

Exam : Cisco 642-542

Title : Cisco SAFE Implementation (CSI)

Update : Demo

1.drag drop

Match the following Internet worms to their characteristics.

exploits a flaw in the remote-procedure call code that deals with message exchange over TCP/IP in Microsoft Windows systems	Code Red
targets Microsoft SQL Server software	Nimda
a hybrid that spreads by using vectors as e-mail, network shares, JavaScript, and infected hosts	MS Blaster
targets Microsoft Windows IIS using vulnerability in the IS Indexing Service	SQL Slammer

Correct:

Green choice2---->Yellow Choice2

Green choice3---->Yellow Choice1

Green choice1---->Yellow Choice4

Green choice4---->Yellow Choice3

2.If split tunneling is disabled, how do remote users access the Internet when they have a VPN tunnel established in the software access option in the SAFE SMR remote user design environment?

- A.access to the Internet is not allowed
- B.the user must disable the VPN tunnel to access the Internet
- C.access to the Internet is provided via the corporate connection
- D.access to the Internet is provided via the ISP connection

Correct:C

3.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

Correct:D

4.Which command implements Unicast RPF IP spoofing protection?

- A.access-list
- B.access-group
- C.ip verify reverse-path interface
- D.tcp verify reverse-path interface
- E.udp verify reverse-path interface

Correct:C

5.What does CBAC dynamically create and delete?

- A.TCP sessions
- B.crypto maps

-
- C.access control lists
 - D.security control lists

Correct:C

6.What is the function of a crypto map on a PIX Firewall?

- A.to define the policy that will be applied to the traffic
- B.to specify which algorithms will be used with the selected security protocol
- C.to configure a pre-shared authentication key and associate the key with an IPSec peer address or host name
- D.to map transforms to transform sets

Correct:A

7.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

Correct:D E

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

- A.4210
- B.4220
- C.4250
- D.4260

Correct:C

9.How does Java applet filtering distinguish between trusted and untrusted applets?

- A.examines the applet for suspicious code
- B.relies on a list of applets that you designate as hostile
- C.relies on a list of applets that you designate as friendly
- D.relies on a list of external sites that you designate as friendly

Correct:D

10.What are three steps of the Security Wheel? Choose three.

- A.improve
- B.log
- C.maintain
- D.test
- E.secure
- F.report

Correct:A D E

11.What is the primary identity component in a Cisco security solution?

- A.Cisco VPN Concentrators
- B.Cisco PIX Firewalls
- C.Cisco IDS Sensors
- D.Cisco Access Control servers

E. Cisco IOS Firewalls

Correct: D

12. Which threats are expected in the SAFE SMR remote user network environment? Choose two.

- A. trust exploitation
- B. port redirection attacks
- C. man in the middle attacks
- D. network reconnaissance

Correct: C D

13. Which techniques does SAFE recommend to mitigate MAC spoofing attacks? (Select two.)

- A. Use port security.
- B. Implement IP Source Guard feature.
- C. Set all user ports to nontrunking mode.
- D. Implement BPDU guard enhancement command.
- E. Implement authentication for DHCP messages.
- F. Use DHCP snooping along with DAI.

Correct: A F

14. Which are key devices in the SAFE SMR remote user network? Choose three.

- A. Layer 2 switch
- B. router with firewall and VPN support
- C. Layer 3 switch
- D. firewall with VPN support
- E. NIDS
- F. personal firewall software

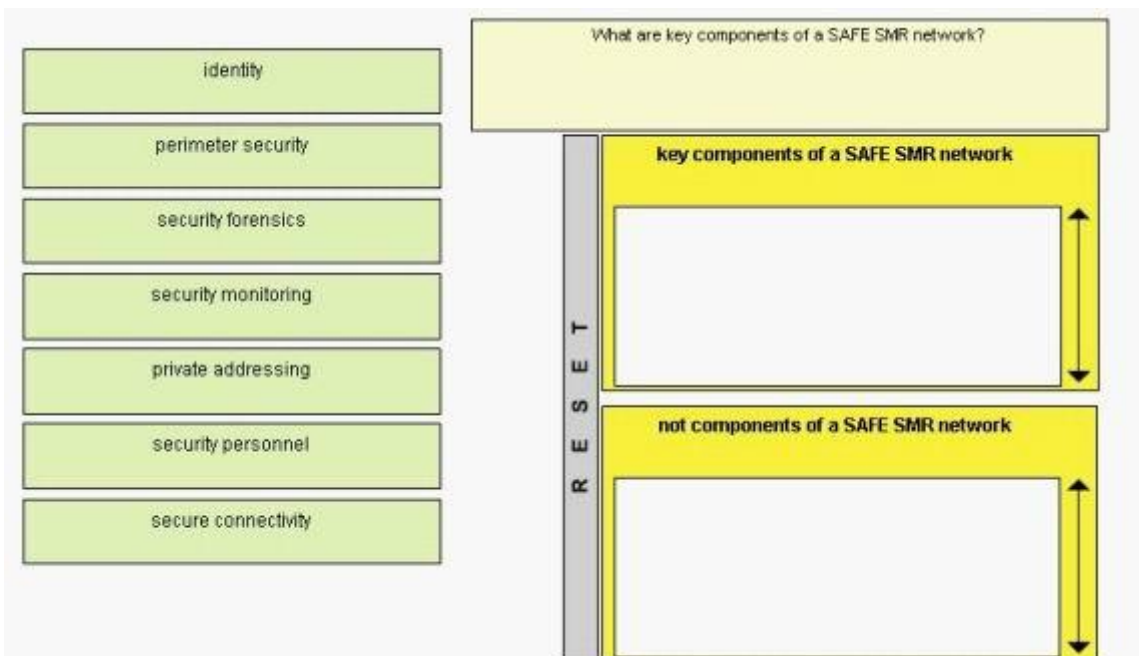
Correct: B D F

15. How are packet sniffer attacks mitigated in the SAFE SMR small network corporate Internet module?

- A. RFC 2827 and 1918 filtering at ISP edge and local firewall
- B. switched infrastructure and HIDS
- C. protocol filtering
- D. restrictive trust model and private VLANs
- E. restrictive filtering and HIDS

Correct: B

16. drag drop



Correct:

Green choice1---->Yellow Choice1

Green choice2---->Yellow Choice2

Green choice4---->Yellow Choice3

Green choice7---->Yellow Choice4

Green choice3---->Yellow Choice5

Green choice5---->Yellow Choice6

Green choice6---->Yellow Choice7

17.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

Correct:C D E

18.What are the three modules in the SAFE SMR midsize network design? Choose three.

- A.frame/ATM module
- B.campus module
- C.ISP edge module
- D.corporate Internet module
- E.WAN module
- F.PSTN module

Correct:B D E

19.What threats are expected for the SAFE SMR small network campus module? Choose two.

- A.IP spoofing

-
- B.packets sniffers
 - C.denial of service
 - D.applications layer attacks

Correct: B D

20. When using PC-based IP phones, which threat is expected between data and voice segments if not protected by a stateful firewall?

- A. TCP flood DoS attack
- B. IP spoofing attack
- C. UDP flood DoS attack
- D. application layer attack

Correct: C

21. Which IDS guidelines should be followed, according to SAFE SMR?

- A. use TCP shunning as opposed to TCP resets
- B. use shunning no longer than 15 minutes
- C. use shunning on only UDP traffic, as it is more difficult to spoof than TCP
- D. use shunning on only TCP traffic, as it is more difficult to spoof than UDP

Correct: D

22. What are the radio frequency bands used by IEEE 802.11 standards? Choose two.

- A. 2.8 MHz
- B. 2.4 GHz
- C. 2.2 MHz
- D. 5 GHz
- E. 900 GHz
- F. 900 MHz

Correct: B D

23. Using the default, how does the Cisco IDS appliance log events? Choose two.

- A. location
- B. type
- C. rule base
- D. effect
- E. severity
- F. user option

Correct: B E

24. What does the Cisco Unified Client framework provide?

- A. distributed push policy technology
- B. centralized push policy technology
- C. centralized pull policy technology
- D. multi-tiered policy technology

Correct: B

25. drag drop

According to SAFE best practices for routing protocols, which items are examples of disrupting peering attacks?

masquerading as a member of the routing domain

compromising a valid member of the routing domain

port flooding

misdirecting traffic to form a routing loop

modifying routing information passed between routers

misdirecting traffic to a black hole

misdirecting traffic to a monitoring point

protocol semantics peering attacks

Correct:

Green choice3---->Yellow Choice1

Green choice8---->Yellow Choice2

Green choice2---->Yellow Choice3

Green choice1---->Yellow Choice4

Green choice5---->Yellow Choice5

26.What are private VLANs?

A.tools that allow segregating traffic at Layer 3, turning broadcast segments into non-broadcast, multi-access-like segments

B.tools that allow segregating traffic at Layer 2, turning broadcast segments into non-broadcast, multi-access-like segments

C.tools that allow segregating traffic at Layer 2, turning non-broadcast, multi-access-like segments into broadcast segments

D.tools that allow segregating traffic at Layer 3, turning non-broadcast, multi-access-like segments into broadcast segments

Correct:B

27.What is the primary method for device authentication in a VoIP network?

A.IP address

B.MAC address

C.SIP address

D.IP and MAC address

Correct:B

28.Which three authentication methods are supported by CSACS? Choose three.

A.PPP

B.RADIUS

C.CHAP

D.TACACS+

E.PAP

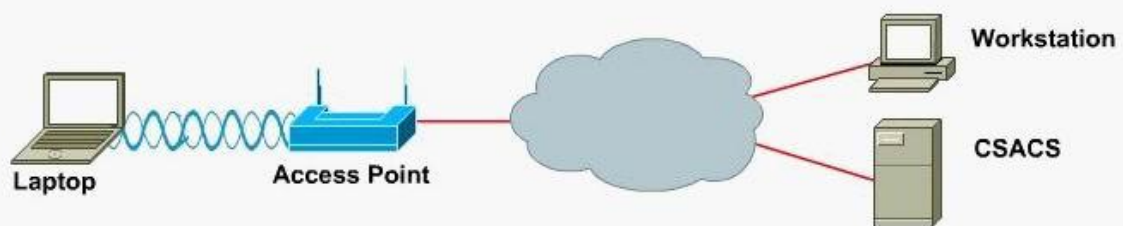
F.static passwords

Correct:B D F

29.lab

Amiable Hotel has moved a wireless access point from Houston to Austin. Your task is to configure the access point with the necessary parameters for access at the new location. 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 were pre-configured in Houston and do not need to be changed.

- 1200 Wireless access point 172.16.133.21 255.255.255.0
- Wireless Client Adapter 172.16.133.15 255.255.255.0
- CSACS 172.16.133.50 255.255.255.0
- Server Name/IP: 172.16.133.50
- Server Type: RADIUS
- Port: 1645
- Shared Secret: everythingsecret
- Authentication Type: EAP
- WEP Key Size: 128 bit
- WEP Key: 12345678901234567890abcdef
- Encryption: Full



eSim Professional v1.0

Hide Scenario

00:00:02

Correct:

30.What service is provided by CSA Profiler?

- A.Profiler analyzes applications to help in generating useful policies.
- B.Profiler monitors and logs security events that occur on CSA protected hosts.
- C.Profiler provides a COM component utility that installs with each CSA.
- D.Profiler configures agent kits that are deployed on CSA protected hosts.

Correct:A