CTC 495 – Network Security through Penetration Testing
Fall 2016

Instructor	G. Poppe	**E-Mail**	gpoppe@csudh.edu
Classroom	SCC-800	**Class Time**	MoWed 2:30pm-3:45pm
Office	Lib-5717	**Office Hours**	Wed 10:15pm-11:15pm
Phone	(310) 243-3398	**URL**	http://csc.csudh.edu

CATALOG DESCRIPTION:

This course teaches students through lectures, discussions, demonstrations, and classroom labs. Students learn the knowledge, skills, and abilities necessary to identify and fix network vulnerabilities through the use of penetration testing techniques. This course is intended for people interest in network security.

PRE-REQUISITES

None

TEXTBOOK

OWASP Testing Guide v4 by The OWASP Testing Project. Students can download the book, or use the free eBook provided by professor. Students with accessibility issues are asked to use the free eBook.

REFERENCE*:*

TBA

COURSE GOALS:

The primary objective of this course is to teach students to determine the feasibility of a particular set of attack vectors, identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence, and identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software. The course presents the process in developing enterprise level network security skills using existing tools, techniques, and programming languages.

SPECIFIC INSTRUCTIONAL GOALS:

The purpose of the course is to provide the student with the knowledge to pass the certified penetration tester examination through a semester long project.

COURSE OUTCOMES:

Upon completion of this course, students will be able to:

- Identify Potential drawbacks of penetration testing
- Understand announced versus unannounced testing
- Patch application-level holes and defenses
- Enumerate NT systems to expose security holes
- Create policies to prevent social engineering methods
- Utilize port scanners and discovery tools
- Utilize web testing tools
- Configure firewalls and intrusion detection systems
- Understand the difference between “white hat” and “black hat”
- Understand penetration testing methodologies
- Prevent network protocol attacks
- Perform network reconnaissance
- Identify vulnerabilities
- Patch windows exploits
- Patch Unix/Linux exploits

- Understand covert channels & rootkits
- Prevent wireless security flaws
- Identify web application vulnerabilities

ATTENDANCE:

Students are expected and encouraged to attend lectures and contribute to discussions. It is the student's responsibility to contact the instructor as early as possible if he/she cannot attend class. There will be no make-up opportunities, although all classes will have companion videos available on line.
The student is responsible for materials missed during an absence, whether excused or not. Classes will start at the prescribed time and will end at the prescribed time. Instructor will be available during the posted office hours and you may make an appointment for times not posted.

GRADING BREAKDOWN:

Homework/quiz	35%
Midterm Exam	25%
Final Exam	40%
	100%

Evaluation criteria explained:

- Students are expected to be active participants in each class meeting. Full credit for participation will be extended to students who regularly ask questions, share observations, and contribute relevant personal experiences.
- The mid-term examination will consist of objective questions and will require a technological comprehension that covers the lecture material and assigned readings.
  The assignments will consist of a number of individual in class and homework tasks.

Students will be given specific guidance on the amount of collaboration permitted for each assignment. Unless otherwise specified, all assignments are individual assignments, and thus must be completely the original work of the student submitting them and include proper citations to the published work of others.

Quizzes:

Quizzes may be given throughout the semester, at a rate of approximately 1 per chapter. Quizzes will always cover the material covered since the last Quiz or Exam. The quizzes will be combinations of objective and short-answer questions. Quizzes will be administered online via Blackboard. Makeup quizzes will not be given. However, the lowest quiz grade will be dropped. Any class material missed by the student is the student's responsibility to acquire.

GRADING SCALE:

96-100 = A	90-95 = A-	87-89 = B+	83-86 = B	80-82= B-	
77-79= C+	73-76= C	70-72= C-	67-6 = D+	63-66= D	below 60 = F

GENERAL POLICIES:

ACADEMIC HONOR CODE

Programming assignments must be done individually. Failure to do so will result in a violation of the CSUDH Academic Honor Code. The following cases will be considered as violations: identical code, and extremely similar code. Violations will be reported to the Office of Vice President of Academic Affairs. Disciplinary action will be taken against any student who alone or with others engages in any act of academic fraud or deceit (Read University Regulations in University Catalog). It is the student's responsibility to ensure they fully understand to what extent they may collaborate or discuss content with other students. No exam work may be performed with the assistance of others or outside material unless specifically instructed as permissible. If an exam or assignment is designated "no outside assistance" this includes, but is not limited to, peers, books, publications, the Internet and the WWW. If a student is instructed to provide citations for sources, proper use of citation support is expected.

ATTENDANCE POLICY

Excessive absences will result in lowered grades. Excessive absenteeism, whether excused or unexcused, may result in a student's course grade being reduced or in assignment of a grade of "F". Absences are accumulated beginning with the first day of class.

STUDENT ACADEMIC APPEALS PROCESS

Authority and responsibility for assigning grades to students' rests with the faculty. However, in those instances where students believe that miscommunication, error, or unfairness of any kind may have adversely affected the instructor's assessment of their academic performance, the student has a right to appeal by the procedure listed in the Undergraduate Catalog and by doing so within thirty days of receiving the grade or experiencing any other problematic academic event that prompted the complaint.

ADA STATEMENT

Students with disabilities, who believe they may need an academic adjustment in this class, are encouraged to contact me as soon as possible to better ensure receipt of timely adjustments.

COURSE OUTLINE

Week	Assignments	Topic
1		Overview and introduction to the ethics of penetration testing
2		Introduction to UNIX/Linux
3		Network addressing and internet protocol
	Homework 1/Quiz	
4		Enumeration using nmap
5		Identifying services and operating systems
6		Operating system vulnerability research
	Homework 2 /Quiz	
7		Metasploit and Armitage
8		Encryption, hashes, and rainbow tables
	Midterm Exam	
9		Windows tools
10		Web application security testing
11		Identity management, Authentication, and Authorizing testing
	Homework 3/Quiz	
12		Session management, input validation, and error handling testing
13		Business logic and client side testing
14		Reporting and documentation
	Homework 4/Quiz	
15		Policy creation
16		CPT test preparation
	Final Exam	