SkillsUSA Cybersecurity

PURPOSE

To evaluate each contestant's preparation for employment and to recognize outstanding students for excellence and professionalism with relation to the entry level digital defensive skills within the field of Cybersecurity

CLOTHING REQUIREMENT

For men: Official SkillsUSA white polo shirt with black dress slacks, black socks, and black leather shoes

For women: Official SkillsUSA white polo shirt with black dress slacks or knee-length skirt, black socks or black or skin tone seamless hose and black leather dress shoes

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 (800) 401-1560 or (703) 956-3723

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

ELIGIBILITY (Team of 2)

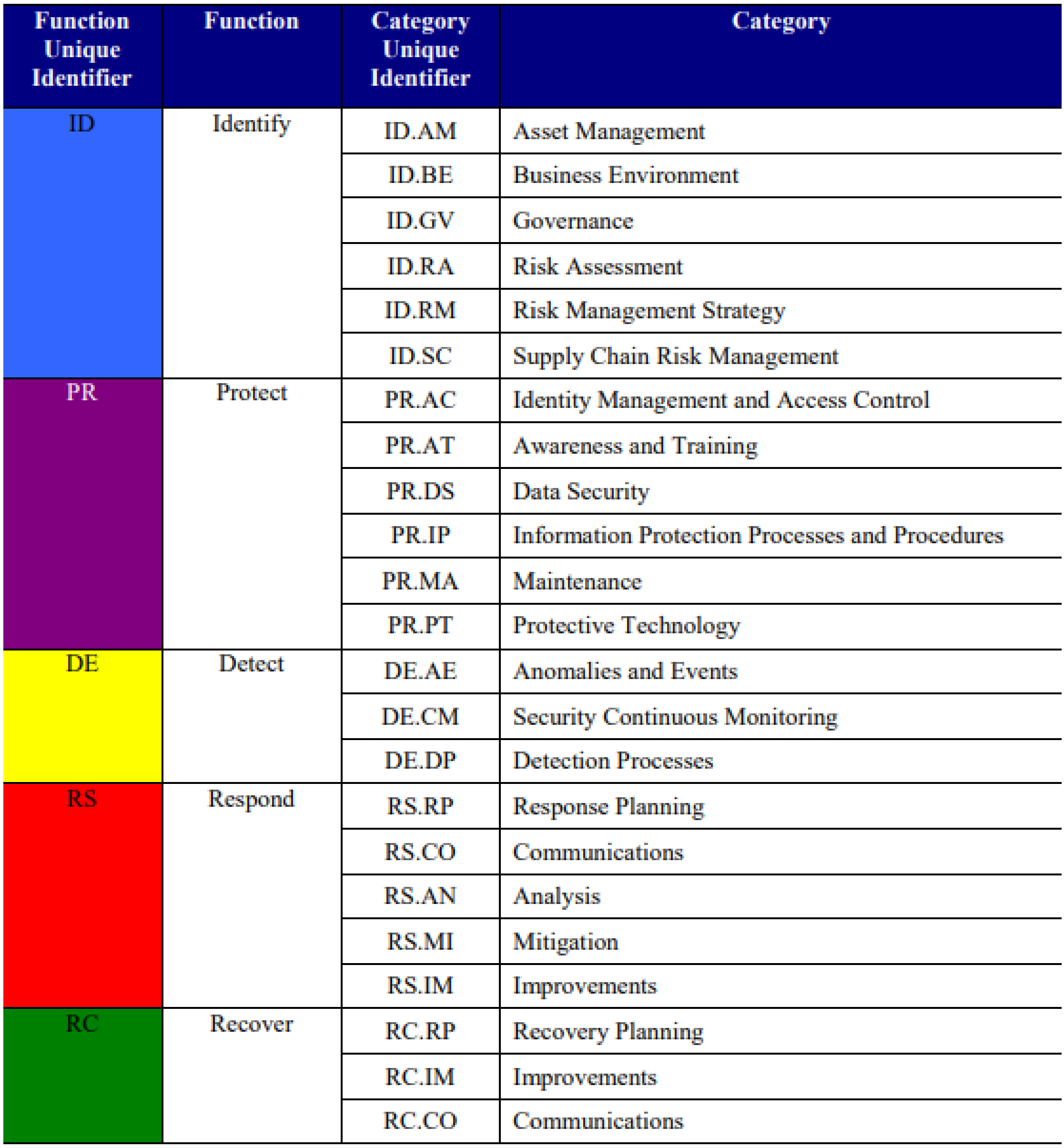
Open to active SkillsUSA members enrolled in programs with Cybersecurity, Information Security, or Systems and Networking Security Architecture as occupational objectives

EQUIPMENT AND MATERIALS

1. Supplied by the technical committee: This includes all reference materials, diagrams, and instructions required for the contest.
    a. Computing devices
    b. Network connectivity devices
    c. Windows 10 operating system
    d. Ethernet cables
    e. Internet connection (contestants must sign internet acceptable use policy. Violation of IAUP disqualifies contestant)
    f. Autopsy software used with network forensics and penetration testing
    g. Forensic image file
2. Supplied by contestant
    a. Flash drives
    b. Wireshark
    c. FTK Imager
    d. Netgear Wireless Router
    e. Resume

SCOPE OF THE CONTEST

The scope of the contest is based on a subset of categories from the ***Framework for Improving Critical Infrastructure Cybersecurity***. Specific details on tasks, knowledge, and skills can be found at https://doi.org/10.6028/NIST.CSWP.04162018



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Skill

Performance

The contest includes securing computer networking equipment including computing devices and network connectivity devices. Contestants will monitor network traffic, conduct an incident response to a security incident, and analyze log and PCAP files.

Knowledge Performance

The contest will include a written exam assessing basic security principles based on the CompTIA Security$^+$ Certification. Exam content source is from ***All-in-One CompTIA Security$^+$ Exam SY0-501 ISBN:978-1-260-01932-2***. The exam will consist of fifty questions. In the event of a tie, contestants will take a timed five question exam that is two minutes until the tie is broken

Cybersecurity Scorecard

Items Evaluated	**Possible Points**
Workstation Security	15
Managed Switch Security	11
Router Security Logging	5
Server Security	8
Wireless Security	10
Network Forensics & Penetration Testing	10
Written Exam	41
Resume Penalty	-10
Clothing Penalty	-5
Total Possible Points	100

Workstation Security (PR.AC-3, PR.AC-4, PR-AC.7, PR.DS-5)				
Element	**3**	**2**	**1**	**0**
Account Policy	Contains all elements of password and account policies	Missing some elements of password or account policy	Missing either password or account policy	Does not include any elements of an account policy
Local Security Restrictions	Configures three restrictions in a local security policy	Configures two restrictions in a local security policy	Configures one restriction in a security policy	Does not configure any restrictions in a local security policy
DHCP Firewall Rules	Allows DHCP client traffic and prevents rouge DHCP servers and can explain the difference between client and server traffic	Allows DHCP client traffic and prevents rouge DHCP servers but cannot explain the difference between client and server traffic	Configures one rule but can explain the difference between client and server traffic	Cannot configure either client or server rules and cannot explain the difference between client and server traffic
Remote Access Rules	Restricts FTP and Telnet traffic and allows SSH	Properly configures two out of three protocols	Properly configures only one out of three protocols	Does not configure FTP, Telnet, and SSH protocols
Restrict Bowser Access	Demonstrates three browser restrictions	Demonstrates two browser restrictions	Demonstrates one browser restrictions	Does not demonstrate any browser restrictions
Total Possible	15 Points			

Managed Switch Security (PR.AC-5, PR.DS-5)				
Element	**3**	**2**	**1**	**0**
IP address of management VLAN	Configures two VLANs and demonstrates VLAN security	Configures two VLANs but does not demonstrate VLAN security	Able to establish IP address of one VLAN	Unable to establish IP address of any VLANs
Encrypted password for switch	Configures encrypted password with password complexity	Configures encrypted password without password complexity	Configures password but not encrypted	Unable to configure password for switch
Switch connection	Establishes two remote connections and differentiates between the two protocols	Establishes two remote connections but does not differentiate between the two protocols	Establishes one remote connection	Unable to establish telnet or SSH connection
Access Control List (ACL)	-	Configures ACL to permit and deny	Configures ACL to either permit or deny but not both	Unable to configure an ACL
Total Possible	11 Points			

Router Security Logging (DE.AE-3, DE.AE-4, DE.AE-5, DE.CM-1)		
Element	**1**	**0**
Configure Static Route	Able to configure a static route	Unable to configure a static route
Show logging status	Able to show logging status	Unable to show logging status
Configure Syslog Server logging	Able to configure Syslog Server Logging	Unable to configure Syslog Server Logging
Configure SNMP Trap logging	Able to configure SNMP Trap logging	Unable to configure SNMP Trap logging
Implement logging messages	Able to implement logging messages	Unable to implement logging messages
Total Possible	***5 Points***	

Server Security (PR.AC-1, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7)				
Element	**3**	**2**	**1**	**0**
Administrative Account	-	-	Able to create a separate administrative account on a server	Unable to create a separate administrative account on a server
Server Logging	-	-	Able to enable logging on a server	Unable to enable logging on a server
Organizational Units (OU)	Able to create two organizational units and place two users in each OU	Only creates one OU and places one user in OU	Able to create organizational units but does not place users in either OU	Unable to create organizational users and place users in the OU
Group Policies	Able to create two group policies and apply them to two organizational units	Creates one group policy and applies to one OU	Able to create group policy but does not apply to any OU	Unable to create a group policy and apply to any OU
Total Possible	8 Points			

Wireless Security (PR.DS-1, PR.DS-2)				
Element	**3**	**2**	**1**	**0**
AP Password	-	Able to create a password for an AP/Wireless Router that meets password complexity requirements	Able to create a password for an AP/Wireless Router. Does not meet password complexity requirements	Unable to create a secure password for an AP/Wireless Router
Secure protocol	-	Able to configure security with the most secure algorithm	Able to configure security but does not include the most secure algorithm	Unable to secure an AP/Wireless password using any security algorithm
SSID	-	Able to change and hide SSID on AP/Wireless Router	Can either hide or change a SSID but not both	Unable to change or hide SSID on an AP/Wireless Router
MAC Filtering	-	-	Able to configure MAC filtering on an AP/Wireless Router	Unable to configure MAC filtering on an AP/Wireless Router
DHCP	Able to perform and three configurations: scope, mask, and lease time	Able to perform two of the three configurations: scope, mask, and lease time	Able to perform one of the three configurations: scope, mask, and lease time	Unable to perform any configuration: scope, mask, and lease time
Total Possible	10 Points			

Network Forensics & Penetration Testing (DE.CM-8, RS.AN-3, RS.AN-4)				
Element	**3**	**2**	**1**	**0**
Wireshark		Able to identify given items that can be enumerated from reading a Wireshark PCAP and conducts an analysis	Able to identify and explain given items in a Wireshark PCAP but does not conduct an analysis	Unable to identify and explain given items in a Wireshark PCAP and cannot conduct an analysis
Log Files	-	Able to identify and explain activity occurring in a log file	Able to identify activity in a log file but cannot explain what is occurring	Unable to identify and explain activity in a log file
Image File Analysis	Able to load image file into given digital forensic tool and identify the criminal incident or security breach and locate all items of evidentiary value	Able to load image file into given digital forensic tool and identify the criminal incident or security breach but does locate all items of evidentiary value	Able to load image file into given digital forensic tool and identify the criminal incident or security breach but does not locate any items of evidentiary value	Unable to load image file into given digital forensic tool and identify the criminal incident or security breach and does not locate any items of evidentiary value
Enumeration	Able to conduct port, network vulnerability and Wireshark scans and enumerate multiple items from the scans	Able to conduct port, network vulnerability and Wireshark scans and enumerate one item from the scans	Able to conduct port, network vulnerability and Wireshark scans but cannot enumerate any items from the scans	Unable to conduct any scans and enumerate any items from the scans
Total Possible	10 Points			