IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **642-541**

Title : VPN and Security Cisco SAFE Implementation Exam (CSI)

Version : DEMO

1. Which routing protocol does not support the use of MD5 authentication?

A. BGP

B. IGRP

C. EIGRP

D. OSPF

E. IS-IS

Answer: C

2. What is an assumption of SAFE SMR?

A. implementing SAFE SMR guarantees a secure environment

B. the security policy is already in place

C. network contains only Cisco devices

D. SAFE SMR does not assume application and OS security

Answer: B

3. Why are all providers of Internet connectivity urged to implement the filtering described in RFC 2827?

A. to prohibit attackers from using source addresses that reside within a range of legitimately advertised prefixes

B. to prohibit attackers from using forged source addresses that do not reside within a range of legitimately advertised prefixes

C. to filter Java applications that come from a source that is not trusted

D. to stop internal users from reaching web sites that violate the established security policy

Answer: B

4. The VPN acceleration module (VAM) is available on what series of VPN optimized routers? Choose two.

A. 1700 Series

B. 2600 Series

C. 3600 Series

D. 7100 Series

E. 7200 Series

Answer: DE

5. Which two devices in the SAFE SMR small network campus module should have HIDS installed? Choose two.

A. Layer 2 switches

B. firewalls

C. management hosts

D. desktop workstations

E. corporate servers

F. lab workstations

Answer: CE

6. In which module does the firewall exist in the SAFE SMR small network design?

A. Internet

B. campus

C. corporate Internet

D. edge

Answer: C

7. What is the NIDS primary function in the SAFE SMR midsize network design corporate Internet module?

A. provide connectivity to the campus module

B. provide connectivity to the WAN module

C. provide connectivity to the LAN module

D. provides detection of attacks on ports that the firewall is configured to permit

E. provide the demarcation point between the ISP and the medium network

F. provide connection state enforcement and detailed filtering for sessions initiated through the firewall

Answer: D

8. Which two general IP spoofing techniques does a hacker use? Choose two.

A. an IP address within the range of trusted IP addresses

B. an unknown IP address which cannot be traced

C. an RFC 1918 address

D. an authorized external IP address that is trusted

Answer: AD

9. Which model is recommended for an IDS with at least 100 Mbps performance?

A. 4210

B. 4220

C. 4250

D. 4260

Answer: C

10. Which is a key server found in SAFE Enterprise network design edge corporate internet module?

A. database server

B. application server

C. URL filtering server

D. proxy server

Answer: C

11. What is the purpose of BGP TTL Security Hash (BTSH)?

A. encrypts private network data when it is being passed through a public network

B. prevents attacker from creating a routing black hole

C. helps to prevent information overload from causing a network to melt

D. prevents attackers from disrupting peering sessions between routers

E. reduces the change rate in the Internet's routing tables

Answer: D

12. What are two characteristics of a packet sniffer designed for attack purposes? Choose two.

A. captures first 300 to 400 bytes

B. typically captures login sessions

C. captures the last 300 to 400 bytes

D. deciphers encrypted passwords

E. unable to capture UDP packets

Answer: AB

13. In the SAFE SMR midsize network design, which module does dial-in traffic terminate?

A. campus module

B. WAN module

C. ISP edge module

D. corporate Internet module

E. PSTN module

F. frame/ATM module

Answer: D

14. Which type of attack is characterized by exploitation of well-known weaknesses, use of ports that are allowed through a firewall, and can never be completely eliminated?

A. network reconnaissance

B. application layer

C. man-in-the-middle

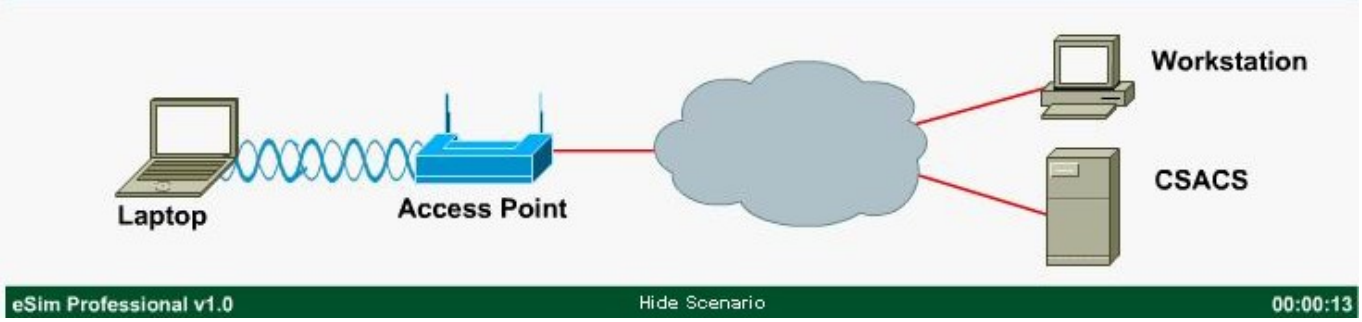
D. trust exploitation

Answer: B

15. LAB

Signature Underwriters has moved a wireless access point from Boston to Atlanta. The Cisco Secure Access Control Server and the wireless client adapter have been configured except the access point. Your task is to configure the access point with new authentication server and WEP key parameters to allow secure access from wireless users in Atlanta. To gain entry to the access point launch the browser by clicking on the "Workstation" and entering the proper IP address. After configuration of the access point has been completed the authentication can be verified by closing the browser and launching the LEAP from the laptop. Use the following parameters to accomplish these objectives. All other parameters on the access point have been pre-configured.

- 1200 Wireless access point 172.16.153.21 255.255.255.0
- Wireless Client Adapter 172.16.153.15 255.255.255.0
- CSACS 172.16.153.50 255.255.255.0
- Server Name/IP: 172.16.153.50
- Server Type: RADIUS
- Port: 1645
- Shared Secret: everythingsecret
- Authentication Type: EAP
- WEP Key Size: 128 bit
- WEP Key: 1234567890123456789Oabcdef
- Encryption: Full



eSim Professional v1.0 Hide Scenario 00:00:13

16. Which three models of the Cisco 3000 Series Concentrator can have redundant power supplies? Choose three.

A. 3005

B. 3020

C. 3030

D. 3060

E. 3080

F. 3090

Answer: CDE

17. What are the SAFE guidelines when routing information is exchanged with an outside routing domain? (Select two.)

A. Use exterior gateway protocols only.

B. Use exterior gateway protocols that operate between routing domains and do not allow administrators to build and act on policies.

C. Use exterior gateway protocols because they allow administrators to build and act on policies rather

than just on reachability information.

D. Do not use autonomous system path filters on every EBGP peering session in network.

E. Use exterior gateway protocols or static routes

F. Make certain that your outside peer advertises your routes to other peers for maximum reachability

Answer: AC

18. What services does EAP provide?

A. EAP provides wireless gateway and complementary code keying.

B. EAP provides centralized authentication and dynamic key distribution.

C. EAP provides open authentication and shared key distribution

D. EAP provides message integrity check and wireless domain service

Answer: B

19. What is not a specific type of attack, but refers to most attacks that occur today?

A. DoS

B. brute force password

C. IP spoofing

D. unauthorized access

Answer: D

20. How are virus and Trojan Horse attacks mitigated in the SAFE SMR midsize network design corporate Internet module?

A. filtering at the ISP, edge router, and corporate firewall

B. IDS at the host and network levels

C. e-mail content filtering, HIDS, and host-based virus scanning

D. OS and IDS detection

E. CAR at the ISP edge and TCP setup controls at the firewall

F. RFC 2827 and 1918 filtering at ISP edge and midsize network edge router

Answer: C