Date of last update 3/23/2017

ETHICAL HACKING

CIS 102 (CRN: 43529) – Hybrid Course
Spring, 2017

*Online class with **two on-campus meetings from 6:00- 7:50PM on 4/13/2017 and 6/29/2017 in ATC203***

Office hours: via Internet video, via e-mail & in person (see below for details)

COURSE DESCRIPTION

This is a "synchronous" online course in which you will be given weekly laboratory assignments and quizzes to complete. **You may work more quickly than the schedule that is specified for this course, but will not receive credit if you more slowly than the schedule.** Students will scan, test, hack and secure systems. Implement perimeter defenses, scan and attack virtual networks. Other topics include intrusion detection, social engineering, "footprinting", DDoS attacks, buffer overflows, SQL injection, privilege escalation, trojans, backdoors and wireless hacking. Legal restrictions and ethical guidelines emphasized. This course also helps prepare students to pass the Certified Ethical Hacker (C|EH) exam.

PREREQUISITE SKILLS

Advisory: Computer Information Systems 66 and CIS 108.

INSTRUCTOR INFORMATION:

Instructor: Leonard (Len) Fisk

Office Hours:

in person at ATC 203b on the De Anza campus from **3:00-3:50 PM** on 4/13/2017 and 6/29/2017.

via web video: from 4:00 to 6:00 every Thursday from 4/20/2017 through 6/22/2017 on CCCConfer as follows:

The **cccconfer.org** website is a videoconferencing site and you need a computer with microphone and speakers, plus, if you wish, a webcam. Or, you can use an iPhone, iPad, or Android device if you download the mobile app "Blackboard Collaborate."

cccconfer office hours: Go to cccconfer.org and select the "**Office Hours / Student**" button, then scroll to find the entry for "Len Fisk Office Hour". Then hit the "**GO**" button. Or, simply use this link: : http://cccconfer.org/GoToMeeting?SeriesID=61e8e505-60b0-419b-aff6-79ad5b9c4c0b. The participant passcode is **198591**. I will be using a webcam and encourage you to do so also, but there is no requirement that you use video (there is a text box). If you do not have Internet capability, you can always call 888-886-3951 to participate by voice.

via e-mail: I can be reached virtually any time via e-mail (see below for address). **Please send e-mail only to the address shown, and use CIS102 in the subject line to ensure that I will get the mail in a timely manner.**

E-mail address: **mailto:fisklen@fhda.edu**

Website: I will post up-to-date information regarding this course at Jones & Bartlett's site for this course. In particular, I will post updates and changes to this syllabus at that site which, like the campus "Catalyst" system, is Moodle-based. You will be accessing this site via https://www.jblcourses.com/ . Various other links and materials will be added at this class site, your completed assignments will be uploaded to it as well, and all quizzes and tests will be via this site. It will be the center point for communications about the course. Effectively, the fee for a "textbook" will also include the fee for access to this site.

ATTENDANCE POLICY

We will meet for the first class meeting on April 13 at 6:00 PM, in ATC 203. Students are required to attend the final class meeting to take the final in AT 203 on Thursday, June 29, 2017, 6:00-7:50 PM.

Drop Policy: By **midnight**, **Wednesday of THE SECOND WEEK OF THE COURSE (4/19/2017)** you must have purchased the text and site access and have registered on the Jones and Bartlett Moodle site that supports the class. (See below for textbook and site access purchase information.) **By midnight on Friday of the second week (4/21/2017), you will also have completed and turned in (to J&B Moodle) the Week 1 Lab assignment posted on the website** (we will ignore the "challenge" assignments). (This due day is two days later than I will expect for all remaining Lab assignments, which will be due at midnight on Wednesday of each week**.) Failure to do so may result in a DROP.**

Students who wish to drop this class must follow the De Anza College drop procedures. The Drop calendar deadlines can be found at https://www.deanza.edu/calendar. Do not assume you will be automatically dropped from this course. If you intend to drop the course, you must drop yourself!

OBJECTIVES

Upon completion of this course, you will be able to use a personal computer and understand the following personal computer objectives.

1. Explore ethical hacking basics
2. Explore cryptography
3. Investigate reconnaissance: Information gathering for the ethical hacker
4. Explore scanning and enumeration
5. Explore hacking through the network: Sniffers and evasion
6. Investigate how to attack a computer system
7. Explore low tech hacking techniques
8. Investigate web-based hacking
9. Explore wireless network hacking
10. Investigate trojans and other attacks
11. Perform penetration testing

STUDENT LEARNING OUTCOMES FOR THIS COURSE:

Demonstrate the ability to attack and defend systems and networks.

REQUIRED COURSE MATERIALS

Textbook: Hacker Techniques, Tools, and Incident Handling, Second Edition, with special virtual lab access, by Sean-Philip Oriyano.

Purchasing text and lab materials: You can purchase access to the Moodle page and virtual labs required for the course in person or via the web, at the De Anza bookstore, where it will be bundled with either a "hard" or "e-copy" of the textbook. If you would prefer a hard-copy version of the textbook, the bookstore will have a number of copies for purchase. Please note that access to the virtual lab is unique for each person and cannot be shared: i.e., the code you purchase will belong to you and to you alone.

The bookstore will sell you a packet with either

- **e-book**:
  Hacker Techniques, Tools, and Incident Handling Edition 2, plus lab access**,** or
- **hard copy text**:
  Hacker Techniques, Tools, and Incident Handling Edition 2, plus lab access, or
- **lab access only, with no text** (assuming you already have a copy of the 2nd Edition of the text):
  (this option is NOT recommended unless you already own a copy of the text).

Any of these three options will provide you with the access code you need for individual access to the Jones & Bartlett virtual lab site (plus the e-book if you have chosen that option). **Please note that the specific code needed to access the virtual laboratory MUST be purchased, otherwise you cannot participate in the class.**

To redeem your access code to the JBL Virtual Security Cloud Lab, do the following:

1. Go to www.jblcourses.com (NOT moodle.jblcourses.com)
2. Click on "**Redeem an Access Code**" on upper right side of screen
3. Enter the **8 digit** lab access code you purchased and the **four digit** code for this specific section of the class - **5751**. Then click **Submit**.
4. Once your access code has been validated, click on the blue **New User Sign Up** link underneath the yellow submit button. You must do the new user "sign-up" before you can enter a username and password.
5. In the **New User** Box type in
   a. **Username** - must contain alphabetical letters, numbers, a hyphen, underscore, period, or @ sign (DON'T FORGET THIS, AS IT IS NECESSARY FOR YOU TO GET INTO THE LAB!).
   b. **Password** – must contain at least 8 characters, and include one digit, one lower case letter, one upper case letter, and one non-alphanumeric symbol such as"#". For instance, ABCabc1# sign (AGAIN, DON'T FORGET THIS, AS IT IS NECESSARY FOR YOU TO GET INTO THE LAB!).
   c. **First Name/Last Name** in appropriate box (please use the name you used to enroll in the class at De Anza, otherwise I cannot give you credit)
   d. **Email**
   e. Click **submit**
   f. You have successfully entered a link to your course on the next screen.
   g. Click on the course name to enter the course.

If your code doesn't work or you are unable register please contact our tech support specific for the virtual labs and lecture presentations at 1-866-601-4525 or www.jblcourses.com/techsupport.

J&B Moodle and Virtual Lab Site: As noted above, the J&B site will be used for completing all class assignments. The J&B site also provides an interesting feature that allows you to create discussion forums and to reach other students to form study groups, etc., as well as a chat-room to use in addition to regular e-mail. I am available at most times during the week via regular e-mail (I have my iPhone nearby at almost all times).

REQUIRED COMPUTER COMPONENTS AND AVAILABILITY

You will need a **broadband Internet connection** (not dial up!) if you wish to work at home.

Hardware Requirements: A PC computer is required to run the Jones and Bartlett software to access the labs for this course. If you do not own a PC, you may use the De Anza lab computers in ATC 203. In addition, some students may wish to install some of the tools that are installed in the Jones & Bartlett virtual environment on their own machines, although this is not required. (Extra-credit will be available for installing and demonstrating such software, although you will be encouraged to exercise great caution in using it. Setting up a virtual environment like the lab, in which both the hacking machine and the targets are virtual, is a very safe way to do it; it spares you the risk of being blacklisted by ISPs.)

Software: (1) You will need a **Firefox** web browser (preferably) to access the Moodle and virtual laboratory sites. The Jones and Bartlett access codes will allow access to the Jones & Bartlett virtual environment that accompanies the Hacker Techniques, Tools, and Incident Handling e-book, and all of the software used will be located on their servers. One exception is the necessary installation of the (free) **Citrix ICA Client**, which you will be prompted to do when you first access the virtual lab from the J&B Moodle site. (2) You will also need Microsoft **PowerPoint**, or a free MS PowerPoint Reader (download from https://www.microsoft.com/en-us/download/details.aspx?id=13). (3) To post Extra Credit assignments, and to post your weekly laboratory assignments, you will need both MS **Word** and **PowerPoint**, or a tool that produces output compatible with Word and PowerPoint (.DOC AND .PPT), like Apache Open Office.

Computers in the De Anza Labs: If you do not have a broadband-connected computer with the proper software, you can use our CIS lab computers. For CIS computer lab hours, see **http://www.deanza.edu/buscs/lab/hours.html**. (Please note that the ATC lab computers are not equipped with speakers, so you will need to provide headphones if you plan to listen to the lectures there.)

WAYS TO EARN POINTS TOWARD A GRADE

This course will require weekly, hands-on lab assignments in which you will be working to either hack or defend a virtual system. You will take 10 quizzes and a final exam. Finally, in addition to these graded activities, you have an opportunity to earn additional "extra credit" points by researching and presenting additional information about tools, hacks, and security issues in the press and on the web to the class. The **m**aximum possible points are summarized in the table shown below.

Source	number	points	total
Laboratory assignments	10	10	100
Unit Quizzes	10	10	100
Final	1	100	100
Extra Credit	5	10	50
Total points possible (300 w/o Extra Credit):			350

SUBMITTING WEEKLY LABORATORY ASSIGNMENTS

This course uses a virtual hacking environment ("sandbox") provided by Jones and Bartlett to accompany the Hacker Techniques, Tools, and Incident Handling textbook, and all of the labs will require access to this environment. All course information, including assignments, course deadlines, etc. will be made available to you online via the Jones and Bartlett course web site. When you enter the Jones and Bartlett online course site, you will find the assignments that you will be asked to complete, listed within each class week of the quarter. The actual course schedule and due dates for exams and assignments are subject to change and will be posted in the schedule in this course syllabus on the J&B Moodle site. Each week's lab assignment will entail using the virtual environment and doing multiple screen captures, which you will use to document your actions there. You will then paste the captured screen images into your narrative, answering the questions and describing what you did, and post the resulting MS Word document (or other .DOC format document) to satisfy the assignment at the class Moodle site.

Each Lab will have both a "due date" and a "drop dead" date associated with it. The "drop dead" date represents the date beyond which no labs will be accepted for scoring. Your job is simply to stay ahead of the "due dates" (and most importantly, the "drop dead" dates). Similarly, your completion of the Lab by uploading the report document will trigger the opportunity to take the unit quiz and the assure the availability of materials in the subsequent units. You will have the opportunity to amend your Lab Report after you uploaded your initial version and before the "drop dead" date.

Late Work

Lab reports will be accepted up to five days after the after the official due date according to the following rules: Ten percent (10%) of the maximum possible points will be subtracted for each working day (24 hours) the assignment is late. This will continue until 5 days have elapsed, when the points total will drop to zero, and no credit will be earned. If you have clear and compelling reasons for not getting an assignment in on time, please let me know on or **before the day it is due**, and I will arrange an extension for you. Quizzes must be completed before the date specified in Moodle, and cannot be taken beyond the deadline. Please note that there are dependencies among Lab Reports and Quizzes: the former being required as pre-requisites to the latter.

Extra Credit Assignments:

Various extra credit assignments will be posted via the J&B site, and will be on topics that you choose and seek approval for before doing. Like the other assigned work, it will be turned in via the Jones & Bartlett site. Unlike lab work, **extra credit work will be prepared as a PowerPoint, with an audio recording of your voice presentation, which I will post for the full class to access**. (Even older versions of PowerPoint permit the recording of your voice for presentation: all you need is a laptop with a built-in microphone, or an external microphone with either USB or audio jack.) You will upload a PowerPoint presentation that has been augmented with your own voice recording, explaining each slide in no more than 10-minutes time for the full

presentation. **Extra credit work will be posted on topics that are truly substantive and that target specific security issues pertinent to this course.** All extra credits will involve:

(1) The demonstration of, and/or installation of, and/or use of, and/or analysis of, major tools used in hacking (like Wireshark, Metasploit, Kalli Linux, etc.), or
(2) The analysis and demonstration of the accomplishment of significant tasks on sites such as hackthissite.org or enigmagroup.org/ (e.g., accomplishment of two "realistic" hacks on HackThisSite), or
(3) The reporting and technical analysis of major events and issues in the digital security realm (e.g., analysis of a major new exploit),

Any extra credit work involving the installation and analysis of tools, and accomplishments at the aforementioned websites **will require the prior approval of Professor Fisk** and will be posted to the Moodle site in order to earn extra credit points. (If it is accepted for credit, Dr. Fisk will make your report available to the full class.)

Your Extra Credit must be submitted in the form of a single, stand-along document that will be both interesting and instructive and can be posted in a format that is readable by all students in the class (i.e., PDF, .DOC, or .PPT). It is subject to the same <1 MB constraint that you have for your Labs. I will accept only the first eight approved Extra Credit submission per week (first come-first served), and you cannot submit any more than one per week. Weeks begin at midnight on Sunday night. Week 1 begins on Midnight September 20.

The Sequence of Events for Finishing Each Unit of the Curriculum:

Initially, you will find that the Moodle page looks rather empty. The reason is that the successive portions of the course only become visible and available to you as you finish each unit/week in the sequence. There will be 10 units associated with specific chapters in the text and specific Laboratory exercises, as shown in the table below:

Unit Sequence Table:

Unit/Week	"Drop-Dead" Dates	Lecture / LabTopic	Reading
Unit 1/ Wk. 1	Unit Lab and Quiz done by midnight 4/21 & 4/25, respectively	**Intro, syllabus, hacking & OSI/TCP-IP / Assessing & Securing Systems on a WAN**	**Chpt 1&2**
Unit 2/ Wk. 2	Unit Lab and Quiz done by midnight 4/26 & 5/2, respectively	**Cryptography, symmetric, asymmetric / Applying Encryption & Hashing Algorithms for Secure Communications**	**Chpt 3**
Unit 3/ Wk. 3	Unit Lab and Quiz done by midnight 5/3 & 5/9, respectively	**Footprinting and social engineering / Data Gathering and Footprinting on a Targeted Website**	**Chpt 5&13**
Unit 4/ Wk. 4	Unit Lab and Quiz done by midnight 5/10 & 5/16, respectively	**Port scanning, enumeration & syst. Hacking / Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation**	**Chpt 6&7**
Unit 5/ Wk. 5	Unit Lab and Quiz done by midnight 5/17 & 5/23, respectively	**Web & database attacks / Attacking a Vulnerable Web Application and Database**	**Chpt 9**
Unit 6/ Wk. 6	Unit Lab and Quiz done by midnight 5/24 & 5/30, respectively	**Malware, worms & viruses / Identifying and Removing Malware on a Windows System**	**Chpt 10**
Unit 7/ Wk. 7	Unit Lab and Quiz done by midnight 5/31 & 6/6, respectively	**Network analysis, Linux & pen testing / Analyzing Network Traffic to Create a Baseline Definition**	**Chpt 11&12**
Unit 8/ Wk. 8	Unit Lab and Quiz done by midnight 6/7 & 6/13, respectively	**Wireless vulnerabilities / Auditing a Wireless Network and Planning for a Secure WLAN Implementation**	**Chpt 8**
Unit 9/ Wk. 9	Unit Lab and Quiz done by midnight 6/14 & 6/20, respectively	**Physical Security, Incident Response / Investigating and Responding to Security Incidents**	**Chpt 4 & 14**
Unit 10/ Wk. 10	Unit Lab and Quiz done by midnight 6/21 & 6/27, respectively	**Defensive Technologies / Securing the Network with an Intrusion Detection System (IDS)**	**Chpt. 15**
Wk. 12	**6/29**	**FINAL - (120 min) 6:15-8:05 PM, 6/29, ATC 203)**	**All Chapters**

For each unit, the materials must be accessed and completed in the required order, and must be completed before the listed "drop-dead" date. The Laboratory for any specific unit/week must be completed before the

unit/week mastery quiz appears on Moodle and you are allowed to take it. (The grading of each of the labs may take several workdays before a score is posted.)

Practice quizzes have been provided (these are T/F questions) with each unit to help you determine if you are ready to take the unit quiz. You can take practice quizzes as often as you wish, and your scores on these will not be used in your grading.

You will be permitted to take each Unit/Week quiz only once. Once you complete the quiz, you will be allowed to continue to the next unit immediately. Again, please note that you will get only one try at the unit quiz.

The Lab report of the first unit must be completed (and uploaded) before midnight, Friday 4/21 in order for you to remain in the class.

In general, the sequence you should follow for each unit is as follows:

1. Read the chapter(s) for the unit and watch the lecture, with audio narrative for the unit;
2. **Do the virtual lab for the unit and post the lab report to Moodle as a single DOC (MS Word format) document**;
3. Take the "self-test" practice quiz for the unit (it is scored, but will not count toward your grade);
4. **Take the unit quiz for the unit after the lab report is uploaded**. ***Until the Lab report is uploaded for that unit, the unit quiz will remain hidden.***

The **bold-faced** items on the numbered list above are the only items that must be done in sequence, and the only activities you are required to do to receive a grade. As you complete each unit quiz, the next two units/weeks will be made visible on the Jones and Bartlett Moodle page for you.

TESTING/GRADING POLICIES/FINAL GRADES

To pass this course, it is recommended that you complete ALL assignments plus ALL Exams with the minimum scores shown below**.** Weekly deadlines for all assignment will be posted via Catalyst.

Exam Grading Scale:

A+	96%-100%
A	93% -95%
A-	90%-92%
B+	87%-89%
B	83%-86%
B-	80%-82%
C+	77%-79%
C	70%-76%
D+	67%-69%
D	63%-66%
F	0%-62%

Final Grade Mix:

The following percentages reflect how the final grade will be determined:

Lab Assignments		33.3%
Quizzes		33.3%
Final Exam		33.3%
Extra Credit		16.7%
		=====
Total	=	116.7%

ACADEMIC INTEGRITY:

Students who submit work of others as their own or cheat on exams or other assignments will receive a failing grade in the course and will be reported to college authorities.

Note to students with disabilities

If you have a disability-related need for reasonable academic accommodations or services in this course, provide your instructor with a Test Accommodation Verification Form (also known as a TAV form) from Disability Support Services (DSS) or the Educational Diagnostic Center (EDC). Students are expected to give a five-day notice of the need for accommodations. Students with disabilities can obtain a TAV form from their DSS counselor (864-8753 DSS main number) or EDC advisor (864-8839 EDC main number).

TECHNICAL DIFFICULTIES

If you have technical problems with the Jones and Bartlett virtual laboratory, please contact Jones and Bartlett Technical Support directly at msupport@jblearning.com or, if the problem stems from a client software glitch in your personal computer, complete your course work using the computers in the CIS lab.

SCHEDULE/CALENDAR

Wk	Date	Topic	News/Extra Credit	Reading	Test (1)/ Quiz (10)	Due
1	4/9-4/15/2017	Intro, syllabus, hacking & OSI-TCP/IP	No	Chpt 1&2		
2	4/16-4/22/2017	Cryptography, symmetric, asymmetric	Yes	Chpt 3	Quiz 1	Lab 1, midnight 4/21/2017
3	4/23-4/29/2017	Footprinting and social engineering	Yes	Chpt 5&13	Quiz 2	Lab 2, midnight 4/26/2017
4	4/30-5/6/2017	Port scanning, enumeration & syst. Hacking	Yes	Chpt 6&7	Quiz 3	Lab 3, midnight 5/3/2017
5	5/7-5/13/2017	Web & database attacks	Yes	Chpt 9	Quiz 4	Lab 4, midnight 5/10/2017
6	5/14-5/20/2017	Malware, worms & viruses	Yes	Chpt 10	Quiz 5	Lab 5, midnight 5/17/2017
7	5/21-5/27/2017	Network analysis, Linux & pen testing	Yes	Chpt 11&12	Quiz 6	Lab 6, midnight 5/24/2017
8	5/28-6/3/2017	Wireless vulnerabilities	Yes	Chpt 8	Quiz 7	Lab 7, midnight 5/31/2017
9	6/4-6/10/2017	Physical Security, Incident Response	Yes	Chpt 4 & 14	Quiz 8	Lab 8, midnight 6/7/2017
10	6/11-6/17/2017	Defensive Technologies, and Incident Response –	Yes	Chpt. 15	Quiz 9	Lab 9, midnight 6/14/2017
11	6/18-6/24/2017	Study for final	No		Quiz 10	Lab 10, midnight 6/21/2017
12	6/29/2017	FINAL - (120 min) 6:15-8:15 PM	No		FINAL	