FCNS FOR REVIEW

1. Which of the following are a benefit of removing unused or unneeded services and protocols?
   - 0 ✗ A. More machine resource availability
   - 0 ✗ B. More network throughput
   - 0 ✗ C. Less need for administration
   - 0 ✓ D. More Security
2. 2.

   Which is the most important reason for the removal of unused, unnecessary, or unneeded protocols, services, and applications?

   - 0 ✓ A. Increased security
   - 0 ✗ B. Increased performance
   - 0 ✗ C. Less need for administration
   - 0 ✗ D. Less machine resource use.
3. 3.

   The component of a DDoS attack that sends commands to DDoS zombie agents is known as a _____.

   - 0 ✗ A. System Commander
   - 0 ✗ B. Console
   - 0 ✓ C. Master
   - 0 ✗ D. Rootkit
4. 4.

   The act of attempting to appear to be someone you're not in order to gain access to a system is known as which of the following?

   - 0 ✓ A. Spoofing
   - 0 ✗ B. DDoS
   - 0 ✗ C. Replay
   - 0 ✗ D. Sniffing
5. 5.

   Which of the following is most likely to make systems vulnerable to MITM attacks?

   - 0 ✗ A. Weak passwords
   - 0 ✓ B. Weak TCP sequence numbers
   - 0 ✗ C. Authentication misconfiguration on routers
   - 0 ✗ D. Use of the wrong operating systems\

6. 6.

   Which of the following is the best way to protect your organization from revealing sensitive information through dumpster diving?

   - 0 ✗ A. Establish a policy requiring employees to change passwords every 30 to 60 days.
   - 0 ✓ B. Teach employees the value of not disclosing restricted information over the telephone to unknown parties.
   - 0 ✗ C. Add a new firewall to the network.
   - 0 ✗ D. Shred all sensitive documentation.

7. 7.

   The use of VPNs and _____ have enabled users to be able to telecommute.

   - 0 ✓ A. PGP
   - 0 ✗ B. S/MIME
   - 0 ✗ C. Wireless NICs
   - 0 ✗ D. RASs

8. 8.

   PDAs, cell phones, and certain network cards have the ability to use _____ networks. Choose the BEST answer.

   - 0 ✗ A. Wired
   - 0 ✓ B. Private
   - 0 ✗ C. Wireless
   - 0 ✗ D. Antique

9. 9.

   There are three recognized levels of hacking ability in the Internet community. The first is the skilled hacker, who writes the programs and scripts that script kiddies use for their attacks. Next comes the script kiddie, who knows how to run the scripts written by the skilled hackers. After the script kiddies come the _____, who lack the basic knowledge of networks and security to launch an attack themselves.

   - 0 ✓ A. Web kiddies
   - 0 ✗ B. Clickers
   - 0 ✗ C. Click kiddies
   - 0 ✗ D. Dunce kiddies

10. 10.

    Your supervisor has charged you with determining which 802.11 authentication method to use when deploying the new wireless network. Given your knowledge of the 802.11 specification, which of the following is the most secure 802.11 authentication method?

    - 0 ✗ A. Shared-key
    - 0 ✓ B. EAP-TLS
    - 0 ✗ C. EAP-MD5
    - 0 ✗ D. Open

11. 11.

    What are the two WEP key sizes available in 802.11 networks?

    - 0 ✗ A. 40-bit and 104-bit
    - 0 ✗ B. 24-bit and 64-bit
    - 0 ✓ C. 64-bit and 128-bit
    - 0 ✗ D. 24-bit and 104-bit

12. 12.

    Which of the following is a weakness in WEP related to the IV?

    - 0 ✗ A. The IV is a static value, which makes it relatively easy for an attacker to brute force the WEP key from captured traffic.
    - 0 ✗ B. The IV is transmitted in plaintext and can be easily seen in captured traffic.
    - 0 ✓ C. The IV is only 24 bits in size, which makes it possible that two or more data frames will be transmitted with the same IV, thereby resulting in an IV collision that an attacker can use to determine information about the network.
    - 0 ✗ D. There is no weakness in WEP related to the IV.

13. 13.

    You are creating a DMZ for a company and need to allow external users to access Web servers in the DMZ using HTTP/S as well as allow internal users to access the same Web servers using standard HTTP. What is the best way to configure the external and internal firewalls to meet these requirements?

    - 0 ✗ A. Open port 80 on the external firewall and port 443 on the internal firewall.
    - 0 ✓ B. Open port 443 on the external firewall and port 80 on the internal firewall.
    - 0 ✗ C. Open port 80 on the external firewall and port 110 on the internal firewall.
    - 0 ✗ D. Open port 110 on the external firewall and port 80 on the internal firewall.

14. 14.

    When you use Java, the JVM isolates the Java applet to a sandbox when it executes. What does this do to provide additional security?

    - 0 ✗ A. This prevents the Java applet from accessing data on the client's hard drive.
    - 0 ✓ B. This prevents the Java applet from communicating to servers other than the one from which it was downloaded.
    - 0 ✗ C. This prevents the Java applet from failing in such a way that the Java applet is unable to execute.
    - 0 ✗ D. This prevents the Java applet from failing in such a way that it affects another application.

15. 15.

    You are setting up a test plan for verifying that new code being placed on a Web server is secure and does not cause any problems with the production Web server. What is the best way to test the code prior to deploying it to the production Web server?

    - 0 ✗ A. Test all new code on a development PC prior to transferring it to the production Web server.

- 0 ✔ B. Test all new code on an active internal Web server prior to transferring it to the production Web server.
- 0 ✖ C. Test all new code on a duplicate Web server prior to transferring it to the production Web server.
- 0 ✖ D. Test all new code on another user's PC prior to transferring it to the production Web server.

16. 16.

    To allow its employees remote access to the corporate network, a company has implemented a hardware VPN solution. Why is this considered a secure remote access solution?

    - 0 ✖ A. Because only the company's employees will know the address to connect to in order to use the VPN.
    - 0 ✖ B. Because VPNs use the Internet to transfer data.
    - 0 ✖ C. Because a VPN uses compression to make its data secure.
    - 0 ✔ D. Because a VPN uses encryption to make its data secure.

17. 17.

    The network team at your company has placed a sniffer on the network to analyze an ongoing network-related problem. The team connects to the sniffer using Telnet to view the data going across the network. What would you recommend to increase the security of this connection without making it significantly more difficult for the network team members to do their jobs?

    - 0 ✖ A. Require the network team to remove the sniffer immediately.
    - 0 ✖ B. Require the network team to view the data from the local console of the sniffer.
    - 0 ✖ C. Encrypt the connection to the sniffer using PAP.
    - 0 ✔ D. Use SSH to make the connection to the sniffer rather than Telnet.

18. 18.

    Some new servers are being installed on your company's network and you have been asked to work with the installer to ensure that they are as secure as possible from hack attempts. What is the most important step you should take to ensure that the servers' OSs is secure?

    - 0 ✖ A. Make sure that the installer is certified.
    - 0 ✖ B. Make sure that the latest OS service pack is installed.
    - 0 ✔ C. Make sure that the latest OS service pack and all security patches are installed.
    - 0 ✖ D. Make sure that the servers have locks on the hot-swap drive chassis.

19. 19.

    What types of computers might you expect to find located on an intranet?

    - 0 ✖ A. Publicly accessible DNS servers and Public Web servers
    - 0 ✖ B. Public Web servers and SQL 2000 servers
    - 0 ✔ C. SQL 2000 servers and User workstations
    - 0 ✖ D. User workstations and Publicly accessible DNS servers

20. 20.

    Which of the following protocols can be used to secure a VPN connection?

    - 0 ✔ A. TCP/IP
    - 0 ✖ B. DNS

- 0 ✗ C. MPPE
- 0 ✗ D. Apple Talk

21. 21.

Sally has come to you for advice and guidance. She is trying to configure a network device to block attempts to connect on certain ports, but when she finishes the configuration, it works for a period of time but then changes back to the original configuration. She cannot understand why the settings continue to change back. When you examine the configuration, you find that the _____ are incorrect, and are allowing Bob to change the configuration, although he is not supposed to operate or configure this device. Since he did not know about Sally, he kept changing the configuration back.

- 0 ✗ A. MAC settings
- 0 ✗ B. DAC settings
- 0 ✗ C. ACL settings
- 0 ✓ D. Permissions

22. 22.

Josh has asked for a clarification of what a firmware update is. How could you briefly describe for him the purpose of firmware updates?

- 0 ✓ A. Firmware updates are control software- or BIOS-type updates that are installed to improve the functionality or extend the life of the device involved.
- 0 ✗ B. Firmware updates are device-specific command sets that must be upgraded to continue operation.
- 0 ✗ C. Firmware updates update the mechanical function of the device.
- 0 ✗ D. Firmware updates are minor fixes, and are not usually necessary.

23. 23.

Your FTP server was just compromised. When you examine the settings, you find that the server allows Anonymous access. However, you know that this is a default condition in most FTP servers, and must dig further for the problem. Where else might you check?

- 0 ✗ A. Access permissions on server's file structure
- 0 ✗ B. ACL settings for server access
- 0 ✗ C. Effective permissions for the anonymous access
- 0 ✓ D. All of the above

24. 24.

You have downloaded a CD ISO image and want to verify its integrity. What should you do?

- 0 ✗ A. Compare the file sizes.
- 0 ✗ B. Burn the image and see if it works.
- 0 ✓ C. Create an MD5 sum and compare it to the MD5 sum listed where the image was downloaded.
- 0 ✗ D. Create an MD4 sum and compare it to the MD4 sum listed where the image was downloaded.

25. 25.

If you wanted to encrypt a single file for your own personal use, what type of cryptography would you use?

- 0 ✗ A. A proprietary algorithm
- 0 ✓ B. A digital signature
- 0 ✗ C. A symmetric algorithm
- 0 ✗ D. An asymmetric algorithm

26. 26.

Which of the following algorithms are available for commercial use without a licensing fee?

- 0 ✗ A. RSA, DES, and IDEA
- 0 ✗ B. DES, IDEA, and AES
- 0 ✗ C. IDEA, AES, and RSA
- 0 ✓ D. RSA, DES, and AES

27. 27.

The PKI identification process is based upon the use of unique identifiers, known as _____.

- 0 ✗ A. Licences
- 0 ✗ B. Fingerprints
- 0 ✓ C. Keys
- 0 ✗ D. Locks

28. 28.

Public Key Cryptography is a system that uses a mix of symmetric and _____ algorithms for the encryption of a secret key.

- 0 ✗ A. Public
- 0 ✓ B. Asymmetric
- 0 ✗ C. Private
- 0 ✗ D. Certificate

29. 29.

Your certificate and keys are about to expire. As long as the certificate is in good standing, you can use your existing key to sign your request to _____ your keys.

- 0 ✓ A. Revoke
- 0 ✗ B. Renew
- 0 ✗ C. Reinitialize
- 0 ✗ D. Redistribute

30. 30.

When a company uses _____, it is keeping copies of the private key in two separate secured locations where only authorized persons are allowed to access them.

- 0 ✓ A. Key escrow
- 0 ✗ B. Key destruction
- 0 ✗ C. Key generetion

- 0 ✗ D. Key rings

31. 31.

    You are the first person to respond to the scene of an incident involving a computer being hacked. After determining the scope of the crime scene and securing it, you attempt to preserve any evidence at the scene. Which of the following tasks will you perform to preserve evidence?

    - 0 ✗ A. Photograph any information displayed on the monitors of computers involved in the incident
    - 0 ✓ B. Document any observations or messages displayed by the computer.
    - 0 ✗ C. Shut down the computer to prevent further attacks that may modify data.
    - 0 ✗ D. Gather up manuals, nonfunctioning devices, and other materials and equipment in the area so they are ready for transport.

32. 32.

    You are the first to arrive at a crime scene in which a hacker is accessing unauthorized data on a file server from across the network. To secure the scene, which of the following actions should you perform?

    - 0 ✗ A. Prevent members of the organization from entering the server room.
    - 0 ✗ B. Prevent members of the incident response team from entering the server room.
    - 0 ✗ C. Shut down the server to prevent the user from accessing further data.
    - 0 ✓ D. Detach the network cable from the server to prevent the user from accessing further data.

33. 33.

    You are the first person to arrive at a crime scene. An investigator and crime scene technician arrive afterwards to take over the investigation. Which of the following tasks will the crime scene technician be responsible for performing?

    - 0 ✗ A. Ensure that any documentation and evidence they possessed is handed over to the investigator.
    - 0 ✗ B. Reestablish a perimeter as new evidence presents itself.
    - 0 ✗ C. Establish a chain of command.
    - 0 ✓ D. Tag, bag, and inventory evidence.

34. 34.

    When evidence is acquired, a log is started that records who had possession of the evidence for a specific amount of time. This is to avoid allegations that the evidence may have been tampered with when it was unaccounted for, and to keep track of the tasks performed in acquiring evidence from a piece of equipment or materials. What is the term used to describe this process?

    - 0 ✗ A. Chain of command
    - 0 ✓ B. Chain of custody
    - 0 ✗ C. Chain of jurisdiction
    - 0 ✗ D. Chain of evidence

35. 35.

    You are manager of the IT department and have designed a new security policy that addresses the IT staff's responsibilities to users, equipment, and data. The policy only affects the IT staff. It

deals with such issues as routine backups of data, network security changes, and audits of data on servers. Now that the new policy is written, which of the following should you do next?

- 0 ✗ A. Publish the policy and make it available for all users to read.
- 0 ✗ B. Obtain authorization from other members of the IT staff.
- 0 ✓ C. Obtain authorization from senior management.
- 0 ✗ D. Provide a copy of the policy to legal counsel, and have them review its content and wording.