CCDC Team Preparation Guidelines

CCDC Teams should process the following skills and knowledge to be successful in a competition. The competitions are designed to measure these areas and general skills. The list is not comprehensive but highlights the core areas.

CAREER ACQUISITION SKILLS

Most Colleges and Universities have Career Services offerings or courses with these features embedded within them. CCDC students should have completed:

- ☑ A career exploration activity in which they discover the variety of jobs within Cybersecurity and the corresponding skills-base they require.
- ☑ A resume writing workshop with a resume critique.
- ☑ A mock interview or other interview preparation workshop.
- ☑ Actively attended a career fair, in which they interacted with employers.

BUSINESS COMMUNICATIONS SKILLS

One of the aspects of CCDC is the sharing of information with senior management. If a technical writing course is not part of the student's curriculum, then a technical writing workshop should be arranged for CCDC students. Students need to acquire the following skills in this area:

- ☑ How to present technical information to a non-technical, business audience.
- ☑ How to structure a document such that:
  - Its purpose is readily ascertained.
  - The document needs to guide the reader through its purpose, data presentation, to its conclusion.
  - Tables and graphs need to be clearly labeled/captioned as to what they are and why they are present.
  - Writing needs to be succinct and present a professional tone.
  - Avoid statements and styles that are likely to distract from the purpose of the document or present a non-professional appearance.

DESIGN & ARCHITECTURE SKILLS

CCDC students should understand network architecture principles as outlined in a CISCO Academy curriculum. In addition, the function of a DMZ and the benefits of network segmentation should be understood.

Students should understand basic operating system architecture principles, particularly as it relates to process and file system security issues.

It is important know the components and issues in designing a resilient network, and the concepts of high availability (HA) configured devices.

EVALUATION & RISK ASSESSMENT SKILLS

CCDC students should be able to use basic tools, such as NMAP or other similar scanners to evaluate the services being offered at the perimeter of their networks, or those offered by a particular device (server).

Students should be able to critically assess a device (Linux/Windows), or appliance (firewall, network equipment) for security vulnerabilities or signs of compromise.

Students should understand the principles of risk assessment and mitigation of vulnerabilities, which include prioritizing resources based upon the risk.

Students should be able to evaluate their security posture and mitigation efforts against a Security Framework.

Students should be familiar with various attack approaches and vectors, and associated mitigation strategies.

LEGAL FRAMEWORKS & POLICY SKILLS

CCDC students should be familiar with concepts and intent of security frameworks. Teams should be able to form their own defense strategies in light of the basic tenets of well-known frameworks such as:

- ☑ NIST 800-171
- ☑ NIST 800-53
- ☑ ISO-27002
- ☑ CIS Critical Security Controls (20 Critical Security Controls)

Students should know the difference and application of a Policy, Procedure and Guideline — in terms of how they are composed and their purpose within an organization. Students should be able to write examples of each of these.

Students should understand the concepts of:

- ☑ Due Care
- ☑ Due Diligence
- ☑ Chain of Custody and how to keep records to be used in evidence
- ☑ The special nature of computerized logs and their exception to the hearsay principle
- ☑ The security goals of Confidentiality, Integrity and Availability
- ☑ Basic tenets of the US cyber security laws
- ☑ The data privacy approach by the US vs Europe as represented by the GDPR.
- ☑ The features of change control that minimize mistakes.

LINUX SYSTEM ADMINISTRATION SKILLS
CCDC students should be able to:

- ☑ Install the operating system.
- ☑ Understand startup configuration files
- ☑ Understand how typical and key services are configured
- ☑ Understand how networking facilities are configured
- ☑ Understand how software firewalls are configured
- ☑ Understand how users and groups are provisioned
- ☑ Understand the deployment of privileges
- ☑ Understand file system security
- ☑ Shell scripting skills
- ☑ Administration of batch-job facilities
- ☑ Configuring SYSLOG and SNMP

WINDOWS SYSTEM ADMINISTRATION SKILLS

- ☑ Install the operating system.
- ☑ Understand how typical and key services are configured
- ☑ Understand how networking facilities are configured
- ☑ Understand how software firewalls are configured
- ☑ Understand how users and groups are provisioned
- ☑ Understand the deployment of privileges
- ☑ Understand file system security
- ☑ Shell and Power Shell scripting skills
- ☑ Administration of batch-job facilities
- ☑ Configuring SYSLOG and SNMP

NETWORKING CONCEPTS & CONFIGURATION SKILLS
CCDC students should be able to configure Cisco routers and switches and know how to harden them. Specific skills areas should include:

- ☑ Knowledge of TCP/IP and network addressing.
- ☑ Securing administrative access.
- ☑ Securing SNMP access.
- ☑ Writing standard and extended access lists and how to apply them.
- ☑ Configuring context-based access lists (CBAC).
- ☑ Configuring the IOS Policy Firewall features.
- ☑ The concept of a screening firewall.
- ☑ Packet capture tools and analysis.
- ☑ Configuring virtual private networks.
- ☑ Configuring SSH functionality.
- ☑ How to disable unneeded services.
- ☑ General best practice configuration guidelines as outlined in a Cisco Academy curriculum.

HUMAN RESOURCE ORGANIZATION SKILLS

CCDC Teams need to be organized in order to provide an effective defense and demonstrate their operational skills. Teams should develop internal procedures and checklist as to how they are going to operate during the competition. An organization should be developed with members that have overlapping skills sets. The organization structure together with the procedures will insure the best utilization of everyone's skills during the competition.

SOFTWARE INSTALLATION & DEBUGGING SKILLS

CCDC students should know how to install software on Linux and Windows machines and develop procedures to verify the integrity and security of any new software.

Students should understand how to use package managers, and leveraging virtualization environments, such as Docker, when installing new software.

Specific backgrounds in the following:

- ☑ Apache and Windows web services.
- ☑ Installing network management tools such as:
  - Libre NMS
  - OpenView
  - Observium
  - Cacti
- ☑ Network evaluation tools:
  - Wire Shark
  - NMAP
  - Open VAS
- ☑ Syslog receivers
  - Syslog NG
  - Kiwi Syslog
  - Splunk

FIREWALL DEVICES & SECURITY TOOLS KNOWLEDGE

CCDC students need to have knowledge and experience with configuring, debugging and fully utilizing the following firewall products:

- ☑ Palo Alto Firewalls
- ☑ PF Sense Firewalls
- ☑ Cisco Firewalls

Students need to have specific knowledge on configuring:

- ☑ Network address translation (NAT/PAT).
- ☑ Application-layer security policies vs layer-3 or 4 policies.
- ☑ Enabling threat (IPS) protection with a security policy.

Experience with other security tools, such as Snort and those found within Security Onion.

CRYPTOGRAPHY
CCDC students should:

- ☑ Understand how cryptographic technology can be used to implement the security goals of confidentiality, data integrity and infrastructure availability.
- ☑ The applications of:
  - Hash functions
  - Symmetric encryption algorithms
  - Asymmetric encryption algorithms
  - IPSEC configuration
  - SSL and TLS configuration
  - The deployment of certificates and using a certificate authority

VIRTUALIZATION SKILLS
CCDC student should be able to:

- ☑ Install, configure and troubleshoot VMWare ESXI installation.
- ☑ Install, configure and troubleshoot Docker environments.
- ☑ Design knowledge of benefits of using virtualization in building out an organization's infrastructure.