Empire College
Business – Law – Technology – Medical

CLASS NUMBER AND NAME:	**CSN325—Security Plus**
TOTAL HOURS/ UNITS:	72 HOURS/5.0 UNITS
PREREQUISITES:	CSN205- Windows Server
TEXTS AND MATERIALS:	*CompTIA Security + Authorized Cert Guide* David L Prowse, Pearson, 2015 (ISBN 9780789753632)
CLASS DESCRIPTION:	This course is designed to be an introduction to Network Security concepts and practices.
CLASS OBJECTIVES:	To provide the student with a fundamental knowledge of Network Security and specifically the types of vulnerabilities that exist in Corporate Networks. Identify attacks, harden systems and create policy's.
CLASS FORMAT OVERVIEW:	This class is a combination of lecture and lab. 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.
METHOD OF INSTRUCTION:	As lecture and lab are the principal means of instruction, it will be expected that all students will be present every day to take part in class.
ATTENDANCE:	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. A minimum of 80 % attendance is required to complete this class. (Note: 80% is 5 days. 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. .
TESTING:	Weekly tests will be given week, with a module final exam on the last Thursday 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	30%
Project	10%
End-of-module final	25%

ANTICIPATED LEARNING OUTCOMES:

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

1.Define and Identify the three A's

2.Identify the different types of Network attacks.

3.Learn the general vulnerabilities in LAN's, WAN's, E-Mail, Web, and FTP services.

4.Explain the major deficiency in the 802.11B Encryption Protocol.

5.Identify the various types of Network Infrastructure devices and services and their vulnerabilities.

6.Explain the different Firewall technologies.

7.Understand what a "honeypot" and "honeynet" are used for. Explain the different types of Intrusion Detection Systems.

8.Harden systems and services in most Corporate Networks.

9.Explain Public Key Infrastructure. Know the difference between symmetric and asymmetric encryption.

10.Create a strong incident response plan. Understand the basics of computer forensics.

11.Create policy's for Security and Disaster Recovery. Explain the necessity for an Acceptable Use Policy.

12.Plan and set up an Audit Policy, including account management auditing and privilege use auditing.

6 Week Tentative Schedule

Week 1
Chapters 1, 2 and 3
Homework due
Presentation Topics due
Test

Week 2
Chapters 4, 5, and 6
Homework due
Test

Week 3
Chapters 7, 8, and 9
Homework due
Test

Week 4
Chapters 10, 11, and 12
Homework due
Test

Week 5
Chapters 13 and 14
Projects Due
Homework due
Test

Week 6
Chapters 15 and 16
Final/Homework Due