K2W Cyber Security CSC Template (LF298.CyberSecurity.Template.K2W)
- K2W Cyber Security
- Support Team
- Cybersecurity Competition
- Web Links
- Network Concepts
- Network Security Basics
- Attacks & Crimes
- Access & Authentication
- Firewalls & E-Commerce
- Network Security Layers
- Legal Topics
- Weekly Interaction
- Competency Progress
- K2W Website
- Library Help
- LFCC Help & Support

Course Management

Control Panel
- My Files
- Course Tools
- Evaluation
- Grade Center
- Users and Groups
- Customization
- Packages and Utilities
- Help

Quick Unenroll

# Attacks & Crimes

Build Content | Assessments | Tools | Partner Content | Discover Content

## Introduction & Procedures

Enabled: Statistics Tracking

This topic area will demonstrate the various methods for attacking and defending a network such as security from the viewpoint of hackers and their attack methodologies, Intrusion Detection Systems, malicious code, computer crime, and industrial espionage.

A student must achieve a minimum of 80% of the total points allowed for this competency. That equates to 760 points out of 950 points. How this score is calculated can be found as descriptions under the various topics. Do not assume that each task is successfully accomplished if 80% is achieved for that particular task. Take notice of the variances.

Completion of the following tasks are required after completing Network Concepts and Network Security Basics:

1. **Hacker Techniques, Tools & Incident Handling VLE labs Competency Assignment:** (Complete ALL 10 virtual labs These labs can be accessed via the Hacker Techniques VLE Competency Lab link given below. Since the student will need to purchase an access code for these labs, a link is also provided below to do that.)
2. **Tools/Techniques Analytical Competency Assignment** (Click on the folder name and the assignments are given within that folder. Please read the background information prior to starting this.)
3. **Hacker Techniques & Tools Competency Assessment #1** (An assessment using multiple choice, and short answer and essay type questions; student gets two attempts to achieve the required score.)
4. **Hacker Techniques & Tools Competency Assessment #2** (An assessment similar in format to assessment #1 cover other materials; Student gets two attempts to achieve the required score)

Furthermore, in order to assist the student, Digital resources are provided as learning tools to enhance the student's knowledge as preparation for accomplishing any of these tasks.

## Required Competencies

Enabled: Statistics Tracking

- Describe the layers, protocols and components of the OSI model.
- Summarize the flow of data through a computer network scenario.
- Use a programming or a scripting language to share data across an integrated IT system.
- Summarize the security implications and risks for distributed IT systems.
- Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario.
- Demonstrate professional behavior in response to an ethically challenging scenario in computing.
- Summarize the tenets of ethics and professional behavior promoted by international computing societies.

## Digital Learning Resources

Enabled: Statistics Tracking

These learning resources will help you learn areas of Network Attacks, Computer Crime and Hacking.

This folder contains digital learning resources that cover the competency areas.

- It is recommended that the learner review this information prior to taking the two assessments.
- If a passing score is not earned on assessments, the learner should review this material before attempting the assessments again

## Hacker Techniques, Tools, and Incident Handling Virtual Lab Access Code Purchasing

Enabled: Adaptive Release, Statistics Tracking

- The student must purchase the access code to complete Lab Activities
- All labs must be completed
- A score of at least 80% must be earned on each lab. See details under the VLE Lab assignment.

Purchase lab access at http://www.shopjblearning.com/shop_home.php

Hacker Techniques, Tools, and Incident Handling Second Edition (Oriyano) – ISBN 978-1-284-06505-3

Plug the ISBN in the search bar and purchase from there. Please read site details before purchasing.

## Hacker Techniques, Tools and Incident Handling Virtual Lab Hands-On Competency Assignment

Enabled: Adaptive Release, Statistics Tracking

Contains introductory descriptions and links to the various labs. There are ten labs. Please see the descriptions as to expectations and points

awarded.

**Tools/Techniques Analytical Competency Assignments**

Enabled: Adaptive Release

Contain individual tasks measuring certain competencies of the student

**Hacker Techniques & Tools Competency Assessment #1**

Enabled: Adaptive Release

Multiple Choice, and an interesting scenario. For success in this competency assessment, 120 points required out of 150 points. (80%)

**Hacker Techniques & Tools Competency Assessment #2**

Enabled: Adaptive Release

Multiple Choice plus challenge questions Success of this competency requires 80% (160 of 200 points)

**Network Attacks, Computer Crime and Hacking**

Enabled: Adaptive Release

To be awarded this competency level one must:

1. Successfully Completed Network Concepts
2. Successfully Completed Network Security Basics
3. Hacker Techniques, Tools and Incident Handling Virtual Lab Hands-on Competency Assignments
4. Tools.Technique Analytical Competency Assignments
5. Hacker Techniques & Tools Competency Assessment #1
6. Hacker Techniques & Tools Competency Assessment #2

**Lord Fairfax Community College (LFCC)**

173 Skirmisher Lane

Middletown, VA 22645-1745

LFCC.edu



This work was funded in part by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. This work was created by Lord Fairfax Community College (LFCC) and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability, or ownership.