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/competitive-event/cyber-security-fbla/

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) What type of attack attempts to circumvent authentication mechanisms by recording authentication messages from a legitimate user and reissuing those messages in order to impersonate the user and gain access to systems?
   A) Man-in-the-Middle Attack
   B) MAC Spoofing Attack
   C) Replay Attack
   D) Scareware Attacks

   Competency: Defend and Attack

2) Spoofing is the act of falsely identifying a packet's IP address, MAC address, etc. Which one of the below are three types of Spoofing?
   A) Web Spoofing, DNS Spoofing, and Relay Spoofing
   B) DNS Spoofing, Relay Spoofing, and ARP Poisoning
   C) Web Spoofing, ARP Poisoning, and Relay Spoofing
   D) ARP Poisoning, Web Spoofing, and DNS Spoofing

   Competency: Defend and Attack

3) This is an example of malware for profit.
A) Man-in-the-Middle
B) Honeypot
C) Rootkit
D) Ransomware

Competency: Defend and Attack

4) Spam, irrelevant or inappropriate messages sent on the Internet to a large number of recipients, affects the following types of media?
A) Email, Internet, Instant Messages
B) Email, Instant Messages, Blogs
C) Email, Online Games, Blogs
D) Email, Newsgroups, Blogs

Competency: Defend and Attack

5) Remote access is a connection to a data-processing system from a remote location. A dialer program, one type of remote access tool, does what?
A) Creates a connection to another computer without the knowledge of the user.
B) Performs malicious tasks of one sort or another under remote direction.
C) Leaves a digital footprint of the data trail left by interactions in a digital environment.
D) Records the keys struck on a keyboard, usually in a covert manner.

Competency: Defend and Attack

6) Call back is an example of what type of security?
A) Scanner
B) Filter
C) Encryption
D) Remote Access

Competency: Network Security

7) What comprises a location where enterprise information systems (websites, applications, databases, data centers and servers, networks, desktops, and other endpoints) are monitored, assessed, and defended?
A) Internet Engineering Task Force
B) Information Security Operations Center
C) Information System Security Association
D) Computer Security Institute

Competency: Network Security

8) Many legislative Acts affect computer security. Laws that lay out requirements that are more stringent for retaining and protecting employee and customer data could be on the horizon. Which Act regulates the availability and breadth of group health plans and certain individual health insurance policies?
A) The Public Health Services Act (PHSA)
B) The Health Information Privacy Act (HIPA)
C) The Health Insurance Portability and Accountability Act (HIPAA)
D) The Health Information Technology for Economic and Clinical Health Act (HITECH)

Competency: Network Security

9) A demilitarized zone (DMZ) refers to a portion of the network that is **not** fully trusted. What type of network zones do administrators use when creating a DMZ?
A) securely protected
B) fully-protected
C) semi-protected
D) decentralized

Competency: Network Security

10) The human factor as it relates to technology includes physical, psychological, team, organizational, and political elements. Attackers have learned to capitalize and take advantage of the human factor in trust relationships. What type of attack uses chat, social media, and email to exploit trust relationships?
A) Chat Attack
B) Cyber Attack
C) Replay Attack
D) Online attack

Competency: Email Security

11) HTML email is the use of a subset of HTML to provide formatting and semantic markup capabilities in email that are not available with plain text. HTML email is common but dangerous. Why?
A) HTML email may not work with all clients or operating systems
B) HTML email is preferred by spammers
C) HTML email does not allow the sender to confirm the email was read
D) HTML email allows malicious code to launch from the preview pane

Competency: Email Security

12) What type of email scam involves Internet fraudsters who send seemingly legitimate e-mail messages to trick unsuspecting victims into revealing personal and financial information, such as a Social Security number (SSN), that can be used to steal the victims' identity and gain access to the victim's finances?
A) Social Engineering
B) Phishing
C) Spoofing
D) Snerting

Competency: Email Security

13) This refers to creations of the mind for which exclusive rights are recognized in law when owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs?
A) intellectual property
B) trade secrets
C) patents
D) trademarks

Competency: Intrusion Detection

14) An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. What type of IDS takes action after intruder detection?
A) passive
B) active
C) dynamic
D) static

Competency: Intrusion Detection

15) Which one of the following are Intrusion Detection tools?
A) Snort, AIDE, and OSSEC HIDS
B) BIDS, OSSEC HIDS, and LSSC HIDS
C) Snort, Bro NIDS, and BIDS
D) AIDE, Bro NIDS, and BIDS

Competency: Intrusion Detection

16) A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. What is the primary role of the Certificate Authority?
A) To use a random number generator to create public keys
B) To digitally sign and publish the public key bound to a given user
C) To review critical transactions communications between two or more parties
D) To track self-signed certificates and third party attestations of those certifications

Competency: Public Key

17) Which technology issues a challenge/response test as a means of ascertaining that a user is a human and **not** a computer program?
A) Munging
B) Site Key
C) CHAP
D) CAPTCHA

Competency: Authentication

18) A binary code represents text or computer processor instructions using the binary number system's two binary digits – 0 and 1. What is added to the end of a string of binary code that indicates whether the number of bits in the string with the value one is even or odd?
A) Parity Bit
B) Parity Word
C) Checksum
D) Modular Sum

Competency: Authentication

19) This computer network authentication protocol works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity.
A) Host Credential Authorization Protocol (HCAP)
B) NT Lan Manager (NTLM)
C) Kerberos Protocol (CNAP)
D) Web Resource Authorization Protocol (WRAP)

Competency: Authentication

20) A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. What are the three primary strategies when developing a DRP?
A) Preventive Measures, Detective Measures, and Corrective Measures
B) Management Support, Detective Measures, Preventative Measures
C) Risk Assessment, Independent Verification and Validation, Management Support
D) Corrective Measures, Detective Measures, Risk Assessment

Competency: Disaster Recovery

21) What is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced failure?
A) remote backup service
B) business continuity
C) continuous data protection
D) disaster recovery

Competency: Disaster Recovery

22) In disaster recovery, this is the point at which a management decision to react is made in reaction to a notice or other data such as a weather report or an activity report from the IT department indicating the escalation of an incident.
A) Trigger
B) Event
C) Initiate
D) Onset

Competency: Disaster Recovery

23) This provides duplication of server data storage by using multiple hard drive volumes.
A) Mirroring
B) Disk Striping
C) Parity
D) Hot Swapping

Competency: Disaster Recovery

24) This type of card is embedded with a thin strip that emits a low-frequency short-wave radio signal and can be read without inserting it into a reader device.
A) Key Card
B) Radio Frequency ID Card
C) Smart Card
D) Proximity Card

Competency: Physical Security

25) TEMPEST refers to the study of compromising emanations. Compromising emanations are defined as unintentional intelligence-bearing signals, which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment. What is the best way to protect against compromising emanations?
A) shield the computer equipment
B) limit physical access to the computer equipment
C) limit use of wireless technology
D) turn the computer equipment off when not in use

Competency: Physical Security

26) What is the primary role of a cryptologist?
A) Designing encryption algorithms
B) Performing encryption and decryption
C) Breaking encrypted text
D) Analyzing algorithms and encrypted text

Competency: Cryptography

27) Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Why is asymmetric encryption better than symmetric encryption?
A) asymmetric encryption provides an easier exchange of encryption keys
B) asymmetric encryption requires a key to be securely shared
C) asymmetric encryption provides a higher level of security
D) asymmetric encryption is faster and more efficient

Competency: Cryptography

28) When performing a computer forensics analysis, examiners must do everything possible to preserve the original media and data. Typically, this involves making a forensic image or forensic copy of the original media, and conducting our analysis on the copy versus the original. This work is an example of what?
A) Identification
B) Interpretation
C) Preservation
D) Extraction

Competency: Forensics Security

29) Which are examples of computer forensic certifications?
A) The International Society of Forensic Computer Examiners Certified Computer Examiner and the Information Assurance Certification Review Board Certified Data Recovery Professional
B) The Information Assurance Certification Review Board Certified Reverse Engineering Analyst and the International Society of Forensic Computer Examiners Certified Computer Examiner
C) The Information Assurance Certification Review Board Certified Reverse Engineering Analyst and the International Association of Computer Investigative Specialists Certified Forensic Computer Examiner
D) The International Society of Forensic Computer Examiners Certified Computer Examiner and Information Assurance Certification Review Board Certified Computer Forensics Examiner

Competency: Forensics Security

30) What is the purpose of the Computer Fraud and Abuse Act of 1986?
A) To improve the security and privacy of sensitive information in federal computer systems and to establish a minimum acceptable security practices for such systems. It requires the creation of computer security plans and the appropriate training of system users or owners where the systems house sensitive information.
B) Establishes a code of fair information practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
C) Enacted as an amendment to existing computer fraud law and written to clarify and increase the scope, while in theory, limiting federal jurisdiction to cases where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature.
D) Served as the first comprehensive revision of the US criminal code since the 1900s and extended the United States Secret Service's jurisdiction over credit card fraud and computer fraud.

Competency: Cyber Security Policy