CYBER SECURITY

PURPOSE

To evaluate each contestant'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.

First, download and review the General Regulations at: http://updates.skillsusa.org.

CLOTHING REQUIREMENT

Class E: Contest specific — Business Casual

- Official SkillsUSA white polo shirt.
- Black dress slacks (accompanied by black dress socks or black or skin-tone seamless hose) or black dress skirt (knee-length, accompanied by black or skin-tone seamless hose).

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.

Note: Contestants must wear their official contest clothing to the contest orientation meeting.

ELIGIBILITY

Open to active SkillsUSA members (Team of 2) enrolled in programs with Cyber Security, Information Security, or Systems and Networking Security Architecture as the occupational objectives.

EQUIPMENT AND MATERIALS

1. Supplied by the technical committee: This includes all reference materials, diagrams, and instruction required for the contest.
   a. Switch fabric for network connectivity
   b. Personal computers
   c. USB thumb drives, L2/L3 managed switches, enterprise routers, Putty software
   d. Network server system
   e. Hardware firewalls
   f. Wireless access points
   g. Wireless network capability
   h. Tablet PCs/smartphone
   i. Autopsy software (installed)
   j. AccessData FTK Imager (installed)
   k. USB thumb drives
   l. Write blocker device
   m. SD card reader
   n. Log files from PCs, access points, servers, and routers
   o. Network cables
   p. Console cables
   q. Bootable Kali USB thumb drives
   r. WiFi adapters capable of promiscuous mode operation
2. Supplied by the contestant:
   a. Résumé
   b. Blank paper
   c. Writing instrument

SCOPE OF THE CONTEST

The contest is defined by industry standards as determined from elements of the NIST publication "800-181 Cyber Security Workforce Framework." Framework categories include:

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

Knowledge Performance

Cognitive Domain Performance: Contestants 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, pen testing tools, and digital/network forensic activities. The exam consists of multiple-choice questions and lasts up to two hours.

Skills 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. Contestants must successfully complete assigned tasks at a number of 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.

Contest Guidelines

1. The contest requires a team or tactical unit of two: Each will have to display equivalent subject matter expertise in all competency areas. The contest will take place in two learning domains. The outcome and winners are determined by the combined scores from both domains . The domains of the contest are as follows:

Standards and Competencies

CSC 1.0 — Professional Activities Station

Contestants will provide verbal instructions or explanations to an evaluator for the task presented at the Professional Activities Station.

1.1 Train a fellow employee how to avoid phishing attempts associated with emails and websites. This should include user-level examples of things to look for to avoid common items used as bait.

1.2 Explain requirement for (and methods of) creating strong passwords to senior management personnel in your company.

1.3 Provide legally sound advice and recommendations to management on a variety of cyber security topics.

1.4 Provide sound recommendations to management on a variety of cyber security policies.

- 1.4.1 Separation of Duties policies
- 1.4.2 Acceptable Use policies
- 1.4.3 Mandatory Vacation policies

1.5 Conduct training of the organization's staff on a variety of employee cyber security activities.

- 1.5.1 Use of antivirus software
- 1.5.2 Use of anti-malware products

1.6 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.

SP 2.4 – Outline principles and concepts of data storage and security (System Architecture SPARC002)

CSC 2.0 — End-Point Security Station

Contestants will display knowledge of industry standard processes and procedures for hardening an endpoint or stand-alone computing device.

2.1 Configuring BIOS/CMOS settings to secure the outer perimeter of a personal computer

- 2.1.1 Configure BIOS passwords to safeguard the CMOS area and control access to the operating system.
- 2.1.2 Enable/disable USB ports.
- 2.1.3 Manage boot devices and boot order.

2.2 Take steps to harden an installed operating system.

- 2.2.1 Create secure passwords.
- 2.2.2 Given a scenario, configure lockout policies.
- 2.2.3 Given a scenario, create and manage local user policies.
- 2.2.4 Given a scenario, assign user privileges based on the principle of least privilege.
- 2.2.5 Disable vulnerable accounts
- 2.2.6 Given a scenario, manage services and ports securely.
- 2.2.7 Identify and remove unnecessary software applications.

2.3 Secure data at rest in a personal computer.

- 2.3.1 Apply file- and folder-level encryption.
- 2.3.2 Apply disk-level encryption.

2.4 Install/configure antivirus/antimalware

- 2.4.1 Perform secure local firewall configurations.
- 2.4.2 Write a rule to allow or deny specific traffic to pass through the firewall.
- 2.4.3 Given a scenario, perform secure browser configurations.

SP 1.1 – Demonstrate abilities to securely provision operating systems, software, and configure security at initial provisioning stages (Securely Provision SPDEV-001)

CSC 3.0 — Managed Switch Security

This task contains security-related activities associated with managed switches.

3.1 Access a managed switch's management environment.
 3.1.1 Establish an IP address for the switch's management VLAN
3.2 Enable access security for the switch's admin environment.
 3.2.1 Configure an encrypted password for the switch.
3.3 Create multiple VLANS to establish segmented network security zones.
3.4 Manage switch port security.
 3.4.1 Given a scenario, configure MAC filtering on a managed switch.
3.5 Create an ACL to control access to different groups of switch ports or IP addresses.
3.6 Given a scenario, establish telnet or ssh administrative access to the switch.

CSC 4.0 — Enterprise Router Security

This task contains activities associated with accessing an enterprise router, configuring it to create network security structures and establish security for the router itself.

4.1 Access an enterprise router's management environment.
 4.1.1 Enable access security for the router's admin environment.
 4.1.2 Configure an encrypted password for the router.
4.2 Create a routing scheme to route traffic from one designated network to another.
 4.2.1 Given a scenario, set up static routing.
 4.2.2 Add a neighbor.
 4.2.3 Configure a router to implement specified traffic control measures.
 4.2.4 Configure an enterprise router to log network system events for incident response auditing.

CSC 5.0 — Server Hardening

This task contains activities related to hardening servers against attack.

5.1 Given a scenario, create and configure an administrative account to replace the default admin account.
5.2 Configure permissions or rights for network users and groups applying the principle of least privilege.
5.3 Implement server security logging and auditing.
5.4 Take steps to harden an installed server operating system.
 5.4.1 Create and manage network user policies.
 5.4.2 Assign user privileges based on the principle of least privilege.
 5.4.3 Disable vulnerable/unnecessary user accounts.
 5.4.4 Manage services and ports securely.
5.5 Secure data at rest in a server environment.
5.6 Perform vulnerability scans and host-based service system calls on operating servers.
5.7 Given a scenario, create virtual machines/networks on a server.

CSC 6.0 — 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.

6.1 Access a hardware firewall's management environment.
 6.1.1 Establish an IP address for the firewall's management console.
6.2 Enable access security for the switch's admin environment.
 6.2.1 Configure an encrypted password for the switch.
6.3 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.
 6.3.1 Implement a network perimeter firewall.
 6.3.2 Create a DMZ.
6.4 Perform file hashing on a downloaded file to verify its integrity.

6.5 Establish and configure an ACL on the firewall to limit or restrict access to assets as required by the organization's security policies.
6.6 Enable NAT for specific types of network traffic.
6.7 Create a VPN connection.
6.8 Span a firewall port for monitoring purposes.
6.9 Configure IPSec on the firewall.
6.10 Configure IDS/Splunk suggested.

CSC 7.0 — Wireless Security

This task contains activities related to installing, configuring and securing wireless access points and mobile devices. Suggested hands-on activities include:

7.1 Securely install, connect and configure a wireless access point.
   7.1.1 Create a secure password for the AP/router.
   7.1.2 Given a scenario, configure the most secure authentication protocol available.
   7.1.3 Turn off any guest networks.
7.2 Configure secure WiFi operation of the AP.
   7.2.1 Hide the SSID broadcast.
   7.2.2 Change the default SSID.
   7.2.3 Lower the antenna power to limit the usable distance of the WiFi signal.
   7.2.4 Configure MAC filtering to restrict access.
7.3 Configure wireless router options.
7.4 Configure wired AP/router options.
   7.4.1 Given a scenario, limit the DHCP pool size to control the number of wireless devices that can connect to the network.
7.5 Configure a WAN (Wireless Area Network)
7.6 Reset a typical access point.

CSC 8.0 — Network Forensics

This task contains activities related to network forensic activities associated with Incident Response Actions. Contestants 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.

8.1 Wireshark PCAP analysis
8.2 Given a set of log files created during a given activity, the contestant must be able to analyze the activity occurring, determine whether it is an event or not, and describe best practices for mitigating the event if so.
8.3 Collect, process, preserve, analyze and present computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence or law enforcement investigations.

> PR 5.1 – Assess systems and networks and identify 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).
>
> 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).

CSC 9.0 — Pen testing

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

9.1 Conduct a port scan.
9.2 Perform a network vulnerability scan.
9.3 Perform a WireShark scan.
9.4 Enumerate a network.
9.5 Analyze collected information to identify vulnerabilities that pose the possibility of exploitation.
9.6 Perform a DoS attack against a specified target.
9.7 Hack a specified file (flag) in a remote network.
9.8 Perform steps to establish persistence in a compromised network or device.

SP 3.2 - Preparation and execution of tests against systems requirements to analyze results (Test and Evaluation SP-TST-001).

Committee Identified Academic Skills

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

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: CareerOne stop https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx. Select "Academic Competencies" from model.

Source: NIST Publication 800-181 "Cyber Security Workforce Framework" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf. Page 60, reference K0052.

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: https://www.mcrel.org/standards-curriculum/

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: https://ncte.org/resources/standards/ncte-ira-standards-for-the-english-language-arts/.