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

This is an individual online test.

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

Website Resources

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

CYBER SECURITY SAMPLE QUESTIONS

1. _____ encompasses spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs apart from viruses that are designed to harm the performance of computers on your network.
   a. Grayware
   b. Spyware
   c. Adware
   d. Malware

   Competency: Defend and Attack

2. _____ is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.
   a. Buffer overflow
   b. Spamtrap
   c. Fast flux
   d. DNS hosting

   Competency: Defend and Attack

3. In computer networking, a _____ is a network route (routing table entry) that goes nowhere.
   a. bottleneck route
   b. core route
   c. null route (blackhole route)
   d. network route

   Competency: Defend and Attack

4. A rootkit variant called a bootkit is used predominantly to attack _____systems, such as in the Evil Maid Attack of 2004.
    a. full disk encryption
    b. Active Directory
    c. hard drive
    d. boot Sector

    Competency: Defend and Attack

5. What is the **best** way to configure a router against a denial of service attack?
    a. packet sniffing
    b. non-standard port management
    c. default passwords
    d. configure router to use WPA encryption

    Competency: Defend and Attack

6. _____, networks of virus-infected computers, are used to send about 80 percent of spam.
    a. Zombie computers
    b. Botnets
    c. SMTP mail relays
    d. Spammers

    Competency: Defend and Attack

7. Windows Vista and Windows 7 changes to security have made it a little more difficult for spammers and hackers to send viruses, worms, spyware, and Trojans by introducing a privilege elevation system called _____, and if used properly will allow you to sign on as a standard user with only basic privileges assigned, this way you do **not** have the administrators rights to download or install malicious content from the Internet.
    a. User Accounts
    b. Limited Account Control
    c. User Account Control
    d. Multi-User Account Control

    Competency: Defend and Attack

8. _____ helps network security administrators and IT Managers for bandwidth monitoring, and Firewall Internet security events monitoring efficiently.
    a. Firewall Analyzer
    b. Cisco PIX
    c. Proxy Servers
    d. Cisco IOS

    Competency: Network Security

9. Network security starts from _____ the user, commonly with a username and a password.
    a. authorizing
    b. authenticating
    c. allowing
    d. accessing

    Competency: Network Security

10. Internet Explorer 8 also has developed a _____ filter potential unsafe websites you browse.
    a. SmartScreen
    b. In-Private Filtering
    c. Pop-up Blocker
    d. Caret Browsing

    Competency: Email Security

11. Which one of the following provides secure methods for IP multihoming and mobile computing?
    a. CryptoSystems
    b. simple public key infrastructure (SPKI)
    c. Transport Format Protocol
    d. Host Identity Protocol (HIP)

    Competency: Public Key

12. The _____ algorithms are used to create a mathematically related key pair: a secret private key and a published public key.
    a. cryptographic
    b. symmetric key
    c. asymmetric key
    d. digital signature

    Competency: Public Key

13. Each user has a pair of _____ , a public key, and a private key.
    a. digital signatures
    b. cryptographic keys
    c. symmetric keys
    d. asymmetric keys

    Competency: Public Key

14. An analogy to public-key encryption is that of a locked _____ with a mail slot.
    a. web of trust
    b. public key infrastructure
    c. message digest
    d. mailbox

    Competency: Public Key

15. _____is the process of verifying a user's identity.
    a. Requesting
    b. Timing
    c. Authorization
    d. Authentication

    Competency: Authentication

16. _____is a mechanism to prove that the sender really sent this message.
    a. Autoenrollment
    b. Non-repudiation
    c. Privacy
    d. Authentication

    Competency: Authentication

17. _____is the process of proving one's identity.
    a. Privacy
    b. Authentication
    c. Integrity
    d. Autoenrollment

    Competency: Authentication

18. What is the maximum lifetime for a user 10 ticket?
    a. 10 hours
    b. 5 minutes
    c. 600 minutes
    d. 7 days

    Competency: Authentication

19. What is the usual max tolerance for computer clock synchronization?
    a. 5 minutes
    b. 7 days
    c. 10 hours
    d. 600 minutes

    Competency: Authentication

20. A credential issued by the Authentication Service that supplies valid authentication credentials. Whenever the client requires access to a new network resource, it must prevent its TGT to the Key Distribution Center.
    a. ticket granting tickets
    b. user certificate
    c. authentication
    d. server credential

    Competency: Authentication

21. Scans of unique eyeball characteristics.
    a. iris/retinal scans
    b. eye masker
    c. pupil verification
    d. pupil storage

    Competency: Authentication

22. Disasters can be categorized into two broad categories.
    a. manmade and digital
    b. manmade and electronic
    c. natural and astronomical
    d. natural and manmade

    Competency: Disaster Recovery

23. _____is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it **cannot** be accessed normally.
    a. Data recovery
    b. Data corruption
    c. Storage protocol
    d. Data digestion

    Competency: Disaster Recovery

24. Which one of the following is a set of policies and procedures for reacting to and recovering from an IT-disabling disaster?
    a. business rules
    b. business continuity strategy
    c. protocoling
    d. IT watchmen

    Competency: Disaster Recovery

25. Refers to backup of computer data by automatically saving a copy of every change made to that data.
    a. backup protocol
    b. continuous data protection
    c. traditional backup
    d. non-continuous data protection

    Competency: Disaster Recovery

26. Which one of the following is a precautionary measure for preventing a disaster?
    a. all of the above
    b. fire alarms
    c. using anti-virus software
    d. HVAC controls

    Competency: Disaster Recovery

27. These controls are aimed at detecting or discovering unwanted events.
    a. detective measures
    b. preventive measures
    c. decided measures
    d. corrective measures

    Competency: Disaster Recovery

28. A state-of-the-art electronic lock:
    a. is impenetrable
    b. will never fail
    c. does not exist
    d. should have a key backup

    Competency: Physical Security

29. _____ is the science of writing in secret code and is an ancient art.
    a. Cryptography
    b. Autoenrollment
    c. Writing
    d. Networking

    Competency: Cryptography

30. _____ uses one key for encryption and another for decryption.
    a. Secret Key Cryptography (SKC)
    b. Public Key Cryptography (PKC)
    c. Hash function
    d. Keylogger

    Competency: Disaster Recovery