CYBER SECURITY

SkillsUSA Championships Technical Standards

PURPOSE

To evaluate each competitor's preparation for employment and to recognize outstanding students for excellence and professionalism with relation to the entry level skills within the field of cyber security.

CLOTHING REQUIREMENT

Class E: Competition Specific — Business Casual

- Official SkillsUSA white polo shirt
- Black dress slacks or black dress skirt (knee-length minimum)
- Black closed-toe dress shoes

Note: Wearing socks or hose is no longer required. If worn, socks must be black dress socks and hose must be either black or skin-tone and seamless/nonpattern.

Note: Competitors must wear their official competition clothing to the competition orientation meeting.

These regulations refer to clothing items that are pictured and described at www.skillsusastore.org. If you have questions about clothing or other logo items, call 1-888-501-2183.

ELIGIBILITY (TEAM OF TWO)

Open to a team of two active SkillsUSA members enrolled in programs with Cyber Security, Information Security, or Systems and Networking Security Architecture as an occupational objective. Each state may send one high school and one college/postsecondary team.

EQUIPMENT AND MATERIALS

1. Supplied by the technical committee (This includes all reference materials, diagrams, and instruction required for the competition):
   a. Switch fabric for network connectivity
   b. USB Thumb Drives
   c. L2/L3 Managed Switches
   d. Enterprise Routers
   e. Network Server Systems
   f. Hardware Firewalls
   g. Wireless Access Points
   h. Wireless Network Capability
   i. Tablet PCs/Smartphones
   j. Write Blocker Device
   k. SD Card Reader
   l. Log files from PCs, access points, servers, and routers.
   m. Network Cables
   n. Console Cables

2. Supplied by the competitor:
   a. Blank Paper
   b. Writing Instrument
   c. Notebook PC with the following software installed:
   d. Dual-booting Windows 10/11 Pro and Kali Linux (or self-bootable Kali USB Thumb Drive) Kali version must be capable of performing RDP operations.
   e. Putty Software
   f. Autopsy Software
   g. AccessData FTK Imager (Freeware version)
   h. Wireshark
   i. Nmap/Zenmap
   j. Wi-Fi Adapters Capable of Promiscuous Mode Operation
      Note: The competition notebook PC must possess an Ethernet port or a USB to Ethernet converter. This is required for access to the competition environment. Only software specified by the technical committee can be installed on the competitor machines used for the competition. The presence of inappropriate games or other inappropriate content on the competition machine may result in disqualification.
   k. All competitors must create a one-page resume. See “Resume Requirement” below for guidelines.

RESUME REQUIREMENT

Competitors must create a one-page resume to submit online. SkillsUSA South Carolina competitors should submit their resume by the deadline published on the state competition updates page of our website. Failure to submit a resume will result in a 10-point penalty.

Your resume must be saved as a PDF file type using file name format of "Last Name_First Name." For example, "Amanda Smith" would save her resume as **Smith_Amanda**. If you need assistance with saving your file as a PDF, visit the Adobe website for more information.

***Note*:** Check the Competition Guidelines and/or the updates page on the state website.

PROHIBITED DEVICES

Cellphones, electronic watches and/or other electronic devices not approved by a competition's national technical committee are ***NOT*** allowed in the competition area. Please follow the guidelines in each technical standard for approved exceptions. Technical committee members may also approve exceptions onsite during the SkillsUSA Championships if deemed appropriate.

Penalties for Prohibited Devices

If a competitor's electronic device makes noise or if the competitor is seen using it at any time during the competition, an official report will be documented for review by the Director of the SkillsUSA Championships. If confirmed that the competitor used the device in a manner which compromised the integrity of the competition, the competitor's scores may be removed.

SCOPE OF THE COMPETITION

The competition is defined by industry standards as determined from elements of the NIST Publication 800-181 Cyber Security Workforce Framework Categories which include:

- Securely Provision (SP)
- Operate and Maintain (OM)
- Protect and Defend (PR)

KNOWLEDGE PERFORMANCE

Cognitive Domain Performance

Competitors will take an examination covering their knowledge of common cyber security tenets as defined by the objectives of CompTIA's Security+ or ETA's ITS certifications. This involves knowledge of common cyber security tools, techniques, and practices. Questions cover key cyber security systems and devices, including those related to end point devices, software, managed switches, enterprise routers, wireless access points, firewalls, pentesting tools, and digital/network forensic activities. The exam consists of multiple-choice questions and lasts up to two hours.

SKILL PERFORMANCE

Psychomotor Domain Performance

This portion of the competition consists of several Provisioning, Testing, Deployment, Operational and Maintenance, and Protection and Defensive procedures with the end goals set by the technical committee. Competitors must successfully complete assigned tasks at several independent activity stations. The tasks are designed to provide a variety of cyber security

challenges based on the recommended best practices of the industry. Identical tasks are used in high school and college/postsecondary categories. Approximately 45 minutes are allowed at each station.

COMPETITION GUIDELINES

1. The competition requires a team (tactical unit) of two competitors. Each will have to display equivalent subject matter expertise in all competency areas. The stages of the competition are as follows:
2. Cognitive Domain — The knowledge/certification exam and the professional interview
3. Psychomotor Domain — Hands-on skills task stations.

COMPETITION STATIONS

This competition skill performance stations are created to be a scouting combine where competitors will demonstrate a wide range of skills sets needed in this industry. The competitors will rotate through the individual activity stations as determined by the technical committee.

Station 1: Cybersecurity Professional Certification Exam Station

Competitors will take either the CompTIA Security+ or ETA ITS Certification exams for professional certification.

Station 2: Professional Activities Station

Competitors will provide verbal instructions or explanations to an evaluator for the task presented at the professional activities station.

1. Train a fellow employee how to avoid phishing attempts associated with emails and web sites. This should include user level examples of things to look for to avoid common items used as bait.
2. Explain requirements for (and methods of) creating strong passwords to senior management personnel in your company.
3. Provide legally sound advice and recommendations to management on a variety of cyber security topics.
    a. Provide sound recommendations to management on a variety of cyber security policies.
        1). Separation of Duties Policies
        2). Acceptable Use Policies
        3). Mandatory Vacation Policies
    b. Conduct training of the organization's staff on a variety of employee-centered cyber security activities.
        1). Use of Antivirus Software
        2). Use of Anti Malware Products.
    c. Explain to a new employee the process for notifying first responders of the Computer Incident Response Team about the possible occurrence of a cyber event.

Station 3: Network Systems Hardening Station

This task contains activities related to hardening network systems including different types of endpoints and network servers. Competitors will display knowledge of industry standard processes and procedures for hardening an end point or stand-alone computing device or a network server. Devices may be running Windows, Linux, or Android operating systems.

Suggested Hands-On Activities Include:

1. Endpoint Hardening — Competitors will display knowledge of industry standard processes and procedures for hardening an end point or stand-alone computing device.
    a. Configuring BIOS/CMOS settings to secure the outer perimeter of a personal computer.
        1). Configure BIOS Passwords to safeguard the CMOS Area and control access to the operating system
        2). Enable/Disable USB ports
        3). Manage Boot devices and boot order
    b. Take steps to harden an installed operating system – including Windows 10/11, Windows Server 2012/R2, 2019, and Linux distributions.
        1). Create secure passwords
        2). Given a scenario, configure lockout policies
        3). Given a scenario, create and manage local user policies
        4). Given a scenario, assign user privileges based on the principle of least privilege
        5). Disable vulnerable accounts
        6). Given a scenario, manage services and ports securely
        7). Identify and remove unnecessary software applications
    c. Secure data at rest in a personal computer.
        1). Apply file and folder level encryption
        2). Apply disk level encryption
    d. Install/configure antivirus/antimalware
        1). Perform secure local firewall configurations
        2). Write a rule to allow or deny specific traffic to pass through the local firewall
        3). Given a scenario, perform secure browser configurations
2. Server Hardening — These tasks contain activities related to hardening servers against attack. Competitors will display knowledge of industry standard processes and procedures for hardening a network server.
    a. Given a scenario, create and configure an administrative account to replace the default admin account
    b. Configure permissions or rights for network users and groups applying the principle of least privilege
    c. Implement server security logging and auditing
    d. Take steps to harden an installed server operating system.
        1). Create and manage network user policies
        2). Assign user privileges based on the principle of least privilege
        3). Disable vulnerable/unnecessary user accounts
        4). Manage services and ports securely
    e. Secure data at rest in a server environment.
    f. Perform vulnerability scans and host-based service system calls on operating servers
    g. Given a scenario, create virtual machines/networks on a server

Station 4: Local Network Device Security

This task contains security-related activities associated with managed switches and enterprise routers and includes activities associated with accessing these devices, configuring them to create network security structures and establish security for the device itself.

Suggested Hands-On Activities Include:

1. Managed Switch Security
    a. Access a managed switch's management environment.
        1). Establish an IP Address for the switch's management VLAN
    b. Enable access security for the switch's admin environment.
        1). Configure an encrypted password for the switch.
    c. Create multiple VLANs to establish segmented network security zones
    d. Manage switch port security
        1). Given a scenario, configure MAC filtering on a managed switch
    e. Create an ACL to control access to different groups of switch ports or IP addresses
    f. Given a scenario, establish SSH administrative access to the switch.
2. Enterprise Router Security
    a. Access an enterprise router's management environment.
        1). Enable access security for the router's admin environment.
        2). Configure an encrypted password for the router.
    b. Create a routing scheme to route traffic from one designated network to another.
        1). Given a scenario, set up static routing
        2). Add a neighbor
    c. Configure a router to implement specified traffic control measures.
    d. Configure an enterprise router to log network system events for incident response auditing.

Station 5: Network Boundary Security

This task contains activities related to installing and configuring typical network boundary devices and structures to form an effective network zone or edge security systems.

Suggested Hands-On Activities Include:

1. Access a hardware firewall's management environment
    a. Establish an IP Address for the firewall's management console
2. Enable access security for the switch's admin environment
    a. Configure an encrypted password for the switch
3. Given a scenario, use a hardware firewall to create and configure perimeter security that provides a boundary between two network zones that have differing security levels.
    a. Implement a network perimeter firewall
    b. Create a DMZ
4. Perform file hashing on a downloaded file to verify its integrity
5. Establish and configure an ACL on the firewall to limit or restrict access to assets as required by the organization's security policies
6. Enable NAT for specific types of network traffic
7. Create a VPN connection
8. Span a firewall port for monitoring purposes
9. Configure IPSec on the firewall

10. Configure IDS

Station 6: Scripting for Cybersecurity

This task contains activities associated with creating scripts to automate cybersecurity-related activities. Competitors should be prepared to create scripts in Python, Ruby, Powershell 7, or Bash scripting languages.

Suggested Hands-On Activities Include:

1. Create scripts to automate nmap scans to scan an entire network or a portion of a network
2. Create scripts to conduct reverse DNS lookups

Station 7: Wireless and Mobile Device Security

This task contains activities related to installing, configuring and securing wireless access points and mobile devices.

Suggested Hands-On Activities Include:

1. Securely install, connect and configure a wireless access point.
    a. Create a secure password for the AP/Router
    b. Given a scenario, configure the most secure authentication protocol available
    c. Turn off any guest networks
2. Configure secure Wi-Fi operation of the AP
    a. Hide the SSID broadcast
    b. Change the default SSID
    c. Lower the antenna power to limit the usable distance of the Wi-Fi signal
    d. Configure MAC filtering to restrict access
3. Configure wireless router options
4. Configure wired AP/Router options
    a. Given a scenario, limit the DHCP pool size to control the number of wireless devices that can connect to the network
    b. Establish secure Wi-Fi connections to an access point
    c. Create a secure password for the mobile device
    d. Configure locking specifications
    e. Given a scenario, configure the device's services and applications to provide secure operation.
5. Configure a WAN (Wireless Area Network)
6. Reset a typical access point

Station 8: Digital/Network Forensics

This task contains activities related to computer or network forensic activities associated with incident response actions. Competitors will use appropriate measures to collect information from a variety of sources to identify, analyze, and report cyber events that occur (or might occur) to protect information, information systems, and networks from cyber threats.

Suggested Hands-On Activities Include:

1. Wireshark PCAP analysis
2. Given a set of log files created during a given activity, the competitor must be able to analyze the activity occurring, determine whether it is an event or not, and if an event occurred, describe best practices for mitigating the event.
3. Collect, process, preserve, analyze, and present computer related evidence in support of network vulnerability mitigation and/or criminal, fraud, counter intelligence or law enforcement investigations.
4. Scan USB thumb drives or SD cards for deleted files
5. Create a forensic image of a drive.
6. Create a memory dump of a suspected computer.
7. Perform a live data acquisition.

Station 9: Pentesting

This task contains activities related to the process of penetration testing. The competitor will plan, prepare, and execute tests of systems to evaluate results against specifications and requirements as well as analyze and report on test results.

Suggested Hands-On Activities Include:

1. Conduct a port scan on a designated device or network
2. Perform a network vulnerability scan
3. Perform a wireless sniffing operation
4. Perform a WireShark scan
5. Enumerate a network
6. Analyze collected information to identify vulnerabilities that pose the possibility of exploitation.
7. Perform a DoS attack against a specified target
8. Hack a specified file (flag) in a remote network
9. Perform steps to establish persistence in a compromised network or device

Station 10: Capture the Flag Competition

During times when the competitors are not actively participating at one of the other cyber security stations, they will engage in an online Capture the Flag (CTF) event. The competitors will log onto the designated CTF website, enroll themselves, and perform the CTF activity or activities presented.

Suggested possible CTF activities include:

1. Forensics paths
2. Cryptography
3. Web Exploitation
4. Reverse Engineering
5. Binary Exploitation

STANDARDS AND COMPETENCIES

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework https://niccs.cisa.gov/.

CY 1.0 — Outline principles and concepts of data storage and security (System Architecture SP-ARC002)

CY 2.0 — Demonstrate abilities to securely provision operating systems, software, and configure security at initial provisioning stages (Securely Provision SPDEV-001)

CY 3.0 — Assessments of systems and networks and identifies where those deviate from acceptable configurations, enclave policy, or local policy. Measure the effectiveness of architecture against known vulnerabilities. (Protect and Defend: Vulnerability Assessment and Management PRVAM-001)

CY 4.0 — Analyze data collected from a variety of cyber defense tools, (e.g., IDS alerts, firewalls, and network traffic logs.) analyze events that occur within their environments for the purposes of mitigating threats (Protect and Defend: Defense Analyst PR-CDA-001)

CY 5.0 — Preparation and execution of tests against systems requirements to analyze results (Test and Evaluation SP-TST-001)

CY 6.0 — SkillsUSA Framework

The SkillsUSA Framework is used to pinpoint the Essential Elements found in Personal Skills, Workplace Skills and Technical Skills Grounded in Academics. Students will be expected to display or explain how they used some of these Essential Elements. Please reference the graphic, as you may be scored on specific elements applied to your project. For more, visit: www.skillsusa.org/who-we-are/skillsusa-framework/.

COMMITTEE IDENTIFIED ACADEMIC SKILLS

The technical committee has identified that the following academic skills are embedded in this competition.

Math Skills

- Use scientific notation.
- Use logarithms.
- Use statistics.

Science Skills

- Use knowledge of mechanical, chemical and electrical energy.
- Use knowledge of temperature scales, heat and heat transfer.
- Use knowledge of work, force, mechanical advantage, efficiency and power.
- Use knowledge of principles of electricity and magnetism.
- Use knowledge of static electricity, current electricity and circuits.
- Use knowledge of signal frequencies and baud rate.
- Use knowledge of communication modes (full/half duplex).

Language Arts Skills

- Organize and synthesize information for use in written and oral presentations. Demonstrate knowledge of appropriate reference materials.

CONNECTIONS TO NATIONAL STANDARDS

State-level academic curriculum specialists identified the following connections to national academic standards.

Math Standards

- Linear algebra
- Trigonometry
- Calculus
- Data analysis and probability
- Operational analysis
- Problem solving
- Reasoning and proof

Source: *Careeronestop: https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx. Select "Academic Competencies" from model.*

Source: *NIST Publication 800-181 CyberSecurity Workforce Framework: https://doi.org/10.6028/NIST.SP.800-181r1*

Science Standards

- Understands relationships among organisms and their physical environment
- Understands the sources and properties of energy

- Understands forces and motion
- Understands the nature of scientific inquiry

Source: *McREL compendium of national science standards. To view and search the compendium, visit: www2.mcrel.org/compendium/.*

Language Arts Standards

- Students apply a wide range of strategies to comprehend, interpret, evaluate and appreciate texts. They draw on their prior experience, their interactions with other readers and writers, their knowledge of word meaning and of other texts, their word identification strategies and their understanding of textual features (e.g., sound letter correspondence, sentence structure, context, and graphics)
- Students adjust their use of spoken, written and visual language (e.g., conventions, style, vocabulary) to communicate effectively with a variety of audiences and for different purposes
- Students use spoken, written and visual language to accomplish their own purposes (e.g., for learning, enjoyment, persuasion and the exchange of information)

Source: IRA/NCTE Standards for the English Language Arts. To view the standards, visit: http://www.ncte.org/standards/ncte-ira