STATE SKILL PERFORMANCE PROJECT

SkillsUSA®

Competition Overview

Competition Name:

Cyber Security

Competition Date and Location:

Saturday, April 15th
Grand Rapids Community College Applied Technology Center (ATC)
151 Fountain NE
Grand Rapids, MI, US (616) 234-GRCC
http://www.grcc.edu/

Competition Description:

(Team of 2) The competition is open to active SkillsUSA members enrolled in programs with Cyber Security, Information Security, or Systems and Networking Security Architecture. Students will be tested on the elements of the NIST Publication 800-181 Cybersecurity Workforce Framework categories including Securely Provision, Operate and Maintain, and Protect and Defend.

Number of Competitors (team or individual):

Team of 2

Competition Length:

4-6 Hours

Competition Clothing:

Business Casual
- 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.

Competition Material List

Items Brought by Technical Committee

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
o. Bootable Kali USB Thumb Drives.
p. Wi-Fi Adapters Capable of Promiscuous Mode Operation

Items Brought by Competitors

a. Blank Paper
b. Writing Instrument
c. Notebook PC with the following software installed:
d. Dual-booting Windows 10/11 Pro and Kali Linux
e. Putty Software
f. Autopsy Software
g. AccessData FTK Imager (Freeware version)
h. Wireshark
i. Nmap/Zenmap
j. Combined Component Workbench (to be determined)

Note: The notebook must possess an Ethernet port or a USB to Ethernet converter. This is required for access to the competition environment.
3. All competitors must create a one-page resume to be turned in to contest coordinator.
Note: Only software specified by the technical committee can be installed on the competitor machines for the competition.

Competition Schedule

Time	Item	Item Description
8:00 a.m.	Welcome/Orientation	Welcome competitors to the competition and go through a brief review of the competition.
8:30 a.m.	Workstation Set Up	Team sets up computer workstation
9:30 a.m.	Skill Performance	Competitors will work on reporting tasks (scanning 5 IP addresses for security risks)
12:00 p.m.	Lunch	
1:00 p.m.	Skill Performance	Competitors will continue working until competition ends or they reporting tasks (scanning 5 IP addresses for security risks)

Competitor Instructions

Competitors should use the following software or operating system to identify vulnerabilities on provided target equipment:

- Kali
- Backbox
- Windows with the following software
  - Nmap
  - OWasp Zed Zap
  - Nessus

Note: Teams may not pen-test the individual computers or devices to gain access. The purpose of this exercise is to identify vulnerabilities and report how the individual computers or devices can be hardened.

Warning: Password cracking software or defacement will result in a disqualification

Activities to perform

Competitors will conduct vulnerability testing against 5 specific IP addresses that will be given on the day of the event.

1. The following tasks will be completed:
   a. Identify the Operating System of the device
   b. Identify any open ports
   c. Identify any services running
   d. Identify any CVEs and vulnerabilities
   e. Indicate how to patch these systems, including what should be done via routine maintenance

2. Competitors will write a summary report including
   a. Any vulnerabilities found, including the information above
   b. Mitigation steps of "What to do if these vulnerabilities are found"

Category	Possible Points	Points Earned	Notes
Thoroughness of your initial system analysis report	100		Identify Operating Systems and Ports
Proper hardening measures for associated vulnerabilities during initial discovery period	200		Windows Updates MSSQL Updates MYSQL Updates Close Ports Place behind a hardware firewall and close ports Update firmware Disable unneeded services
Completeness of four incident reports on Wednesday as they correlate to Red Team reporting minimally per hour			Reports should include information above
R1	35		
R2	35		
R3	35		
R4	35		
Professionalism and diligence of reporting			Self-explanatory
R1	30		
R2	30		
R3	30		
R4	30		
Red Team subjective and comparative scoring of ability to defend against attacks	200		Mitigation Information from vulnerabilities found – “What you would do if these were found”
Final System report of any incidents, issues, or findings found throughout the competition	200		Completeness of finding all Oss, vulnerabilities, mitigations
Online Skill Test (e.g. CompTIA)	40		
Resume	-10		Penalty
Clothing	-10		Penalty
Safety (per occurrence)	-100		Penalty
Tools	-50		Penalty
Proper hardening measures for associated vulnerabilities during initial discovery period			Tie Breaker
TOTAL			