Cyber Security 2019
SkillsUSA Cyber Security Competition Activities

Activity Stations
The competition consists of several test-station activities. Contestants must successfully complete assigned tasks at each station. 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 (with the exception of the Testing Station which is allowed up to 2 hours).

Station 1 - Cyber Security Exam Station
Contestants will take an examination covering their knowledge of common electronic smart home subsystems as defined by the objectives of CompTIA’s Security+ or ETA’s IT certification. This involves knowledge of common cyber security tools, techniques, and practices. Questions cover key cyber security systems and devices, including those related to personal computers, 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.

Station 2 - Professional Activities Station
Contestants will provide verbal instructions or explanations to an evaluator for that task presented at the Professional Activities Station.

Suggested Activities include:

a. 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.

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

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

*Separation of Duties Policies
*Acceptable Use Policies
*Mandatory Vacation Policies
Station 3 - End-Point Security Station

At this station, the contestant will display knowledge of industry standard processes and procedures for hardening an end point or standalone computing device.

*Station Requirements:*

a. Personal Computer

b. USB Thumb Drive

*Suggested Activities include:*

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

   *Configure BIOS Passwords to Safeguard the CMOS Area and Control Access to the Operating System*

   *Enable/Disable USB ports*

   * Manage Boot devices and boot order*

Station 4 - Managed Switch Security Station

This activity contains tasks associated with security of and with a managed switch

*Suggested Activities include*

a. L2/L3 Managed Switch

b. Personal Computers (x*)

   *Putty Installed*

c. Network Cables
d. Console Cable

*Suggested Hands-On Activities Include:

a. Access a managed switch’s management environment.

   *Establish an IP Address for the Switch’s Management VLAN*


   *Configure an Encrypted Password for the Switch.*

c. Create Multiple VLANs to Establish Segmented Network Security Zones
Station 5 - Enterprise Router Station

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

Station Requirements:

a. Enterprise Router
b. UTP Cables
c. Personal Computers
   * Putty Installed
d. Console Cable

Suggested Hands-On Activities Include:

* Configure an Encrypted Password for the Router

Station 6 - Server Security Station

This task contains common tasks related to hardening servers against attack

Station Requirements:

a. Network Server System
   * Server
   * Infrastructure Switch with VLAN
c. Network Cables

Suggested Hands-On Activities Include:

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
Station 7 - Network Boundary Security Station

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

Station Requirements:

a. Hardware Firewall
b. Personal Computers (x2)
   * Putty Installed
c. Network Cables
d. Console Cable

Suggested Hands-On Activities Include:

a. Access a hardware Firewall’s management environment.
   * Establish an IP Address for the Firewall’s Management Console
b. Enable Access Security for the Switch’s Admin Environment

Station 8 - Wireless and Mobile Device Security Station

This task contains a task related to installing, configuring and securing wireless Access Points and Mobile Devices.

Station Requirements:

a. Wireless Access Point
b. Personal Computer with Wireless Network Capability
c. Ethernet Cables
d. Tablet PC/Smartphone

Suggested Hands-On Activities Include:

a. Securely Install, Connect and Configure a Wireless Access Point.
   * Create a Secure Password for the AP/Router
   * Given a Scenario configure the most Secure Authentication Protocol Available
   * Turn Off any Guest Networks
b. Configure Secure WiFi operation of the AP.
   * Hide the SSID Broadcast
Station 9 - Digital/Network Forensics Station

This task contains a task related to computer or 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.

Station Requirements

a. Log files from PCs, access points, servers, and routers.

b. Enterprise Router.

c. Wireless Access Point

d. Personal Computer

Suggested Hands-On Activities Include:

a. 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.

   *Access a Wireless AP to Examine its Activity Logs for Auditing Purposes

   *Access an End Point’s Activity Logs for Auditing Purposes

Station 10 - Pentesting Station

This task contains tasks 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.

Station Requirements

a. Pentest Notebook PC.

b. Bootable Kali USB Thumb Drive.

   *Keylogger Software

c. WiFi Adapter Capable of Promiscuous Mode Operation

d. Network Cable

Suggested Hands-On Activities Include:

a. Conduct a Port Scan

b. Perform a Network Vulnerability Scan

c. Perform a Wireless Sniffing Operation

   *Perform a DeAuth Attack on a Wireless AP