

CLASS NUMBER AND NAME: CSN342- Ethical Hacking II

TOTAL HOURS/ UNITS: 72 HOURS/5.0 UNITS

PREREQUISITES: CSN332—Ethical Hacking 1

TEXTS AND MATERIALS: *CompTIA Pentest + Certification Guide*, First Edition, Omar Santos, Ron Taylor ,Pearson Education, 2018 (ISBN 9780789760357)

CLASS DESCRIPTION: A combination of lecture, lab exercises, and hands-on training introducing the student to the concepts and techniques of ethical hacking. Students will use a wide variety of tools to perform hacking on Web Servers and applications, databases and wireless networks. Students will implement various types firewalls and intrusion detection systems as well as have knowledge of cryptography and cryptographic attacks

CLASS OBJECTIVES: To provide the student with an in-depth knowledge and implementation of hacking techniques to prepare for the Certified Ethical Hacker certification.

CLASS FORMAT OVERVIEW: The class is conducted in lecture and instructor demonstrations, opportunity will be given for questions-and-answer discussion as well as tactile learning experiences.

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: Each topic will be discussed thoroughly and will be supplemented with written materials. Class work and homework will give the student experiential opportunities.

ATTENDANCE:

It is expected that each student will be in class when class begins. Should the student arrive more than five minutes late 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: 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 each week, 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. Perform hacking on web servers, web applications and databases.
2. Perform hacking on wireless networks and mobile devices.
3. Implement firewalls, intrusion detection systems and honeypots.
4. Identify types of physical security measures and their vulnerabilities.
5. Identify cryptographic attacks and their defenses.
6. Identify security techniques for cloud computing and botnets.

Week 3

Chapters 9
Homework due, review,
Test

Week 4

Chapters 10
Homework due, review,
Test

Week 5

Chapters 11
Homework due, review,
Test

Week 6

Chapters 12 and 13
Homework due, review,
Test

6 Week Tentative Schedule

CSN342

Week 1

Chapter 7
Homework due, review,
Test

Week 2

Chapter 8
Homework due, review,
Test

