PASS QUESTION

QUESTION & ANSWER

HIGHER QUALITY, BETTER SERVICE

Provide One Year Free Update!

https://www.passquestion.com

Exam : **SY0-101**

Title : SECURITY+ CERTIFICATION

Version : Demo

1. A VPN typically provides a remote access link from one host to another over:

A. an intranet.

B. a modem.

C. a network interface card.

D. the Internet.
Answer: D

2. IPSec uses which of the following protocols to provide traffic security? (Select TWO).

A. SSH

B. AH

C. PPTP

D. SSL

E. L2TP

F. Encapsulating Security Protocol (ESP)
Answer: BF

3. The employees at a company are using instant messaging on company networked computers. The MOST important security issue to address when using instant messaging is that instant messaging:

A. communications are a drain on bandwidth.

B. communications are open and unprotected.

C. has no common protocol.

D. uses weak encryption.
Answer: B

4. Which of the following would be BEST to do when network file sharing is needed? (Select TWO).

A. Allow read permissions only for unauthenticated users.

B. Create local users who have no access to the shares.

C. Allow access to administrators only.

D. Place the share on a different volume than the operating system.

E. Set a disk quota.
Answer: DE

5. Which of the following programming techniques should be used to prevent buffer overflow attacks?

A. Input validation

B. Nested loops

C. Signed applets

D. Automatic updates
Answer:A

6. A large company wants to deploy an FTP server to support file transfers between business customers and partners. Which of the following should the security specialist consider before making these changes?

A. FTP can be deployed on an isolated server but is unencrypted.

B. FTP can consume significant bandwidth.

C. FTP facilitates business-to-business file transfers and has few risks.

D. FTP transfers data in an unencrypted format.
Answer: D

7. WEP uses which of the following stream ciphers?

A. RC2

B. RC4

C. IKE

D. 3DES
Answer: B

8. A common tool used for wireless sniffing and war driving is:

A. S/MIME.

B. Sam Spade.

C. NetStumbler.

D. NESSUS.
Answer: C

9. Which of the following is a common type of attack on web servers?

A. Birthday

B. Buffer overflow

C. Spam

D. Brute force
Answer: B

10. Which of the following would be needed to ensure that a user who has received an email cannot claim that the email was not received?

A. Anti-aliasing

B. Data integrity

C. Asymmetric cryptography

D. Non-repudiation
Answer: D

11. Spam is considered a problem even when deleted before being opened because spam:

A. verifies the validity of an email address.

B. corrupts the mail file.

C. wastes company bandwidth.

D. installs Trojan horse viruses.
Answer: C

12. In order to secure web-based communications, SSL uses: (Select TWO).

A. PPP.

B. IPSec.

C. Public-key cryptography.

D. Blowfish encryption.

E. Symmetric cryptography.

F. Challenge Handshake Authentication Protocol (CHAP).
Answer: CE

13. A URL for an Internet site begins with 'https:' rather than 'http:' which is an indication that this web site uses:

A. Kerberos.

B. PGP.

C. PKI.

D. SSL.
Answer: D

14. To reduce vulnerabilities on a web server, an administrator should adopt which of the following preventative measures?

A. Use packet sniffing software on all inbound communications.

B. Apply the most recent manufacturer updates and patches to the server.

C. Enable auditing on the web server and periodically review the audit logs.

D. Block all Domain Name Service (DNS) requests coming into the server.
Answer: B

15. A VPN is needed for users to connect to a remote site and the VPN must be transparent to the user. Which of the following VPN models would be BEST to use?

A. Gateway to Gateway

B. Host to Host

C. Host to Gateway

D. Gateway to Host
Answer:A

16. A web page becomes unresponsive whenever the embedded calendar control is used. Which of the following types of vulnerabilities is occurring?

A. Common Gateway Interface (CGI)

B. ActiveX

C. Cross-site scripting

D. Cookies
Answer: B

17. A company is upgrading the network and needs to reduce the ability of users on the same floor and network segment to see each other's traffic. Which of the following network devices should be used?

A. Router

B. Hub

C. Switch

D. Firewall
Answer: C

18. Which of the following would be the MOST important reason to apply updates?

A. Software is a licensed product and the license will expire if not updated.

B. Software is a supported product and vendors won't support the product if the latest version is not installed.

C. Software is a productivity facilitator and as new functionality is available the functionality must be enabled.

D. Software is inherently insecure and as new vulnerabilities are found the vulnerabilities must be fixed.
Answer: D

19. Which of the following types of firewalls provides inspection at layer 7 of the OSI model?

A. Application-proxy

B. Network address translation (NAT)

C. Packet filters

D. Stateful inspection
Answer:A

20. A company implements an SMTP server on their firewall. This implementation would violate which of the following security principles?

A. Keep the solution simple.

B. Use a device as intended.

C. Create an in-depth defense.

D. Address internal threats.
Answer: B