9. Which two NAT types allows only objects or groups to reference an IP address? (choose two)

A. dynamic NAT

B. dynamic PAT

C. static NAT

D. identity NAT

Answer: A,C

10. For what reason would you configure multiple security contexts on the ASA firewall?

A. To separate different departments and business units.

B. To enable the use of VRFs on routers that are adjacently connected.

C. To provide redundancy and high availability within the organization.

D. To enable the use of multicast routing and QoS through the firewall.

Answer: A

11. What is example of social engineering

A. Gaining access to a building through an unlocked door.

B. something about inserting a random flash drive.

C. gaining access to server room by posing as IT

D. Watching other user put in username and password (something around there)

Answer: C

12. 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

13. What is the effect of the ASA command crypto isakmp nat-traversal?

A. It opens port 4500 only on the outside interface.

B. It opens port 500 only on the inside interface.

C. It opens port 500 only on the outside interface.

D. It opens port 4500 on all interfaces that are IPSec enabled.

Answer: D

14. Which statement is a benefit of using Cisco IOS IPS?

A. It uses the underlying routing infrastructure to provide an additional layer of security.

B. It works in passive mode so as not to impact traffic flow.

C. It supports the complete signature database as a Cisco IPS sensor appliance.

D. The signature database is tied closely with the Cisco IOS image.

Answer: A

15. What configure mode you used for the command ip ospf authentication-key c1$c0?

A. global

B. privileged

C. in-line

D. Interface

Answer: D

Explanation: ip ospf authentication-key is used under interface configuration mode, so it’s in interface level, under global configuration mode. If it asks about interface level then choose that.

interface Serial0

ip address 192.16.64.1 255.255.25

16. How does a zone-based firewall implementation handle traffic between interfaces in the same zone?

A. Traffic between two interfaces in the same zone is allowed by default.

B. Traffic between interfaces in the same zone is blocked unless you configure the same- security permit command.

C. Traffic between interfaces in the same zone is always blocked.

D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair.

Answer: A

17. Which description of the nonsecret numbers that are used to start a Diffie-Hellman exchange is true?

A. They are large pseudorandom numbers.

B. They are very small numbers chosen from a table of known values

C. They are numeric values extracted from hashed system hostnames.

D. They are preconfigured prime integers

Answer: D

18. What is a potential drawback to leaving VLAN 1 as the native VLAN?

A. It may be susceptible to a VLAN hoping attack.

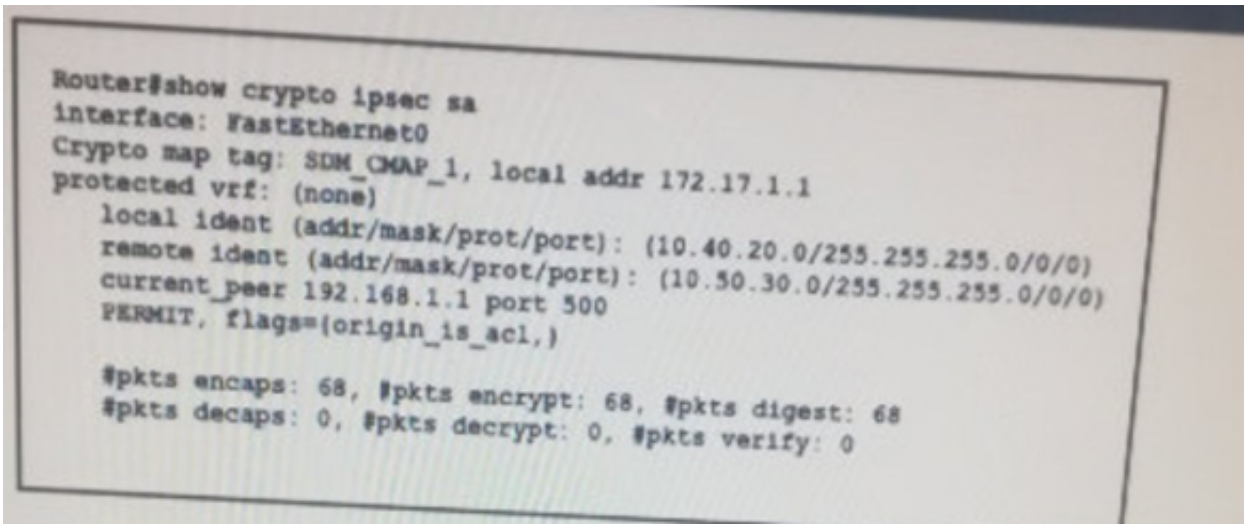
B. Gratuitous ARPs might be able to conduct a man-in-the-middle attack.

C. The CAM might be overloaded, effectively turning the switch into a hub.

D. VLAN 1 might be vulnerable to IP address spoofing.

Answer: A

19. Refer to the exhibit.



For which reason is the tunnel unable to pass traffic?

A. UDP port 500 is blocked.

B. The IP address of the remote peer is incorrect.

C. The tunnel is failing to receive traffic from the remote peer.

D. The local peer is unable to encrypt the traffic.

Answer: C

20. Which two functions can SIEM provide? (Choose Two)

A. Correlation between logs and events from multiple systems.

B. event aggregation that allows for reduced log storage requirements.

C. proactive malware analysis to block malicious traffic.

D. dual-factor authentication.

E. centralized firewall management.

Answer: A,C

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 210-260 Exam with Our Prep Materials Via below:

http://www.certleader.com/210-260-dumps.html