CYBER SECURITY

Overview
This event provides recognition for FBLA members who understand security needs for technology.

This is an individual objective test.

Competencies and Task Lists
http://www.fbla-pbl.org/docs/ct/FBLA/CYBERSECURITY.pdf

Web Site Resources

- An Overview of Cryptography
  http://www.garykessler.net/library/crypto.html
- Cyber Security Tips
  http://www.us-cert.gov/cas/tips/
- How Firewalls Work
  http://www.howstuffworks.com/firewall.htm

CYBER SECURITY SAMPLE QUESTIONS

1. What is the attack called in which the aggressor poses as the victim's legitimate DNS server?
   a. Web spoofing
   b. man in the middle
   c. DNS spoofing
   d. ARP poisoning

2. What technique is used so that a file is encoded so only the intended recipient may read the original contents?
   a. encryption
   b. password
   c. algorithm
   d. key

3. What allows you to pass reserved IP address through a public network that otherwise would not accept them?
   a. authentication
   b. tunneling
   c. VPN
   d. cipher

4. The _____ studies security issues and provides publications and alerts to help educate the public to threats facing information.
   a. IETF
   b. CERT/CC
   c. ISOC
   d. IESG

5. Packet sniffing can be used to obtain username and password information in clear text from which of the following?
   a. FTP (File Transfer Protocol)
   b. SSH (Secure Shell)
   c. SSL (Secure Sockets Layer)
   d. HTTPS (Hypertext Protocol over Secure Sockets Layer)

6. For system logging to be an effective security measure, an administrator must:
   a. implement circular logging
   b. configure SNMP (Simple Network Management Protocol) traps for logging events
   c. configure the system to shutdown when the logs are full
   d. review the logs on a regular basis

7. When an attacker targets an e-mail communication that uses POP3, which TCP port is he or she likely to use in the attack?
   a. 110
   b. 35
   c. 125
   d. 18

8. Information like financial information, product designs, and business strategies are classified as ____ by most organizations.
   a. secure
   b. secret
   c. sensitive
   d. classified

9. When an attacker modifies the transaction log, ____ is the target.
   a. integrity
   b. information
   c. accountability
   d. availability

10. The IDS signature that is based on the packet's TCP or UDP port is called:
    a. sensor signature
    b. NIDS
    c. port signature
    d. IP session logging

11. What does HTTPS stand for?
    a. Hypertext Transfer Protocol Software
    b. Hypertext Transfer Protocol Shell
    c. Hypertext Transfer Protocol System
    d. Hypertext Transfer Protocol Secure

12. What type of lock blocks access to disk drives or serial ports?
    a. preset lock
    b. slot lock
    c. cable trap
    d. port controls

13. What type of lock covers and controls on/off switches?
    a. switch control
    b. port lock
    c. slot lock
    d. switch lock

14. What is a common major hash function in use today that is in the public domain and requires no licensing?
    a. MD1
    b. SHA-1
    c. SHA-2
    d. MD5

15. A database that allows users to submit and retrieve digital certificates is called a(n):
    a. certificate server
    b. block algorithm
    c. distinguished name
    d. web of trust

16. What is another name for a public key algorithm, a method that uses different encryption and decryption keys?
    a. stream algorithm
    b. block algorithm
    c. symmetric algorithm
    d. asymmetric algorithm

17. The most important configuration file on your firewall is the____ file.
    a. access list
    b. data
    c. filter
    d. rules

18. Which type of cable is most difficult for an intruder to tap into without calling attention to his action?
    a. thin coax
    b. shielded twisted pair
    c. fiber optic
    d. thick coax

19. _____ protects files and databases in case of an unexpected system crash or power failure by backing out of a data entry that is not fully completed before the system goes down, keeping the file from being corrupted.
    a. The Transaction Tracking System
    b. Parallel Processing
    c. A standby UPS
    d. Net Ware File Synchronization

20. In _____ packet filtering the firewall examines every individual packet and decides whether to pass or block the packet, depending on the packet's content.
    a. stateful
    b. network
    c. static
    d. stateless

21. When you receive an e-mail that warns you of a virus and that encourages you to forward the message to all your friends, you should:
    a. forward it to everyone in your address book
    b. delete it
    c. forward it to your boss
    d. forward it to the local police

22. Which one of the following is **not** true of a service pack from Microsoft?
    a. A service pack can be downloaded from Microsoft's Web site or obtained as a CD-ROM.
    b. You should back up your system before installing a service pack.
    c. If there are several service pack versions, the most recent version also includes all previous versions.
    d. Only one service pack is issued at a time, and there are options in that service pack so that it can be applied to any Microsoft operating system.

23. The ____ mode of DES uses a previously-generated ciphertext as input to DES.
    a. cipher block chaining
    b. output feedback
    c. electronic code book
    d. cipher feedback

24. A(n) _____ is a device that provides power to electronic devices for a limited time period when the power goes out.
    a. NIC
    b. RAID
    c. USB
    d. UPS

25. _____ are people who use and create software for enjoyment or to gain access to information illegally.
    a. Surfers
    b. Contenders
    c. Hackers
    d. Lockers

26. RAID 4 is _____ -level stripping of data in which the data are stored in segments on dedicated data drives, and parity information is stored on a separate drive.
    a. incremental
    b. byte
    c. bit
    d. word

27. What method would an attacker use to attempt to penetrate a company's network through its remote access system?
    a. war driving
    b. PBX sniffing
    c. war dialing
    d. network sniffing

28. A _____ is a computer that is located between a computer on an internal network and computer on an external network with which the internal computer is communicating.
    a. Web server
    b. gateway
    c. proxy
    d. server

29. In the _____, any e-mail user can sign another user's digital certificate, thus vouching for that public key.
    a. trustworthy Web
    b. pretty good Web
    c. web of privacy
    d. web of trust

30. Which one of the following is a mechanism that can protect against repudiation attacks?
    a. smart cards
    b. backups
    c. digital signatures
    d. failovers