COURSE INFORMATION

COURSE TITLE
CNG 133: Firewalls/Network Security

COURSE DESCRIPTION
Teaches students the basics of network firewall security. It covers basic installation techniques, discusses how to make an intelligent choice of firewall technology, and presents basic firewall troubleshooting.

CREDIT HOURS
3

CCCOnline Course Policies

The CCCOnline Course Policies page contains information about the student's role in the classroom, grading policies, and rights and responsibilities.
COURSE MATERIALS

Your textbook is available online as an eText. You do not need to purchase any additional materials. For specific information on refund policies and the optional black and white textbook available for purchase please contact the CCCOnline bookstore.

MINIMUM COMPUTER REQUIREMENTS

To complete this course, you will need regular access to a computer from which you can get to the internet and use email. In order to ensure that your course functions properly, you must run the System Check. This is a CRITICAL STEP, and taking the time to do it now will eliminate a tremendous amount of frustration for you later. To run the System Check, click Tools in the course NavBar and then click System Check.

REQUIRED eText

MAIN eText

The assigned readings introduce concepts and terminology necessary for effective participation in class discussions and completion of assignments, including the Practice Certification Exam at the end of the course.


DIGITAL MATERIALS ACCESS AND SETUP

This course uses uCertify digital content which contains the ebook and as well as interactive multimedia study tools, homework and labs (also named eText - you do not need to purchase it separately).

Visit the uCertify Course Start page for details on first access of the materials.

To make sure your computer is set up correctly to access the eText and other digital content, review the uCertify Technical Support page, also linked in the Technical Support Module.
COURSE COMPETENCIES AND OUTCOMES

STUDENT COMPETENCIES

The competencies you will demonstrate in this course are as follows:

A. Identify basic firewall installation techniques.
B. Establish how to make intelligent choices for firewall technology.
C. Define basic firewall troubleshooting.

The module outcomes that will permit you to demonstrate course competencies are:

MODULE 1

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Identify the network's top threats: security breaches, denial of service attacks, and malware.</td>
<td>B</td>
</tr>
<tr>
<td>2 Compare and contrast network protocols and communication equipment.</td>
<td>B</td>
</tr>
<tr>
<td>3 Identify Internet scams, crimes, and frauds.</td>
<td>B</td>
</tr>
</tbody>
</table>

MODULE 2

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Describe how denial of service (DoS) attacks work, such as SYN flood, Smurf, and DDoS.</td>
<td>B</td>
</tr>
<tr>
<td>2 Discover how viruses and Trojan horses operate and how they propagate.</td>
<td>B</td>
</tr>
<tr>
<td>3 Identify the basic methods and tools used by hackers.</td>
<td>B</td>
</tr>
</tbody>
</table>

MODULE 3

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Explain the methods and spyware used in industrial espionage.</td>
<td>B</td>
</tr>
<tr>
<td>2 Select appropriate cryptography for your organization.</td>
<td>B</td>
</tr>
<tr>
<td>3 Choose the best type of firewall for an organization.</td>
<td>A, B, C</td>
</tr>
</tbody>
</table>

MODULE 4

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Evaluate existing policies for network administration.</td>
<td>B</td>
</tr>
<tr>
<td>2 Evaluate potential security vulnerabilities.</td>
<td>B</td>
</tr>
<tr>
<td>3 Discuss the basics of cyber terrorism and information warfare.</td>
<td>B</td>
</tr>
</tbody>
</table>

MODULE 5

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Locate information as a cyber detective.</td>
<td>B, C</td>
</tr>
<tr>
<td>2 Apply basic computer forensics principles.</td>
<td>B, C</td>
</tr>
</tbody>
</table>
GRADING AND EVALUATION

METHODS
Evaluation includes a combination of discussion participation, assignments, and other evaluations. Rubrics are provided for assignments and discussions.

GRADING POLICIES
Mark all module due dates on your calendar for this class. You may submit assignments AHEAD of schedule. Late assignments will not be accepted without prior approval.

SUMMARY OF GRADING

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Points</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussions (10 @ 30 points each)</td>
<td>300</td>
<td>30%</td>
</tr>
<tr>
<td>Quizzes (14 @ 10 points each)</td>
<td>140</td>
<td>14%</td>
</tr>
<tr>
<td>Labs (11 chapters @ 25 points per chapter)</td>
<td>275</td>
<td>27.5%</td>
</tr>
<tr>
<td>Module 1 Cyberstalking Assignment</td>
<td>25</td>
<td>2.5%</td>
</tr>
<tr>
<td>Module 1 Cyberstalking Game Assignment</td>
<td>60</td>
<td>6%</td>
</tr>
<tr>
<td>uCertify Final Exam</td>
<td>200</td>
<td>20%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1000</td>
<td>100%</td>
</tr>
</tbody>
</table>

Grading Scale

A = 90 to 100%   B = 80 to 89%   C = 70 to 79%   D = 60 to 69%   F = 59% and below

DISCUSSIONS
For each discussion, write a main post that 1) discusses the topic and 2) offer examples that illustrate and support your discussion. Include a reference using APA style.

In each of your two replies, offer a suggestion, an example, or an analysis of the concepts they described. A discussion on cyber stalking includes your example and the steps you might take to prevent it.

Here is an example of an APA style reference:

ASSIGNMENTS

Module 1 features two assignments related to the lessons. The second assignment has several options, so read the instructions, complete the activity, write out your answers, and post them in the Assignments area.

LABS

Chapters 4-14 have one or more labs. Some of the labs are short activities that take 1-3 minutes to complete and others require more interaction. Complete all of your chapter labs to complete this activity. You must complete all of the labs in a chapter to receive a grade for the labs.

Click on Validate the submission in the Task box to record your score. You may retake labs to increase your understanding and the grade area reports your highest score.

QUIZZES

Complete each quiz question and click on validate your answer to record the response. At the end of a quiz, you may retake the quiz and the grade reflects your highest score.

uCertify Final Exam

uCertify includes a 100-question final exam in Module 5 to assess what you learned. The exam questions are similar to questions you might see on a certification exam.
COURSE SCHEDULE

The Schedule is subject to change as needed.

This page summarizes all of the graded assignments, discussions, quizzes, and reading assignments for the course. If you want, you can print it out and post it somewhere handy.

All assignments are described in detail on the Module Assignment pages. If you have questions check there and/or send me an e-mail.

**This course is not self-paced and is not open-exit.** All assignments, quizzes, discussions, etc., are to be completed by no later than 11:59 pm MST/MDT of the due date.

NOTE: Important CCCOnline semester dates (e.g., drop/withdraw(term end) appear on the [CCCOnline calendar](http://ccc Onlinecalendar).

### MODULE 1

<table>
<thead>
<tr>
<th>Reading/Assignments/Exams</th>
<th>Due Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read the Introduction and Chapter 1 in the uCertify eText:</td>
<td></td>
</tr>
<tr>
<td>Intro to Computer Security</td>
<td></td>
</tr>
<tr>
<td>View Flashcards for Chapter 1</td>
<td></td>
</tr>
<tr>
<td>Complete Chapter 1 Quiz</td>
<td></td>
</tr>
<tr>
<td>Participate in M1 Discussion 1: Introduce Yourself</td>
<td></td>
</tr>
<tr>
<td>Read Chapter 2 in the uCertify eText Networks and the Internet</td>
<td></td>
</tr>
<tr>
<td>Read M1 Exploration 1: Cyber Threats</td>
<td></td>
</tr>
<tr>
<td>View Flashcards for Chapter 2</td>
<td></td>
</tr>
<tr>
<td>Submit M1 Assignment 1: Cyberstalking Essay</td>
<td></td>
</tr>
<tr>
<td>Complete Chapter 2 Quiz</td>
<td></td>
</tr>
<tr>
<td>Participate in M1 Discussion 2: Cyber Threats</td>
<td></td>
</tr>
<tr>
<td>Read M1 Exploration 2: Case Study: Anonymous</td>
<td></td>
</tr>
<tr>
<td>Read Chapter 3 in the uCertify eText: Cyber Stalking, Fraud, and Abuse</td>
<td></td>
</tr>
<tr>
<td>View Flashcards for Chapter 3</td>
<td></td>
</tr>
<tr>
<td>Submit M1 Assignment 2: Cybersecurity Game</td>
<td></td>
</tr>
<tr>
<td>Complete Chapter 3 Quiz</td>
<td></td>
</tr>
</tbody>
</table>
MODULE 2

Reading/Assignments/Exams
Read Chapter 4 in the uCertify eText: Denial of Service Attacks
Read M2 Exploration 1: Green, White, Grey, and Black Hat Hackers
Read M2 Exploration 2: Ethical Hacking video
View Flashcards for Chapter 4
Complete Chapter 4 Labs
Complete Chapter 4 Quiz
Participate in M2 Discussion 1: Ethical Hacking
Read Chapter 5 in the uCertify eText: Malware
Read M2 Exploration 3: Social Engineering
View Flashcards for Chapter 5
Complete Chapter 5 Labs
Complete Chapter 5 Quiz
Participate in M2 Discussion 2: Ransomware
Read Chapter 6 in the uCertify eText: Techniques Used by Hackers
View Flashcards for Chapter 6
Complete Chapter 6 Labs
Complete Chapter 6 Quiz

MODULE 3

Reading/Assignments/Exams
Read Chapter 7 in the uCertify eText: Industrial Espionage in Cyberspace
Read M3 Exploration 1: Cryptology and Cryptanalysis
View Flashcards for Chapter 7
Complete Chapter 7 Quiz
Participate in M3 Discussion 1: Cryptography
Read Chapter 8 in the uCertify eText: Encryption
Read M3 Exploration 2: Steganography
View Flashcards for Chapter 8
Complete Chapter 8 Labs
Complete Chapter 8 Quiz
Participate in M3 Discussion 2: Steganography
Read Chapter 9 in the uCertify eText: Computer Security Technology
View Flashcards for Chapter 9
Complete Chapter 9 Labs
Complete Chapter 9 Quiz
MODULE 4

Reading/Assignments/Exams
Read Chapter 10 in the uCertify eText: Security Policies
Read M4 Exploration 1: Ransomware and Phishing
View Flashcards for Chapter 10
Complete Chapter 10 Labs
Complete Chapter 10 Quiz
Participate in M4 Discussion 1: Cyber Terrorism and Information Warfare
Read Chapter 11 in the uCertify eText: Network Scanning and Vulnerability Scanning
Read M4 Exploration 2: Blockchain, Identity and Cryptocurrencies
View Flashcards for Chapter 11
Complete Chapter 11 Labs
Complete Chapter 11 Quiz
Participate in M4 Discussion 2: Blockchain
Read Chapter 12 in the uCertify eText: Cyber Terrorism and Information Warfare
View Flashcards for Chapter 12
Complete Chapter 12 Quiz

MODULE 5

Reading/Assignments/Exams
Read Chapter 13 in the uCertify eText: Cyber Detective
Read M5 Exploration 1: Cyber Detection
View Flashcards for Chapter 13
Complete Chapter 13 Labs
Complete Chapter 13 Quiz
Participate in M5 Discussion 1: Cybersecurity and Cloud Computing
Read Chapter 14 in the uCertify eText: Introduction to Forensics
Read M5 Exploration 2: Future Directions
View Flashcards for Chapter 14
Complete Chapter 14 Labs
Complete Chapter 14 Quiz
Participate in M5 Discussion 2: Lessons Learned
Complete the uCertify Final Exam