Prerequisite Competencies for NCC 210: Information Security Fundamentals Course
(Mastery Learning Version)

In Competency Based Education (CBE), the focus is on personalizing the educational experience in order to increase the number of the capable individuals who can perform the work. CBE instruction is driven by embedded assessments within each learning module that are designed to accurately identify and eliminate the obstacles to the development of competency. It follows that readiness for a CBE-based course is also assessed using instruments that accurately identify deficiencies and direct towards prerequisite instructional knowledge.

Before brainstorming the instructional topics in the National CyberWatch Center's (NCC) 210: Information Security Fundamentals course, a concrete understanding of the expected learner background and competencies possessed is required. The project leadership team has established the following incoming pathways to the NCC 210 course.

Incoming Pathways

When thinking about competencies, they tend to be grounded in specific technologies as that is where skills and abilities are acquired. As a result, specific certification exams from technology vendors may be recommended to identify target student populations. Here are some examples:

- **Computer Services:**
  - Comptia: A+
  - Apple: Apple Certified Support Professional (ACSP)

- **Networking:**
  - Comptia: Network+
  - Cisco: CCENT, CCT
  - Microsoft: MTA
  - Juniper: JNCIA-JUNOS

- **Administration (Advanced):**
  - LF: LPIC-1: System Administrator
Comptia: Linux+, Server+

- 2+ years of technology experience

The project leadership team has also identified potential outgoing pathways and expectations for a learner after mastering the competencies in the NCC 210 course.

Outgoing Pathways

- Certifications
  - Comptia: Security+
  - ISC²: SSCP (Systems Security Certified Practitioner)

- Advanced NCC Courses
  - Digital Forensics
  - Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS)
  - Advanced Network Security

Course Readiness Domains and Topics

The project leadership team has determined the following 9 domains¹ demonstrate readiness for the NCC 210 course. This list is meant to help the Information Security Fundamentals Standards Panel to baseline student preparedness for topics proposed to be included in the competency-based, mastery learning NCC 210 course library:

1. Modular Arithmetic
2. Hexadecimal (Hex) and Binary Number System Arithmetic
3. Regular expressions
4. Memory management and organization
5. Computer Architecture
6. Networking
7. Linux Administration
8. Bash Scripting
9. Windows Administration

For each domain the following topics have been identified:

1. Modular Arithmetic
   a. Declarative Knowledge

¹ See Taxonomy document for definition of terms used in this document.
i. Modular Arithmetic

2. Hexadecimal (Hex) and Binary Number System Arithmetic
   a. Declarative Knowledge
      i. Hex Numeral System Symbols
      ii. Binary Numeral System Symbols
   b. Procedural knowledge (Hex - Decimal Conversion) ²
      i. Steps to convert a hex number to decimal
      ii. Steps to convert a decimal number to hex
   c. Procedural knowledge (Binary - Hex Conversion)
      i. Steps to convert a binary number to hex
      ii. Steps to convert a binary number to decimal

Potential test bank for binary-hex-decimal conversion

3. Regular expressions
   a. Declarative knowledge
      i. Regex Metacharacters
         Test: Match meta-characters to their meaning
   b. Procedural knowledge
      i. Steps to write a regex for a given match criteria
         Test: Online test for Regex skills, Test bank for Regex

4. Memory management and organization
   a. Declarative knowledge
      i. Types of memory
         Test: Distinguish RAM from ROM
      ii. Program organization in memory
         Test: Describe code and data organization in memory
   b. Procedural knowledge
      i. Steps to get a live memory dump

² If there are multiple steps in a topic, a procedural assessment instrument would list the correct steps plus other distractor steps in a question that asks subjects to select and order the steps in this procedure. A step error would be due to incorrect understanding of the steps involved. An order error would be due to incorrect understanding of step relationships.

If the procedure only involves a single step, then per Anderson & Jones (1981) this should be considered a "rule" -- a type of declarative knowledge.

REFERENCE
Test: recognize steps for getting a memory dump in Linux
   Test: recognize steps for getting a memory dump in Windows

ii. Steps to examine a binary in a hex editor
   Test: Identify sections of a binary file in a hex editor

5. Computer Architecture
   a. Declarative knowledge
      i. Computer organization and architectures
         Test: Describe von Neumann architecture. Both x86 and ARM follow von Neumann.

6. Networking
   a. Declarative knowledge
      i. TCP-IP Network layers
         Test: Identify the layers
      ii. Routers
         Test: Describe how routing works at the network layer
         Test: Identify basic admin commands to view current configuration
         Test: Identify basic admin commands to modify configuration settings
   b. Procedural knowledge
      i. Steps to access the admin console for a router and modify settings for a given requirement

7. Linux Administration
   a. Declarative knowledge
      i. User Privileges
         Add user
         Give sudo permissions to user
      ii. File Permissions
         Chmod and permission types
      iii. Editing Files
         Nano and vi
      iv. Data Manipulation
         grep, sed, awk
      v. Processes and Services
         Service command usage
      vi. Managing Networking (Prerequisite: Networking)
         ifconfig, route, /etc/network/interfaces, netstat -antp
         Recon: whois, nslookup
      vii. Netcat: The Swiss Army Knife of TCP/IP Connections
Check ports, listen on a port, connect to a listening port, command shell listener, push a command shell to listener, file redirection

b. **Procedural knowledge**
   i. Steps to search a string in a file and parse out relevant text
   ii. Steps to install a package after adding a repository
   iii. Steps to open a netcat command shell listener and connect to it
   iv. Automating Tasks with cron Jobs
   v. Steps to automate backups using a daily cron job

References:
- Chapter 2: Penetration testing: a hands-on introduction to hacking by Georgia Weidman, Peter Van Eeckhoutte

8. **Basic Bash Scripting (Prerequisite: Linux Administration)**
   a. **Declarative knowledge**
      i. Specify bash interpreter
      ii. Make script executable
      iii. Run a bash script
      iv. if condition
      v. for loop
      vi. Avoiding side-effects
   b. **Procedural knowledge**
      i. A bash script to accomplish a network scan

References:
- Penetration testing: a hands-on introduction to hacking by Georgia Weidman, Peter Van Eeckhoutte
- Other scripting tasks for pentesting
- Question bank to assess *advanced* shell scripting: [http://www.freeos.com/guides/lsst/ch08.html#q7](http://www.freeos.com/guides/lsst/ch08.html#q7)

9. **Windows Administration**
   a. **Declarative knowledge**
      i. ACL
         Basic permissions (Full control, modify, …)
         Advanced permissions
         Powershell (Get-Acl, Set-Acl)
      ii. Windows shares
net share, net view, net use

iii. Registry manipulation
Query for keys
Add registry key and value
Export and import registry
reg command

iv. Windows Management Instrumentation Command-line (WMIC) tool
General structure
List all attributes of an alias
List callable methods

v. Process and service information
List processes
List processes running a DLL
List processes and associated services
Query service status
Query service configuration

vi. Network Query and Manipulation
Network usage
Firewall configuration
Network interface configuration
Configure DNS
Configure DHCP

vii. Miscellaneous
Shutdown and restart
File search
Loops
Invoking utilities from command line

Reference: