NSA/DHS CAE in IA/CD

2014 Mandatory Knowledge Unit Checklist – 4 Year+ Programs

Mandatory Knowledge Units

1.0 Core2Y

1.1 Basic Data Analysis

The intent of this Knowledge Unit is to provide students with basic abilities to manipulate data into meaningful information.

1.1.1 Topics

____ Summary Statistics
____ Graphing / Charts
____ Spreadsheet Functions
____ Problem solving

1.1. 2 Outcomes

Students will be able to:
____ Apply standard statistical inference procedures to draw conclusions from data.

1.2 Basic Scripting or Introductory Programming

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

1.2.1 Topics

____ *Basic Security
    ____ Bounds checking, input validation
____ Program Commands
____ Program Control Structures
____ Variable Declaration
____ Debugging
____ Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)
____ *Basic Boolean logic/operations
    ____ AND / OR / XOR / NOT

1.2.2 Outcomes

Students will be able to:
____ Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).
____ Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
____ Write simple linear and looping scripts.

1.3 Cyber Defense

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

1.3.1 Topics:

____ Network mapping (enumeration and identification of network components)
____ *Network security techniques and components
    ____ Access controls, flow control, cryptography, firewalls, intrusion detection systems, etc.
____ Applications of Cryptography

* = Can include a summary justification for that section.

____ Malicious activity detection / forms of attack
____ Appropriate Countermeasures
____ Trust relationships
____ *Defense in Depth
    ____ Layering of security mechanisms to achieve desired security
____ *Patching
    ____ OS and Application Updates
____ Vulnerability Scanning
____ Vulnerability Windows (0-day to patch availability)

1.3.2 Outcomes:

Students will be able to:
____ Describe potential system attacks and the actors that might perform them
____ Describe cyber defense tools, methods and components
____ Apply cyber defense methods to prepare a system to repel attacks
____ Describe appropriate measures to be taken should a system compromise occur.

1.4 Cyber Threats

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

1.4.1 Topics:

____ Adversaries and targets
____ Motivations and Techniques
____ The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)
____ *Types of Attacks
    ____ Password guessing / cracking
    ____ Backdoors / trojans / viruses / wireless attacks
    ____ Sniffing / spoofing / session hijacking
    ____ Denial of service / distributed DOS / BOTs
    ____ MAC spoofing / web app attacks / 0-day exploits
    ____ Vulnerabilities that enable attacks
____ Attack Timing (within x minutes of being attached to the net)
____ Social Engineering
____ Events that indicate an attack is/has happened
____ Legal Issues
____ Attack surfaces / vectors
____ Attack trees
____ Insider problem
____ Covert Channels
____ Threat Information Sources (e.g., CERT)

1.4.2 Outcomes:

Students will be able to:
____ Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk
____ Describe different types of attacks and their characteristics

1.5 Fundamental Security Design Principles

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

1.5.1 Topics:

____ Separation (of domains)
____ Isolation
____ Encapsulation
____ Least Privilege
____ Simplicity (of design)
____ Minimization (of implementation)
____ Fail Safe Defaults / Fail Secure
____ Modularity
____ Layering
____ Least Astonishment
____ Open Design
____ Usability

1.5.1 Outcomes:

Students will be able to:

____ List the first principles of security
____ Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
____ Analyze common security failures and identify specific design principles that have been violated
____ Identify the needed design principle when given a specific scenario
____ Describe why good human machine interfaces are important to system use
____ Understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms

1.6 Information Assurance Fundamentals

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

1.6.1 Topics

____ Threats and Adversaries
____ Vulnerabilities and Risks
____ Basic Risk Assessment
____ Security Life-Cycle
____ Intrusion Detection and Prevention Systems
____ Cryptography
____ Data Security (in transmission, at rest, in processing)
____ Security Models
____ Access Control Models (MAC, DAC, RBAC)
____ Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
____ Security Mechanisms (e.g., Identification/Authentication, Audit)

1.6.2 Outcomes

Students will be able to:

____ List the fundamental concepts of the Information Assurance / Cyber Defense discipline

____ Describe how the fundamental concepts of cyber defense can be used to provide system security

____ Examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed

1.7 Introduction to Cryptography

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

1.7.1 Topics

____ Symmetric Cryptography (DES, Twofish)

____ *Public Key Cryptography

- ____ Public Key Infrastructure
- ____ Certificates

____ *Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)

- ____ For integrity
- ____ For protecting authentication data
- ____ Collision resistance

____ Digital Signatures (Authentication)

____ Key Management (creation, exchange/distribution)

____ Cryptographic Modes (and their strengths and weaknesses)

____ Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)

____ Common Cryptographic Protocols

____ DES -> AES (evolution from DES to AES)

____ Security Functions (data protection, data integrity, authentication)

1.7.2 Outcomes

Students will be able to:

____ Identify the elements of a cryptographic system

____ Describe the differences between symmetric and asymmetric algorithms

____ Describe which cryptographic protocols, tools and techniques are appropriate for a given situation

____ Describe how crypto can be used, strengths and weaknesses, modes, and the issues that must be addressed in an implementation (e.g., key management), etc

1.8 Information Technology System Components

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

1.8.1Topics

____ Workstations

____ Servers

____ Network Storage Devices

____ Routers / Switches / Gateways

____ Guards / CDSes / VPNs / Firewalls
____ IDSes, IPSes
____ Mobile Devices
____ Peripheral Devices / Security Peripherals

1.8.2 Outcomes

Students will be able to:

____ Describe the hardware components of modern computing environments and their individual functions

1.9 Networking Concepts

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

1.9.1 Topics

____ Overview of Networking (OSI Model)
____ Network Media
____ Network architectures (LANs, WANs)
____ Network Devices (Routers, Switches, VPNs, Firewalls)
____ Network Services
____ Network Protocols (TCP/IP, HTTP, DNS, SMTP, UDP)
____ Network Topologies
____ Overview of Network Security Issues

1.9.2 Outcomes

Students will be able to:

____ Describe the fundamental concepts, technologies, components and issues related to communications and data networks.
____ Describe a basic network architecture given a specific need and set of hosts/clients.
____ Track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
____ Use a network monitoring tool (e.g., WireShark).
____ Use a network mapping tool (e.g., Nmap).

1.10 Policy, Legal, Ethics and Compliance

The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

1.10.1 Topics

____ HIPAA / FERPA
____ Computer Security Act
____ Sarbanes – Oxley
____ Gramm – Leach – Bliley
____ Privacy (COPPA)
____ Payment Card Industry Data Security Standard (PCI DSS)
____ State, US and international standards / jurisdictions
____ Laws and Authorities
____ US Patriot Act
____ BYOD issues

____ Americans with Disabilities Act, Section 508

1.10.2 Outcomes

Students will be able to:

____ List the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data

____ Describe their responsibilities related to the handling of information about vulnerabilities

____ Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it

1.11 Systems Administration

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

1.11.1 Topics

____ OS Installation
____ User accounts management
____ Password policies
____ Authentications Methods
____ Command Line Interfaces
____ Configuration Management
____ Updates and patches
____ Access Controls
____ Logging and Auditing (for performance and security)
____ Managing System Services
____ Virtualization
____ Backup and Restoring Data
____ File System Security
____ Network Configuration (port security)
____ Host (Workstation/Server) Intrusion Detection
____ Security Policy Development

1.11.2 Outcomes

Students will be able to:

____ Apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup

2.0 Core to 4 year+ only

2.1 Database Management Systems

The intent of this Knowledge Unit is to provide students with the skills to utilize database management system to solve specific problems.

2.1.1 Topics

____ Overview of database types (e.g., flat, relational, network, object-oriented)
____ SQL (for queries)
____ Advanced SQL (for DBMS administration – e.g., user creation/deletion, permissions and access controls)

____ Indexing, Inference, Aggregation, Polyinstantiation
____ How to protect data (confidentiality, integrity and availability in a DBMS context)
____ Vulnerabilities (e.g., SQL injection)

2.1.2 Outcomes

Students will be able to:
____ List the most common structures for storing data in a database management system
____ Configure a commodity DBMS for secure access
____ Describe alternatives to relational DBMSs and their unique security issues
____ Describe the role of a database, a DBMS, and a database server within a complex system supporting multiple applications
____ Demonstrate basic SQL proficiency for table creation, data insertion and data query
____ Describe DBMS access controls and privilege levels and apply them to a simple database
____ Develop a DB structure for a specific system/problem.

2.2 Network Defense

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

2.2.1 Topics

____ Implementing IDS/IPS
____ Implementing Firewalls and VPNs
____ Defense in Depth
____ Honeypots and Honeynets
____ Network Monitoring
____ Network Traffic Analysis
____ Minimizing Exposure (Attack Surface and Vectors)
____ Network Access Control (internal and external)
____ DMZs / Proxy Servers
____ Network Hardening
____ Mission Assurance
____ Network Policy Development and Enforcement
____ Network Operational Procedures
____ Network Attacks (e.g., session hijacking, Man-in-the-Middle)

2.1.2 Outcomes

Students will be able to:
____ Describe the various concepts in network defense.
____ Apply their knowledge to implement network defense measures.
____ Use a network monitoring tools (e.g., WireShark).
____ Use a network mapping tool (e.g., Nmap).

2.3 Network Technology and Protocols

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

2.3.1 Topics

____ Network Architectures
____ Networks Infrastructure

____ Network Services
____ Network Protocols (TCP/IP – v4 and v6, DNS, HTTP, SSL, TLS)
____ Network Address Translation and Sub-netting
____ Network Analysis/Troubleshooting
____ Network Evolution (Change Management, BYOD)
____ Remote and Distributed Management

2.3.2 Outcomes

Students will be able to:
____ Apply their knowledge of network technologies to design and construct a working network
____ Analyze a trace of packets to identify the establishment of a TCP connection
____ Demonstrate the use of a network monitor to display packets

2.4 Operating Systems Concepts

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

2.4.1 Topics

____ Privileged and non-privileged states
____ Processes and Threads (and their management)
____ Memory (real, virtual, and management)
____ Files Systems
____ *Access Controls (Models and Mechanisms)
    ____ Access control lists
____ Virtualization / Hypervisors
____ How does the an OS protect itself from attack?
____ *Fundamental Security Design Principles as applied to an OS
    ____ Domain separation, process isolation, resource encapsulation, least privilege

2.4.2 Outcomes

Students will be able to:
____ Identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)

2.5 Probability and Statistics

The intent of this Knowledge Unit is to provide students with the ability to use basic statistics to analyze and attach meaning to datasets.

2.5.1 Topics

____ Probability as a concept
____ Random variables/events
____ Odds of an event happening
____ Data Interpretation
____ Statistical Problem Solving
____ Probability Distributions

2.5.2 Outcomes

Students will be able to:
____ Evaluate probabilities to solve applied problems
____ Describe how basic statistics and statistical methods can be applied in a given situation

2.6 Programming

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

2.6.1 Topics

____ Programming Language, such as: C
____ Programming constructs and concepts variables, strings, assignments, sequential execution, loops, functions
____ Security issues, such as type checking and parameter validation
____ *Basic Boolean logic/operations
____ AND / OR / XOR / NOT

2.6.2 Outcomes

Students will be able to:

____ Demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner
____ Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL)
____ Demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web)