Cyber Security

FBLA High School

FBLA High School Competitive Events Guidelines

2022–2023

Objective Test Events

Overview

These events consist of a 60-minute test administered during the National Leadership Conference (NLC).

ELIGIBILITY

Each state may submit four entries. Competitors must have paid FBLA national and state dues by 11:59 p.m. Eastern Time on March 1 of the current school year. These events are for individual competitors only.

NLC Registration

Participants must be registered for the NLC and pay the national conference registration fee to participate in competitive events.

Cyber Security

Objective Test Competencies

- Defend and attack (virus, spam, spyware)
- Network security
- Disaster recovery
- Email security
- Intrusion detection
- Authentication
- Public key
- Physical security
- Cryptography
- Forensics security
- Cyber security policy

Objective Test Guidelines

- No materials may be brought to the testing site.
- No calculators may be brought into the testing site; calculators will be provided.
- Electronic devices must be turned off and out of sight.
- Bring a writing instrument.

Competency A: Defend and Attack (virus, spam, spyware, Trojans, hijackers, worms)	Minimum: 15
Tasks	
1. Identify basic security risks and issues to computer hardware, software, and data.	
2. Define the various virus types and describe the common symptoms caused by viruses and their potential effects.	
3. Define concepts such as phishing, social engineering, spoofing, identify theft, and spamming.	
4. Describe importance and process of incidence reporting.	
5. Implement security preventive maintenance techniques such as installing service packs and patches.	
6. Assess security threats, diagnose, and troubleshoot hardware, software, and data security issues.	
7. Implement virus protection and removal procedures to recover information from failures and security breaches (e.g., malware and viral infection).	
8. Explain the impact of malware protection, including antivirus software, spam, adware, spyware filtering, and patch management.	
9. Scan storage devices and equipment for viruses and spyware and disinfect as needed.	
10. Install and configure anti-X software (e.g., anti-virus, anti-spyware, and anti-spam).	
11. Identify potential sources of virus infection and describe methods of preventing the spread of computer virus.	
12. Identify how to protect privacy and personal security online (e.g., to avoid fraud, identity theft and other hazards).	
13. Explain the benefits and demonstrate the use of privacy, password, and protection utilities.	

Competency B: Network Security	Minimum: 15
Tasks	
1. Explain the importance of network security (e.g., ethics and rights).	
2. Explain principles of basic network security (e.g., IP spoofing, packet sniffing, password compromise, and encryption).	
3. Determine threats and analyze risks to network perimeters.	
4. Determine the impact on network functionality of a particular security implementation (e.g., port blocking/filter, authentication, and encryption).	
5. Identify the following security protocols and describe their purpose and function: IPSEC, L2TP, SSL, WEP, WPA, and 802.1x.	
6. Identify specific access levels that need to be accommodated.	
7. Match security system design to identified security requirements.	
8. Develop, document and implement a network security plan (e.g., install, configure, upgrade, and optimize security).	
9. Train users about malicious software prevention technologies.	
10. Diagnose and troubleshoot hardware, software, and data security issues.	
11. Implement hardware and software network security solutions (e.g., VPN, SSL, and firewall).	
12. Identify the purposes and characteristics of access control and permissions, auditing and event logging.	
13. Know and implement user security policies and procedures to maintain, monitor, and support the security and integrity of a network.	
14. Implement secured access to network resources.	
15. Describe the importance and demonstrate forms of network security (e.g., password strategies and user accounts).	
16. Illustrate fundamental legal issues involved with security management.	
17. Design an audit policy and incident response procedures.	
18. Manage and distribute critical software updates that resolve known security vulnerabilities and other stability issues.	
19. Explain the importance of educating users and supervisors in regard to network security.	
20. Implement security controls such as MAC or DAC to ensure user policies are enabled.	
21. Implement server and Web-based services security features.	
22. Describe what a firewall is, its uses, and how it works.	
23. Explain the characteristics, uses, and benefits of software firewalls and hardware firewalls.	
24. Install and update a firewall.	
25. Configure personal firewall protection.	
26. Describe the four basic firewall techniques (e.g., proxy server, packet filter, application gateway, and circuit-level gateway).	
27. Implement global, domain, and local account policies.	
28. Distinguish among the following security methods: DMX (including dual-homed and triple-homed firewalls), VLan, intranet, extranet, PKI	

Competency C: Email Security	Minimum: 10
Tasks	
1. Identify common problems associated with electronic communication (e.g., delivery failure, junk mail, fraud hoaxes, phishing, and viruses) and recommend mitigation strategies.	
2. Define E-Mail and Instant Messaging protocol.	
3. Recognize social engineering and address social engineering situations.	
4. Identify netiquette including the use of e-mail, social networking, blogs, texting, and chatting.	
5. Explain the benefits and demonstrate the use of privacy, password, and protection utilities.	
6. Discuss security issues and guidelines for legal and responsible electronic communications and Internet use for business (e.g., includes copyright, netiquette, privacy issues, and ethics).	
7. Scan e-mail messages and attachments received to ensure they are not spam.	
8. Establish and manage spam/junk mail folders.	
9. Identify issues regarding unsolicited e-mail (spam) and how to minimize or control unsolicited mail.	
10. Identify contamination protection strategies for e-mail.	
Competency D: Intrusion Detection	**Minimum: 10**
Tasks	
1. Explain concepts such as denial of service, hacking/cracking, intrusion, and intellectual property.	
2. Assess security threats and develop plan to address.	
3. Analyze and inspect the system's configuration and vulnerabilities to detect inadvisable settings.	
4. Inspect the password files to detect inadvisable passwords.	
5. Inspect other system areas to detect policy violations.	
6. Assess system and file integrity.	
7. Recognize patterns typical of attacks.	
8. Analyze abnormal activity patterns.	
9. Track user policy violations.	
10. Demonstrate an understanding of Internet use and security issues.	
11. Investigate security issues related to Internet technology (e.g., virus, firewalls, spam, system backup, passwords, wireless, and data encryption).	
12. Identify types of intrusion detection and recommend tools to protect against each type.	

Competency E: Public Key	Minimum: 5
Tasks	
1. Define public key infrastructure.	
2. Describe the advantages and risks associated with a public key infrastructure.	
3. Identify and analyze precautions included in programs used on networks (e.g., self-metering, security keys, and required configuration settings).	
4. Explain the purpose of temporary certificates and single sign-on.	
5. Describe Web of Trust and when it is appropriate to use.	
6. Describe certificate authority and its role in security.	
7. Distinguish between public key encryption and digital signatures.	
8. Describe cryptographic protocols and applications, like digital cash, password-authenticated key agreement, multi-party key agreement, and time stamping service.	
Competency F: Authentication	**Minimum: 10**
Tasks	
1. Describe authentication process to network devices for users.	
2. Discuss the need for authentication and non-repudiation of information (e.g., PKI).	
3. Describe the steps to achieve authentication and confidentiality.	
4. Provide for user authentication (e.g., assign passwords and access level).	
5. Identify and resolve a network configuration with incorrect protocols, client software misconfiguration, authentication misconfiguration, and insufficient rights/permissions.	
6. Evaluate electronic sources of information for authenticity.	
7. Identify authentication protocols (e.g., CHAP, MS-CHAP, PAP, RADIUS, Kerbero, and EAP.)	
8. Explain and implement Secure Sockets Layer (SSL) authentication.	
9. Explain and install a certificate.	
10. Describe concepts related to logon authentication.	
11. Educate employees on how to properly handle passwords.	
12. Establish policies on choosing a secure password.	
13. Describe the biometrics authentication method.	
14. Give an example of a two-factor authentication security process.	
15. Discuss the need for dual-role authentication	

Competency G: Disaster Recovery	Minimum: 15
Tasks	
1. Identify possible effects of natural disasters on computer.	
2. Describe the purpose and characteristics of disaster recovery: backup/restore, offsite storage, hot and cold spares, and hot, warm, and cold sites.	
3. Differentiate between disaster recovery and business continuity.	
4. Design a disaster recovery plan.	
5. Compare different options of backing up and securing data and restoring a system and perform system backup.	
6. Select and test a disaster recovery plan against several disaster scenarios.	
7. Demonstrate the ability to recover operating systems (e.g., boot methods, recovery console, ASR, and ERD).	
8. Backup and restore files and directories.	
9. Implement procedures used to recover information from failures and security breaches (e.g., malware and viral infection).	
10. Identify method for avoiding common computer system disasters (e.g., UPS and RAID).	
11. Compare/contract streaming file-by-file backup systems.	
12. Establish process for archiving files.	
13. Use the features of a server operating system to prevent a disaster or recover when one occurs.	
14. Identify and maintain battery backup equipment.	
15. Install surge suppression protection.	
16. Develop and document a plan to avoid data loss, including backups and remote storage.	
Competency H: Physical Security	**Minimum: 5**
Tasks	
1. Define physical security.	
2. Identify names, purposes, and characteristics of hardware and software security issues including wireless, data, and physical security.	
3.	
4. Describe basic physical security risks inherent to computer hardware and software.	
5. Describe physical security best practices for enterprises.	
6. Describe risk-mitigation techniques (e.g., policies, procedures, hardware, and software).	
7. Establish and implement controls for physical site access and security.	
8. Identify and analyze environmental hazards (e.g., fire, flood, moisture, temperature, electricity,) and establish environmental security controls to protect and restore.	
9. Perform a physical configuration audit.	
10. Train and test employees in area of physical security awareness.	
11. Describe the physical security components of a Disaster Recovery/Business Continuity Plan	

Competency I: Cryptography	Minimum: 5
Tasks	
1. Explain the purpose of cryptography.	
2. Identify levels of encryption.	
3. Describe the types of cryptography algorithms (e.g., secret key, public key, and hash functions).	
4. Describe trust models such as web of trust, Kerberos, and certificates.	
5. Identify cryptography applications used for password protection and private communication. (IP security protocol, clipper, Identify Base Encryption, Internet Security Association and Key Management Protocol, and Secure sockets Layer).	
6. Illustrate concepts of data encryption and its use with protecting network resources.	
7. Identify uses for VPN and network data encryption.	
8. Define the advantages and risks associated with passwords.	
9. Explain how passwords are stored.	
10. Describe DES (Data Encryption Standards) and explain how it operates.	
11. Explain the purpose and use of AES (Advanced Encryption Standard).	
12. Explain export controls associated with cryptography.	
Competency J: Forensics Security	**Minimum: 5**
Tasks	
1. Review incident responses, priorities, and requirements.	
2. Identify recoverable evidence in computer hardware and mobile devices.	
3. Preserve evidence in an acceptable forensically manner.	
4. Review time line of computer files based on the creation, file modification, and file access.	
5. Identify past Internet browsing, downloads, and e-mail communications.	
6. Examine and analyze evidence.	
7. Differentiate between operating systems from a forensics standpoint.	
8. Use computer forensics software tools to cross validate findings in computer evidence-related cases.	
9. Prepare a report of findings.	
10. Identify forensic analysis tools and their uses	
11. Describe Legislative Acts governing Digital Forensics	
Competency K: Cyber Security Policy	**Minimum: 5**
Tasks	
1. Identify national legislative initiatives that affect cyber security	
2. Identify Executive Orders that affect cyber security	

References:

Career Cluster Resources for Business, Management and Administration. 2008
National Association of State Directors of Career Technical Education Consortium. Washington, DC.

Career Cluster for Information Technology. 2008. National Association of State Directors of Career Technical Education Consortium. Washington, DC.

Business Education Standards. National Business Education Association. Reston, VA.

Computer Network Software Operations, Computer Applications, Information Technology Fundamentals, and Computer Information Systems Competency-Based Tasks/Competency Lists. 2009-2010. Virginia Department of Education. Richmond, VA.

Computer Business Applications and Network Administration. 2001. Career and Technical Education. Missouri Department of Elementary and Secondary Education. Jefferson City, MO.

Networking 1, 2, 3 and 4 Course Student Profiles. 2008. South Carolina Career and Technology, South Carolina Department of Education. Columbia, SC.

Information Support Services and Networking Strands. 2007. Massachusetts VTEC Frameworks. Office for Career/Vocational Technical Education, Massachusetts Department of Elementary and Secondary Education, Malden, MA.

PC Support Courses 1, 2, 3, 4, and 5 Student Performance Standards. 2010. Florida Department of Education, Tallahassee, FL.

Information Technology Support, Georgia Standards. 2009. Career Technical and Agriculture Education, Georgia Department of Education. Atlanta, GA.

Information Technology Industry Sector Curriculum Standards. 2005. Career and Workforce Innovations Unit, California Department of Education, Sacramento, CA.

Information and Support Services, Business and Information Technology Standards. 2006. Career & Technical Education. Indiana Department of Education, Indianapolis, IN.

Computer Maintenance Option A Course Standards. 2009. Career and Technical Education. Arizona Department of Education, Phoenix, AZ.

Internet and Computing Core Certification Standards. 2008. Certiport, Inc. American Fork, UT.

Kessler, Gary. "*An Overview of Cryptography.*" June, 2010. www.garykessler.net/library

Pagoria, Bob. "*Implementing Robust Physical Security—A Lord of the Rings."* July 2004. SANS Institute, www.sans.org

"*Public Key infrastructure.*" Wikipedia, http://en.wikipedia.org/wiki/Public_key_infrastructure

"Public Key Cryptography." Wikipedia, http://en.wikipedia.org/wiki/Public-key_cryptography

"What is intrusion detection?" What is.com. March 2009.
http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci295031,00.html

"Authentication." SearchSecurity.com Definitions.
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html

"*Computer Forensics Training Course.*" New Technologies, Inc., Jacksonville, FL. http://www.forensics-intl.com/forensic.html

CYBER SECURITY SAMPLE QUESTIONS

1) A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would best serve this purpose?
   A) antivirus
   B) host-based firewall
   C) anti-spyware
   D) web content filter

2) The below report indicates that the system is most likely infected by which of the following? Protocol LOCAL IP FOREIGN IP STATE, TCP 0.0.0:445 0.0.0.0:0 Listening, TCP 0.0.0.0:3390 0.0.0.0:0
   A) worm
   B) trojan
   C) listening
   D) logic bomb

3) The network manager has obtained a public IP address for use with a new system to be available via the internet. This system will be placed in the DMZ and will communicate with a database server on the LAN. Which of the following should be used to allow for secure communication between internet users and the internal systems?
   A) NAT
   B) SSL
   C) DNS
   D) VLAN

4) The SS ID broadcast for wireless router has been stopped, but a LAN administrator has noticed that authorized users are still accessing the wireless LAN. The administrator has determined that the attackers are still able to detect the presence of the wireless LAN even though the SS ID has been stopped. What would further obscure the presence of the wireless LAN?
   A) reroute wireless users to honeypot
   B) disable responses to a broadcast probe request
   C) create a non-zero length SS ID for the wireless router
   D) upgrade the encryption to WPA or WPA2

5) Which of the following is a Data Loss Prevention (DLP) strategy that addresses data in transit issues?
A) scanning of outbound IM
B) scanning copying of documents to USB
C) scanning of SharePoint document library
D) scanning printing of documents

6) An employee in the accounting department recently received a phishing email that instructed them to click a link in the email to view an important message from the IRS which threatened penalties if a response was **not** received by the end of the business day. The employee clicked on the link and the machine was infected with malware. Which of the following principles best describes why this social engineering ploy was successful?
A) scarcity
B) urgency
C) social proof
D) familiarity

7) A system administrator would like to safeguard the integrity of data while in transit over the local LAN. What should be implemented to fulfill this requirement?
A) encryption
B) data loss prevention
C) access control lists
D) HIPS

8) An attacker wants to get confidential data from an organization. The attacker decides to implement stenography as the method of hacking. Which of the following techniques should the attacker use?
A) use a substitution cipher
B) add information to a sound file
C) encrypt an existing image file
D) hash an existing document

9) What is a protocol that could be used to support authentication services for several local devices from a central location without the use of tokens or tickets?
A) biometrics
B) TACACS+
C) PKI
D) smartcards

10) Which of the following offerings typically allows the customer to apply operating system patches?
A) cloud-based storage
B) software as a service
C) public clouds
D) infrastructure as a service

11) A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the next step to minimize the business impact?
A) launch an investigation to identify the attacking host
B) review lessons learned in the process
C) remove malware and restore the system to normal operation
D) initiate the incident response plan

12) An external auditor visits the human resource department and performs a physical security assessment. The auditor observes documents on printers that are unclaimed. A closer look at these documents reveals employees' names, addresses, ages, and type of medical and dental coverage options each employee has selected. Which of the following is the most appropriate action to take?
A) flip the documents face down so no one knows these documents are PII sensitive
B) retrieve the documents, label them with PII cover sheets, and return them to the printer
C) shred the documents and let the owner of the printer discover the missing documents on their own
D) report to the human resources manager that their personnel are violating a privacy policy

13) Following a system review, one corporate workstation was found to be storing passwords in plain text. Which of the following is the correct method for storing passwords?
A) hashing the password prior to storing
B) creating a digital certificate of the password prior to storing
C) using cryptography to conceal the password prior to storing
D) run the passwords through a quaternion system of equations

14) Which of the following best describes the initial processing phase used in mobile device forensics?

A) the phone and storage cards should be examined as a complete unit after examining the removable storage cards separately

B) the phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device

C) the mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again

D) the removable data storage cards should be processed first to prevent data alteration when examining the mobile device

15) The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

A) HPM technology

B) DLP policy

C) TPM technology

D) Full-disk encryption

1) C
2) C
3) B
4) D
5) A
6) B
7) A
8) B
9) B
10) D
11) C
12) D
13) A
14) B
15) B

General Competitive Events Guidelines

The general event guidelines below are applicable to all FBLA High School national competitive events. Please review and follow these guidelines when competing at the national level. When competing at the state level, check the state guidelines since they may differ.

All members and advisers are responsible for reading and following competitive event guidelines.

Eligibility

- Dues: Competitors must have paid FBLA national and state dues by 11:59 p.m. Eastern Time on March 1 of the current school year.
- NLC Registration: Participants must be registered for the NLC and pay the national conference registration fee in order to participate in competitive events.
- Deadlines: The state chair, or designee, must register each state competitor on the official online entry forms by 11:59 p.m. Eastern Time on the second Tuesday in May.
- Each state may submit four entries in all events.
- Each competitor can only compete in one individual/team event and one chapter event.
- Each competitor must compete in all parts of an event for award eligibility.
- A team shall consist of two or three members. The exception is Parliamentary Procedure, which must be a team of four or five members.
- All members of a team must consist of individuals from the same chapter.
- If competitors are late for a competitive event, there are no guarantees they will get to compete. Competitive event schedules cannot be changed. **PLEASE NOTE** that competitive events start in the morning before the opening session of NLC.
- Competitors may be disqualified if they violate competitive event guidelines.
- Picture identification (drivers' license, passport, state-issued identification, or school-issued identification) is required when checking in for competitive events.

General Competitive Events Guidelines

Repeat Competitors

- Members may compete in an event at NLC more than once if they have not previously placed in the top ten of that event at NLC. If a member places in the top ten of an event at NLC, they are no longer eligible to compete in that event. This eliminates the exceptions for team events that were previously in place, as this change will now affect all events.
- Modified Events: A competitor may compete in the same event when the event is modified, regardless of placement at a National Leadership Conference. Note, if the only modification is a name change, competitors may not compete in the renamed event if they have previously placed in the top ten at the National Leadership Conference.
- Chapter Events: Competitors may compete in a chapter event as many times as they wish, regardless of placement at a previous National Leadership Conference (American Enterprise Project, Community Service Project, Local Chapter Annual Business Report, and Partnership with Business Project).
- Pilot Event: Competition in a pilot event does not disqualify a competitor from competing in the same event if it becomes an official competitive event. The participant may compete in another event as well as a pilot event.

Breaking Ties

- Objective Tests: Ties are broken by comparing the correct number of answers to the last 10 questions on the exam. If a tie remains, the competitor who completed the test in a shorter amount of time will place higher. If this does not break the tie, answers to the last 20 questions will be reviewed to determine the winner.
- Objective and Production Tests: The production test scores will be used to break a tie.
- Objective Tests and Performances: The objective test score will be used to break a tie based on the tie-breaking criteria of objective tests.
- Reports/Projects and Performances: The report/project scores will be used to break a tie.
- Performances: Judges must break ties and all judges' decisions are final.

General Competitive Events Guidelines

National Deadlines

- State chair/adviser must register all competitors for NLC competitive events online by 11:59 p.m. Eastern Time on the second Tuesday in May.
- All prejudged components (reports and projects) must be submitted by 11:59 p.m. Eastern Time on the second Tuesday in May.
- All prejudged projects and reports must be submitted electronically.
- All production tests must be submitted by 11:59 p.m. Eastern Time on the third Tuesday in May.
- All production tests must be uploaded online on the required platform.
- State chair/adviser may make name changes only (no additional entries) by 11:59 p.m. Eastern Time on the first Tuesday in June. Competitor drops are the only changes allowed after this date and onsite.

National Awards

- The number of competitors will determine the number of winners. The maximum number of winners for each competitive event is 10.

Americans With Disabilities Act (ADA)

- FBLA-PBL meets the criteria specified in the Americans with Disabilities Act for all participants who submit an accommodation form.
- The form must be submitted by 11:59 p.m. Eastern Time on the second Tuesday in May.

Recording of Presentations

- No unauthorized audio or video recording devices will be allowed in any competitive event. Participants in the performance events should be aware the national association reserves the right to record any performance for use in study or training materials.