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 digital defensive skills within the field of Cybersecurity.

First, refer to General Regulations, Page 9.

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 Cyber Security, Information Security, or Systems and Networking Security Architecture as the occupational objectives.

- Up to four addition students from the same school and program may assist the team, as long as they are properly credited per the instructions below in **Sections 3 under Equipment and Materials**

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
2. Supplied by the contestant:
    a. Laptop manufactured within the last 3 years with:
    b. Minimum 16 GB of RAM
    c. A working and tested Ethernet 100/1000 network card
    d. 1 TB Free Space
    e. Functioning and tested wireless radio
    f. Two multiple outlet surge protectors
    g. (2) 10 ft Category 5e Network Patch cables
    h. Any writing utensils
    i. software tool(s)

3. A loose-leaf affidavit signed by all team members on 8.5"x11" paper, countersigned by their school's administrator and instructor or SkillsUSA advisor, stating the team submission is original work created by the team members during the current school year. Credits for any students assisting in the project should be listed along with detail regarding ***any and all work performed with advanced material provided or requested work to be performed in advance of competition (e.g. log files analysis or forensics, development/coding, structuring or writing governance/change control material)***.

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 Categories include Securely Provision (SP), Operate and Maintain (OM), Protect and Defend (PR).

Knowledge Performance
This portion of the contest will be a series of comprehensive modules demonstrating skillsets evaluated by progression and advancement in stages.

Skills Performance

This portion of the contest will be a series of Provisioning, Testing, Deployment, Operational and Maintenance, and Protection and Defensive procedures with the end goals set by the technical committee.

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 three stages.
2. The stages of the contest are as follows:
    a. At the first stage, the team members will independently demonstrate their skillsets in specifically designed modules.
        i.
    b. At the second stage, the team will affectively be given a strategic objective and must complete it to advance to the next stage. They will face two to three additional teams.
        i.
    c. At the third stage, the team that successfully completed their tactical objective from stage two will face four to five remaining team finalists.
        i. During stage three, all tactical units may encounter additional challenges staged by the technical committee
        ii. The goal of the final stage will be to technologically incapacitate the infrastructure of the remaining teams
    d. The outcome and winners are determined by the combined scores from all stages
        i. The remaining teams that did not advance will not have credit during the 3rd stage.

Standards and Competencies

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

1.1.1 Knowledge of computer networking concepts and protocols, and network security methodologies

1.1.2 Establish methods for assessing and mitigating risks

1.1.3 Knowledge of cybersecurity and privacy principles

1.1.4 Knowledge of cyber threats and vulnerabilities

1.1.5 Knowledge of data mining and data warehousing principles

1.1.6 Demonstrate business continuity and disaster recovery continuity of operations plans

1.1.7 Demonstrate use of network protocols and interactions that provide network communications

1.1.8 Knowledge of organization's enterprise information security architecture

1.1.9 Knowledge of operating systems

1.1.10 Knowledge of organization's evaluation and validation requirements (Such as patch or vulnerability audit)

1.1.11 Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services

1.1.12 Demonstrate use of networks tools including but not limited to ping, traceroute, nslookup

1.1.13 Knowledge of defense-in-depth principles and network topology security architecture

1.1.14 Compare and contrast the network types (e.g., LAN, WAN, MAN, WLAN, WWAN)

1.1.15 Understand the purposes and functions of files of type (e.g., .dll, .bat, .zip, .pcap, .gzip)

SP 1.2 – Demonstrate abilities to securely provision software including development and modification of code in post-development stages (Securely Provision SP-DEV-002 & SP-SYS-001)

1.2.1 Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy

1.2.2 Knowledge of software development models

1.2.3 Knowledge of software design tools, methods, and techniques including automated systems analysis

1.2.4 Knowledge of complex data structures

1.2.5 Knowledge of programming language structures and logic

1.2.6 Knowledge of embedded systems

1.2.7 Demonstrate security methodologies that apply to software development (relevant to confidentiality, integrity, availability, authentication, non-repudiation)

1.2.8 Demonstrate that development meets regulatory compliance with relation to Privacy Impact Assessments (PIA)
1.2.9 Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org)
1.2.10 Knowledge of structured analysis principles and methods
1.2.11 Demonstrate secure coding techniques
1.2.12 Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, and simplicity/minimization).
1.2.13 Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations
1.2.14 Demonstrate ability to perform conduct coding reviews using knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA])
1.2.15 Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing)
1.2.16 Knowledge of Personally Identifiable Information (PII) data security standards
1.2.17 Knowledge of Payment Card Industry (PCI) data security standards.
1.2.18 Knowledge of Personal Health Information (PHI) data security standards.
1.2.19 Knowledge of penetration testing principles, tools, and techniques.
1.2.20 Knowledge of root cause analysis techniques.

SP 2.1 – Demonstrate abilities to develop and maintain systems. Create enterprise architectural strategies encompassing baseline and target architectures (System Architecture SP-ARC-001)

2.1.1 Knowledge of organization's enterprise information security architecture
2.1.2 Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware)
2.1.3 Demonstrate installation, integration, and optimization of system components
2.1.4 Knowledge of how traffic flows across the network
    a. Open System Interconnection Model [OSI]
    b. Information Technology Infrastructure Library, current version [ITIL]
2.1.5 Knowledge of database systems
2.1.6 Demonstrate key concepts in security management (e.g., Release Management, Patch Management).
2.1.7 Demonstrate systems testing and evaluation methods
2.1.8 Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing)
2.1.9 Knowledge of the systems engineering process
2.1.10 Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools
2.1.11 Knowledge of circuit analysis
2.1.12 Compare and contrast various types of computer architectures
2.1.13 Knowledge of N-tiered typologies (e.g. including server and client operating systems)
2.1.14 Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)
2.1.15 Knowledge of integrating the organization's goals and objectives into the architecture
2.1.16 Determine resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
2.1.17 Knowledge of system fault tolerance methodologies
2.1.18 Demonstrate establishment of demilitarized zones
2.1.19 Demonstrate the network design processes, to include understanding of security objectives, operational objectives
2.1.20 Knowledge of network security (e.g., encryption, firewalls, accounting, authorization authentication, honey pots, perimeter protection)

SP 2.2 – Demonstrate abilities to address all aspects of enterprise architecture including reference

models, segment and solution architectures. (System Architecture SP-ARC-002)

2.2.1 Knowledge of human-computer interaction principles
2.2.2 Demonstrate the functions of authentication, authorization, and access control methods
2.2.3 Contrast Authentication and Identity
  a. Define attribute collection
    i. Preferences
    ii. Traits
  b. Define verification of identity
  c. Define security of the identity
2.2.4 Provide examples of digital identities
2.2.5 Describe the purposes and functions of Digital Object Architecture (DOA)
2.2.6 Identify exploitations in Authorization as defined in IT organizations
2.2.7 Define least privilege
2.2.8 Contrast permissions, rights, and privileges
2.2.9 Define access control lists (ACL)
2.2.10 Describe the purposes and functions of access control models
2.2.11 Identify exploitations in Authentication for methods and services as defined in IT organizations (e.g., SSO, One-Time Passwords, PAP, CHAP, NTLM, NTLMv2, Kerberos, LDAP and Secure LDAP, RADIUS, Diameter, TACACS, XTACACS, and TACACS+, L2TP and PPTP)
2.2.12 Knowledge of communication methods, principles, and concepts that support the network infrastructure
2.2.13 Knowledge of capabilities and applications of network equipment as it relates to transmission media
2.2.14 Knowledge of cyber defense and vulnerability assessment tools for their capabilities and limitations
2.2.15 Knowledge of computer algorithms
2.2.16 Knowledge of encryption algorithms
2.2.17 Knowledge of cryptography and cryptographic key management concepts
2.2.18 Knowledge of industry-standard and organizationally accepted analysis principles and methods
2.2.19 Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML)
2.2.20 Knowledge of parallel and distributed computing concepts
2.2.21 Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions)
2.2.22 Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing)
2.2.23 Knowledge of multi-level security systems and cross domain solutions
2.2.24 Knowledge of program protection planning (e.g. information technology (IT) supply chain risk management policies, anti-tampering techniques
2.2.25 Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features)

SP 2.3 – Knowledge of the theory of information as it pertains data and storage and the ability to manipulate signals in digital form (System Architecture SP-ARC-002)

2.3.1 Describe the conjunction of random variables and mutual information and how they apply to compression principles
2.3.2 Describe the purposes of joint entropy
2.3.3 Describe the purposes of conditional entropy
2.3.4 Describe the purposes of mutual information
2.3.5 Describe the purpose of relative entropy or divergence
2.3.6 Describe source coding theory
2.3.7 Describe channel coding theory
2.3.8 Differentiate binary symmetric channels binary erasure channels
2.3.9 Describe the functions and purposes of digital signal processing and frequency domains
2.3.10 Describe storage types and functions
2.3.11 Describe the functions magnetic storage
2.3.12 Describe the functions of solid state storage

2.3.13 Contrast functions of storage types and outline requirements of maintaining data

a. When defragmentation may be used
b. When trim may be used
c. Leveling strategies or channel level wear

2.3.14 Describe the lifespan of data and retention characteristics

SP 2.4 – Outline principles and concepts of data storage and security (System Architecture SP-ARC-002)

2.4.1 Identify known conventions for Storage Attached Networks
2.4.2 Describe ports and protocols for iSCSI
2.4.3 Describe Fiber channel and current methods of connectivity used
2.4.4 Contrast file level access storage (NAS) vs. storage area networks (SAN)
2.4.5 Describe known methods to secure NFS, iSCSI, SMB3, CIFS when using NAS or SAN
2.4.6 Describe methods to secure data
2.4.7 Demonstrate software level encryption
2.4.8 Demonstrate hardware level encryption
2.4.9 Define data at rest storage and retention policies

SP- 3.1 Demonstrate abilities to complete requirements planning with customer and translate into technical solutions (Systems Requirements Planning SP-SRP-001)

3.1.1 Knowledge of applicable business processes and operations of customer organizations
3.1.2 Knowledge of the organization's enterprise information technology (IT) goals and objectives
3.1.3 Knowledge of capabilities and requirements analysis
3.1.4 Knowledge of encryption algorithms
3.1.5 Knowledge of cryptography and cryptographic key management concepts
3.1.6 Knowledge of resiliency and redundancy
3.1.7 Knowledge of installation, integration, and optimization of system components
3.1.8 Knowledge of controls related to the use, processing, storage, and transmission of data
3.1.9 Knowledge of industry-standard and organizationally accepted analysis principles and methods
3.1.10 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
3.1.11 Knowledge of information security systems engineering principles
3.1.12 Knowledge of information technology (IT) architectural concepts and frameworks
3.1.13 Knowledge of network access, identity, and access management
3.1.14 Knowledge of new and emerging information technology (IT) and cybersecurity technologies
3.1.15 Knowledge of operating systems
3.1.16 Knowledge of Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]
3.1.17 Knowledge of Privacy Impact Assessments
3.1.18 Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org)
3.1.19 Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design
3.1.20 Knowledge of system life cycle management principles, including software security and usability
3.1.21 Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes)
3.1.22 Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures
3.1.23 Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures

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

3.2.1 Demonstrate the ability to conduct testing events
3.2.2 Ability to design data analysis structures (i.e., the types of data a test must generate and how to analyze that data)
3.2.3 Determining an appropriate level of test rigor for a given system(s)
3.2.4 Develop operations-based testing scenarios
3.2.5 Develop testing for systems integration
3.2.6 Writing code in a currently supported programming languages
3.2.7 Proper documentation of testing plans
3.2.8 Evaluating test plans for applicability and completeness
3.2.9 Demonstrate readiness capabilities with regards to testing
3.2.10 Determine adequate resources and personnel to managing test assets, to ensure effective completion of events
3.2.11 Providing time estimates for evaluations

OM 4.1 – Administer databases and data management systems that allow for the secure storage, query, and utilization of data (Operate and Maintain: Data Administration OM-DTA-001)

4.1.1 Knowledge of computer networking protocols and network security methodologies
4.1.2 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk)
4.1.3 Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy
4.1.4 Knowledge of cyber threats and vulnerabilities

4.1.5 Knowledge of specific operational impacts of cybersecurity lapses
4.1.6 Knowledge of data administration and data standardization policies
4.1.7 Knowledge of data backup and recovery including measures to secure backup data
4.1.8 Knowledge of data mining and data warehousing principles
4.1.9 Knowledge of database management systems, query languages, table relationships, and views
4.1.10 Knowledge of digital rights management
4.1.11 Knowledge of enterprise messaging systems and associated software
4.1.12 Knowledge of network access, identity, and access management
4.1.13 Knowledge of policy-based and risk adaptive access controls
4.1.14 Knowledge of database theory
4.1.15 Knowledge of query languages such as SQL (structured query language)
4.1.16 Knowledge of sources, characteristics, and uses of the organization's data assets
4.1.17 Knowledge of the characteristics of physical and virtual data storage media
4.1.18 Knowledge of database access API (e.g., Java Database Connectivity [JDBC])
4.1.19 Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features)
4.1.20 Knowledge of current and emerging data remediation security features in databases
4.1.21 Knowledge of an organization's information classification program and procedures for information compromise
4.1.22 Knowledge of Personally Identifiable Information (PII) data security standards
4.1.23 Knowledge of Payment Card Industry (PCI) data security standards
4.1.24 Knowledge of Personal Health Information (PHI) data security standards

OM 4.2 – Provides technical support and incident management to customers who need assistance utilizing client level hardware and software (Operate and Maintain: Customer Service and Technical Support OM-STS-001)

4.2.1 Knowledge of measures or indicators of system performance and availability
4.2.2 Knowledge of systems administration concepts
4.2.3 Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)
4.2.4 Knowledge of computer systems/components, access control devices, digital cameras, digital scanners, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, and facsimile machines
4.2.5 Knowledge of files of type (e.g., .dll, .bat, .zip, .pcap, .gzip)
4.2.6 Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration
4.2.7 Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems
4.2.8 Knowledge of industry best practices for service desk
4.2.9 Knowledge of remote access processes, tools, and capabilities related to customer support
4.2.10 Knowledge of Personally Identifiable Information (PII) data security standards
4.2.11 Knowledge of Payment Card Industry (PCI) data security standards
4.2.12 Knowledge of Personal Health Information (PHI) data security standards
4.2.13 Knowledge of an organization's information classification program and procedures for information compromise
4.2.14 Knowledge of the operations and processes for incident, problem, and event management
4.2.15 Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly
4.2.16 Knowledge of procedures used for documenting and querying reported incidents, problems, and events
4.2.17 Knowledge of Capabilities to identify the solutions to less common and more complex system problems

OM 4.3 – Plans, implements, and operates network services/systems, to include hardware and virtual environments. (Operate and Maintain: Network Services OM-NET-001)

4.3.1 Use communication methods, principles, and concepts to support the network infrastructure
4.3.2 Demonstrate ability to manage applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware
4.3.3 Manage all Local and Wide Area Network connections
4.3.4 Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data
4.3.5 Explain and demonstrate the process of bandwidth management
4.3.6 Measure and monitor system performance including establishing indicators of system performance and availability
4.3.7 Identify and use in practice how OSI layer models relate to network traffic
4.3.8 Use in application remote access technology
4.3.9 Practice server administration and systems engineering , concepts, and methods
4.3.10 Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
4.3.11 Establish and maintain Virtual Private Network (VPN) security
4.3.12 Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless)
4.3.13 Demonstrate use of network tools to further network informational knowledge or to identify an known or unknown issue
4.3.14 Contrast different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN)
4.3.15 Identify or use in practice web filtering technologies
4.3.16 Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts)
4.3.17 Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA)
4.3.18 Identify common attack vectors on the network layer
4.3.19 Provide application of defense-in-depth to network security architecture
4.3.20 Use of symmetric key rotation techniques and concepts
4.3.21 Identify security models (e.g., Bell-LaPadula model, Biba integrity model, Clark Wilson integrity model)
4.3.22 Review transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly
4.3.23 When compromised, identify an organization's information classification program and procedures for communication and response

OM 4.4 – Integration, testing and operation. Including but not limited to operations and maintenance of systems security (Operate and Maintain: Systems Analysis OM-ANA-001)

4.4.1 Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
4.4.2 Employ computer algorithms, encryption algorithms, cryptography and cryptographic key management concepts
4.4.3 Identify potential security compromises to database systems and provide analysis
4.4.4 Act upon vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins)
4.4.5 Ensure confidentiality, integrity, availability, authentication, non-repudiation while maintaining systems
4.4.6 Provide in-depth subject matter expertise for firewalls and demilitarized zone configuration and operation
4.4.7 Manage and configure public key infrastructure
4.4.8 Identify operating system security compromises and close security loopholes
4.4.9 Use the systems engineering process and knowledge of computer architecture to ensure redundancy of systems

4.4.10 Provide analysis of network state and security using end to end system performance monitoring
4.4.11 Use network analysis tools to identify vulnerabilities
4.4.12 Use in practice risk management policies/procedures
4.4.13 Evaluate the trustworthiness of the supplier and/or product
4.4.14 Demonstrate developing and applying user credential to a management system
4.4.15 Implement enterprise key escrow systems to support data-at-rest encryption
4.4.16 When compromised, determine the classification program and procedures for the level of information compromised
4.4.17 Deploy countermeasures designed for identified security risks

PR 5.1 – 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 PR-VAM-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)

5.1.1 Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures
5.1.2 Knowledge of Insider Threat investigations, and reporting
5.1.3 Demonstrate use of authentication, authorization, and access control methods including auditing trails
5.1.4 Demonstrate abilities to identify gaps in access control lists and modify ACL
5.1.5 Knowledge of cyber defense and vulnerability assessment tools and their capabilities
5.1.6 Demonstrate use of cryptography and cryptographic key management abilities
5.1.7 Demonstrate use of database systems and analysis
5.1.8 Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins)
5.1.9 Execute incident response procedures and demonstrate response handling methodologies
5.1.10 Communicate cyber defensive responses as they pertain to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
5.1.11 Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools
5.1.12 Validate intrusion detection methodologies and demonstrate skillsets for detecting host and network-based intrusions
5.1.13 Knowledge of the use of sub-netting tools
5.1.14 Present network defense strategies including but not limited to firewalls, demilitarized zones (includes all devices within the DMZ address space), and encryption methods
5.1.15 Demonstrate public key infrastructure security including, Oauth, OpenID, SAML, SPML
5.1.16 Demonstrate packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump) to identify intrusion(s)
5.1.17 Knowledge of operating system command-line tools
5.1.18 Identify and close operating systems security loopholes or unsecured configurations, apply where necessary operating filtering policies (e.g., hardening techniques, software firewalls, OS local or group policies, trap/redirection of infiltration to honeynets)
5.1.19 Knowledge of policy-based and risk adaptive access controls (e.g., system based firewall policy, OS local or group policies, cloud based security intelligence)
5.1.20 Identify security threats and vulnerabilities (e.g., buffer overflow, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)
5.1.21 Demonstrate Release Management and Patch Management
5.1.22 Demonstrate knowledge of reporting structure and processes within one's own organization
5.1.23 Identify potential security risks between VPN connections and offer/implement solutions to reduce threats

5.1.24 Identify what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
5.1.25 Demonstrate adversarial tactics, techniques, and procedures
5.1.26 Identify how defense-in-depth principles and network security architecture has been compromised
5.1.27 For any service or server with ability to communicate on a WAN determine what files of type must be secured from operation (e.g., .cab, .rar, tar, gz, .zip, .pcap, .gzip)
5.1.28 Knowledge of collection management processes, capabilities, and limitations
5.1.29 Identify and provide examples of front-end collection systems, including traffic collection, filtering, and selection
5.1.30 Identify and close gaps on all common attack vectors on the network layer
5.1.31 Identify and differentiate classes of attacks (e.g., passive, active, insider, close-in, distribution attacks)
5.1.32 Profile cyber attackers by methods of operation and signatures (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored)
5.1.33 Identify cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)
5.1.34 Describe Signature implementation impact for viruses and malware
5.1.35 Develop countermeasure design for identified security risks
5.1.36 Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

PR 5.2 – Investigate, analyze, and respond to cyber incidents within organization. Test, implement, deploy, maintains and administer the infrastructure hardware and software (Protect and Defend: Incident Response PR-CIR-001) (Protect and Defend: Cyber Defense Infrastructure Support PR-INF-001)

5.2.1 Identify procedural requirements based on information security policies
5.2.2 Execute data backup, continuity, and recovery procedures
5.2.3 Identify capabilities based on ACL for host/network control mechanisms
5.2.4 Initiate incident response and handling
5.2.5 Examine organizational requirements to determine confidentiality, integrity, availability, authentication, non-repudiation to establish categorical level of information breach
5.2.6 Demonstrate network traffic and packet-level analysis methods
5.2.7 Provide packet-level analysis of VPN tunnels
5.2.8 Identify common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications
5.2.9 Establish when analysis constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
5.2.10 Demonstrate the ability to filter URL or Web based on specific parameters including categorical and block reputation listings (BRL)
5.2.11 Provide in depth defense of network security architecture
5.2.12 Demonstrate OS hardening techniques
5.2.13 Demonstrate test procedures and methods
5.2.14 Produce transmission records (e.g., Bluetooth, RFID, IR, Wi-Fi. Secured Texting, VoIP) to validate installed systems are operating correctly
5.2.15 Demonstrate use of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools

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

Source: NIST Publication 800-181 CyberSecurity Workforce Framework
http://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:
http://www.ncte.org/standards/ncte-ira