Note:

Course content may be changed, term to term, without notice. The information below is provided as a guide for course selection and is not binding in any form, and should <u>not</u> be used to purchase course materials.

COURSE SYLLABUS

CSCI 632

ETHICAL HACKING

COURSE DESCRIPTION

This course goes into the how and why of ethical hacking, and how it is used to strengthen security of systems, including issues in penetration testing, such as physical security and social engineering.

RATIONALE

The Ethical Hacking course introduces the student to the methods and techniques used by computer hackers and penetration testers from a real-world perspective. The objective of this course is to provide the student with an understanding of offensive security, with an emphasis on practical exposure to hacking via hands-on assignments, in order to prepare him/her to better defend against cyber attacks in live systems.

I.   PREREQUISITE

For information regarding prerequisites for this course, please refer to the Academic Course Catalog.

II.   REQUIRED RESOURCE PURCHASE

Click on the following link to view the required resource(s) for the term in which you are registered: http://bookstore.mbsdirect.net/liberty.htm

III.   ADDITIONAL MATERIALS FOR LEARNING

A.   Computer with basic audio/video output equipment

B.   Internet access (broadband recommended)

C.   Microsoft Office

IV.   MEASURABLE LEARNING OUTCOMES

Upon successful completion of this course, the student will be able to:

A.   Know the ethical issues regarding professional ethical hacking and penetration testing.

B.   Use the tools available for crafting exploits.

C.   Understand the basic techniques for gaining unauthorized access into a large network and computer system, using both technical and non-technical means.

D.   Be able to assess potential vulnerabilities in a network security system within executable programs or within network protocols.

E.   Intregrate biblical principles within the field of computer security.

V.   COURSE REQUIREMENTS AND ASSIGNMENTS

A.   Textbook readings and lecture presentations

B.   Course Requirements Checklist

After reading the Course Syllabus and Student Expectations, the student will complete the related checklist found in Module/Week 1.

C.   Discussion Board Forums (3)

Discussion boards are a collaborative learning experience. Therefore, the student is required to create an thread in response to the provided topic for each forum. Each thread must be 500 words and demonstrate course-related knowledge. The student must integrate relevant biblical principles into the thread. In addition to the thread, the student is required to reply to 2 other classmates' threads. Each reply must be 250 words.

D.   Labs (8)

The student will complete labs associated with the course material. Each lab will have specific instructions for tasks, along with deliverables, to be completed in the virtual lab environment.

E.   Projects (2)
The student will complete 2 projects using the provided Vulnerability Assessment Report and Penetration Test Report templates. The content for the report will be gathered from the completed Labs. Each project must include at least 2 references in addition to the class textbook.

F.   Quizzes (8)

Each quiz will cover the Reading & Study material for the modules/weeks in which it is assigned and will include questions that may require independent research. Each quiz will be open-book/open-notes, contain 4 multiple-choice questions, and have a 1-hour time limit.

VI.   COURSE GRADING AND POLICIES

A.   Points

Course Requirements Checklist	10
Discussion Board Forums (3 at 50 pts ea)	150
Labs (8 at 50 pts ea)	400
Project 1	140
Project 2	150
Quizzes (8 at 20 pts ea)	160
Total	1010

B.   Scale

     A = 940–1010   A- = 920–939   B+ = 900–919   B = 860–899   B- = 840–859

     C+ = 820–839   C = 780–819   C- = 760–779   F = 0–759

C.   Disability Assistance

     Students with a documented disability may contact Liberty University Online's Office of Disability Academic Support (ODAS) at LUOODAS@liberty.edu to make arrangements for academic accommodations. Further information can be found at www.liberty.edu/disabilitysupport.

COURSE SCHEDULE

CSCI 632

MODULE/WEEK	READING & STUDY	ASSIGNMENTS	POINTS
1	Walker: Introduction, ch. 1 2 presentations Lab 1 Worksheet 2 websites	Course Requirements Checklist Class Introductions Lab 1: Introduction to the Lab Environment Quiz 1	10 0 50 20
2	Walker: ch. 2 2 presentations Lab 2 Worksheet 1 website	Lab 2: Passive Reconnaissance Quiz 2	50 20
3	Walker: ch. 3 1 presentation Lab 3 Worksheet	DB Forum 1 Lab 3: Scanning and Enumeration Quiz 3	50 50 20
4	Walker: ch. 5 1 presentation Lab 4 Worksheet 4 websites	DB Forum 2 Lab 4: Linux/OSX Exploitation Project 1 – Vulnerability Assessment Report Quiz 4	50 50 140 20
5	Walker: ch. 12 1 presentation Lab 5 Worksheet	Lab 5: Windows Exploitation Quiz 5	50 20
6	Walker: pp. 380–394 ("Mobile Based Attacks") 1 presentation Lab 6 Worksheet 1 website	DB Forum 3 Lab 6: Client-side Exploitation with Social Engineering Quiz 6	50 50 20
7	5 presentations Lab 7 Worksheet 1 website	Lab 7: Evasive Maneuvers and Post Exploitation Quiz 7	50 20
8	Walker: ch. 7, pp. 394–399 ("Death of the Password") 4 presentations Lab 8 Worksheet 2 websites	Lab 8: Physical Security Project 2 – Penetration Test Report Quiz 8	50 150 20
		TOTAL	1010

DB = Discussion Board

NOTE: Each course module/week begins on Monday morning at 12:00 a.m. (ET) and ends on Sunday night at 11:59 p.m. (ET). The final module/week ends at 11:59 p.m. (ET) on **Friday**.