

| | |
|------------------------|--|
| CLASS NUMBER AND NAME: | CSN323—Strategic Infrastructure Security |
| TOTAL HOURS/ UNITS: | 72 HOURS/5.0 UNITS |
| PREREQUISITES: | CSN313- Tactical Perimeter defense |
| TEXTS AND MATERIALS: | <i>Strategic Infrastructure Security</i> , Warren Peterson, Element K, 2007 (ISBN 9975112168) |
| CLASS DESCRIPTION: | A combination of lecture, lab exercises, and hands-on training introducing the student to the concepts and techniques of ethical hacking, Internet security, security policies, cryptography and the hardening of Linux and Microsoft operating systems. |
| CLASS OBJECTIVES: | To provide the student with an in-depth knowledge of securing Network Infrastructure. |
| CLASS FORMAT OVERVIEW: | <p>The class is conducted in lecture and instructor demonstrations, opportunity will be given for questions-and-answer discussion as well as tactile learning experiences.</p> <p>Time spent in preparation for or reflection on course lecture will approximate two hours outside of class for each lecture credit hour utilized by the instructor in delivery of the material and ¼ hour outside of class for each hour of structured lab time.</p> |
| METHOD OF INSTRUCTION: | Each topic will be discussed thoroughly and will be supplemented with written materials. Class work and homework will give the student experiential opportunities. |
| ATTENDANCE: | <p>It is expected that each student will be in class <u>when class begins.</u> Should the student arrive more than <u>five minutes late</u> they should notify the instructor of their presence, it will be up to the instructor to decide if the student has arrived in time to be counted as present- the instructor's decision is final.</p> <p>A minimum of 80 % attendance is required to complete this class. (Note: If a student misses more than this, he or she will not get a passing grade in this class!)It will be the student's responsibility to learn of any assignments given in class when absent.</p> |
| TESTING: | Weekly tests will be given each, with a module final exam on the last week of the module. |
| LATE TESTING: | A late test will result in a 10% penalty (Tests start with a B). All retakes and late tests must be scheduled with the instructor in a timely manner. |

GRADING POLICIES:

The grading system for this module consists of the following:

| | |
|--|-----|
| Attendance, participation, professional attitude | 10% |
| Homework | 25% |
| Weekly exams | 40% |
| End-of-module final | 25% |

**ANTICIPATED LEARNING
OUTCOMES:**

Upon completing this course, the student will be able to:

- 1.Cryptography
- 2.Hardening Linux
- 3.Hardening Windows 2003 Server
- 4.Ethical Hacking
- 5.Security on the internet and WWW
- 6.Analyzing Packet Signatures.
- 7.Performing Risk Analysis.
- 8.Creating a Security Policy

6 Week Tentative Schedule

CSN323

Week 1

Chapters 1 and 3
Homework due
Test

Week 2

Chapter 2
Homework due
Test

Week 3

Chapters 4
Homework due
Test

Week 4

Chapters 5 and 6
Homework due
Test

Week 5

Chapters 7
Homework due
Test

Week 6

Chapters 8
Homework due
Test

