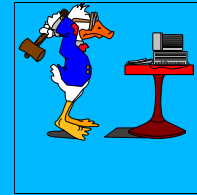


ITSY-2459-8001
Security Assessment/Auditing
Spring 2010
Professor: Zoltan Szabo
D111 LEC TR 11:20AM 12:45PM
D111 LAB TR 12:50PM 02:15PM



CATALOG DESCRIPTION:

Capstone experience for the security curriculum. Synthesizes technical material covered in prior courses to monitor, audit, analyze, and revise computer and network security systems to ensure appropriate levels of protection are in place.

LEARNING OUTCOMES:

Review security plan to ensure appropriate level of protection; implement network security design; audit network system based on security design; use relevant tools to maintain security requirements; and review all security policies and procedures on a regular basis.

COURSE OBJECTIVES:

With the threats of cyber terrorism and corporate espionage increasing, the need for trained network security professionals continues to grow. This course covers penetration-testing tools and techniques that ethical hackers and security testers use to protect computer networks. This course provides a structured knowledge base for preparing security professionals to discover vulnerabilities and recommend solutions for tightening network security and protecting data from potential attackers.

Specific topic coverage includes:

1. Ethical Hacking Overview
 - a. Role of an ethical hacker
 - b. Legality
 - c. Illegal activities
2. TCP/IP Concepts Review
 - a. TCP/IP protocol stack
 - b. Basic concepts of IP addressing
 - c. Binary, octal, and hexadecimal numbering systems
3. Network and Computer Attacks
 - a. Types of malicious software
 - b. Protecting against malware attacks
 - c. Types of network attacks
 - d. Physical security attacks and vulnerabilities
4. Footprinting and Social Engineering
 - a. Web tools for footprinting
 - b. Conducting competitive intelligence
 - c. DNS zone transfers
 - d. Types of social engineering
5. Port Scanning
 - a. Port scanning methodology
 - b. Different types of port scans
 - c. Various port-scanning tools
 - d. Ping sweeps usage
 - e. Shell scripting to automate security tasks
6. Enumeration
 - a. Enumeration step of security testing
 - b. Enumerate Microsoft OS targets
 - c. Enumerate NetWare OS targets
 - d. Enumerate *NIX OS targets
7. Programming for Security Professionals
 - a. Basic programming concepts
 - b. C programming
 - c. HTML programming
 - d. Perl programming
 - e. Object-oriented programming concepts

8. Microsoft Operating System Vulnerabilities
 - a. Tools available to assess Microsoft system vulnerabilities
 - b. Vulnerabilities of Microsoft operating systems
 - c. Vulnerabilities of services running on Microsoft operating systems
 - d. Harden Microsoft systems against common vulnerabilities
 - e. Best practices for securing Microsoft systems
 9. Linux Operating System Vulnerabilities
 - a. Fundamentals of the Linux operating system
 - b. Vulnerabilities of the Linux operating system
 - c. Linux remote attacks
 - d. Countermeasures for protecting the Linux operating system
 10. Hacking Web Servers
 - a. Web applications
 - b. Web application vulnerabilities
 - c. Tools used to attack Web servers
 11. Hacking Wireless Networks
 - a. Wireless technology
 - b. Wireless networking standards
 - c. Process of authentication
 - d. Wardriving
 - e. Wireless hacking and tools used by hackers and security professionals
 12. Cryptography
 - a. The history of cryptography
 - b. Symmetric and asymmetric cryptography algorithms
 - c. Public key infrastructure (PKI)
 - d. Possible attacks on cryptosystems
 13. Protecting Networks with Security Devices
 - a. Network security devices
 - b. Firewall technology
 - c. Intrusion detection systems
 - d. Honeypots
 14. Business and IA Policy Integration
 - a. Threat Modeling to ensure Business Continuity
 - b. Mandates and Law
 - c. Policies (people, operation, technology)
 - d. Preparing for the Unknown
 15. System Auditing (OVAL, nessus, MSBA)
 - a. Existing and Recommended Security Controls
 - b. Following Government guidelines
 - c. PCI certification
 - d. NIST 800-37
-

COURSE PREREQUISITES: None. It is recommended, however that students know how to type, use Microsoft Windows© and have completed a computer literacy course.

TEXTBOOK and MATERIALS:

- Michael Simpson, ISBN 13: 978-0-619-21708-2, ISBN 10: 0-619-21708-1, Publish date: October 19, 2005
 - Three high-density computer diskettes (3 ½ inch), IBM formatted, labeled with your name.
 - Two 8 ½ x 11 inch pocket folders.
 - Richland College Student picture ID, to allow use of the drop-in computer labs.
-

SCANS COMPETENCIES (Secretary's Commission of Achieving Necessary Skills)

Foundation Skills

- Read, write, perform arithmetic and mathematical operations, listen, and speak effectively.
- Think creatively, make decisions, solve problems, visualize, know how to learn, and reason effectively.
- Display responsibility, self-esteem, sociability, self-management, integrity, and honesty .

Workplace Competencies

- Identify, organize, plan, and allocate resources effectively.
- Acquire and use information.
- Work with others effectively.
- Understand complex interrelationships.
- Work with a variety of technologies

Institution Policies	
ADA statement	If you are a student with a disability and/or special needs who requires accommodations, please contact the college Disability Services Office.
Religious holidays	Absences for observance of a religious holy day are excused. A student whose absence is excused to observe a religious holy day is allowed to take a make-up examination or complete an assignment within a reasonable time after the absence.
Academic dishonesty	Scholastic dishonesty is a violation of the Code of Student Conduct. Scholastic dishonesty includes, but is not limited to, cheating on a test, plagiarism, and collusion. As a college student, you are considered a responsible adult. Your enrollment indicates acceptance of the <u>DCCCD Code of Student Conduct</u> published in the DCCCD Catalog. https://www1.dcccd.edu/cat0506/ss/code.cfm
Withdrawal policy (with drop date)	If you are unable to complete this course, it is your responsibility to withdraw formally. The withdrawal request must be received in the Registrar's Office by (semester's drop date). Failure to do so will result in your receiving a performance grade, usually an "F." If you drop a class or withdraw from the college before the official drop/withdrawal deadline, you will receive a "W" (Withdraw) in each class dropped.
Repeating this course	Effective for Fall Semester 2005, the Dallas County Community Colleges will charge additional tuition to students registering the third or subsequent time for a course. All third and subsequent attempts of the majority of credit and Continuing Education/Workforce Training courses will result in additional tuition to be charged. Developmental Studies and some other courses will not be charged a higher tuition rate. Third attempts include courses taken at any of the Dallas County Community Colleges since the Fall 2002 Semester.
Disclaimer reserving right to change syllabus	The instructor reserves the right to amend this syllabus as necessary.

ATTENDANCE POLICY: It is expected that students will attend class regularly. Class attendance is 5% of the course grade. Students who will be absent from class for the observance of a religious holiday will be allowed to makeup examinations or assignments missed that day IF their instructor was notified not later than the 15th day of the semester. Please refer to the college catalog Student Obligations- Attending Classes section.

WITHDRAWAL AND IMPORTANT DATES: The deadline for receiving a "W" is indicated on the academic calendar and the current class schedule.

For sixteen week classes:

- Last day to drop a class without a "W" - Monday, February 1
- Last day to drop a class with a "W" - Thursday, April 15

Refund Dates

Refunds may take up to 30 days to process. To receive a 100% refund you must drop before the first day of the semester.

For sixteen week classes withdraw:

- Before January 19 - 100% refund
- January 19 - February 4 - 70% refund
- February 5 - 10 - 25% refund
- On or After February 11 - No refund

For flex term, fast track and mini-mester classes:

Students must withdraw PRIOR to the first class day of the semester to receive a 100% refund.

If your class does not start on the first day of the semester and end on the last day of the semester, your refund dates could be different than the ones listed above. Please contact the Admissions Office or Business Office for the refund schedule.

Holidays - No Classes/Admissions/Registration

- Martin Luther King Jr. Day - January 18
- District Conference Day/Staff Development Day* - March 4-5
- Spring Break - March 15 - 19
- Campus Closed - March 19
- Spring Holiday - April 2

DISABILITY SERVICES/SPECIAL SERVICES:

Student with a disability and/or special needs that requires ADA accommodations should contact the Richland College Disability Services Office, T120, (972) 238-6180.

COMPUTER/INTERNET POLICY:

Richland College students, have access to the Del Rio computer labs for educational and instructional purposes. You are required to show your Richland Student ID when requested by lab personnel. You are expected to follow lab policies as well as the Student Code of Conduct specified in the catalog. Richland Computer Lab cannot provide any software for outside use.

<https://www1.dcccd.edu/cat0506/ss/computer.cfm>

TUTORING AND OTHER ASSISTANCE POLICIES:

Tutoring is available through the Center for Teaching and Learning Connections ((972) 238-6226, Medina 216) and the Del Rio lab D229 ((972) 238-6317, large counter center of second floor). Generally, one hour per week is free.

SAFETY POLICY: It is important for students to participate in this class in a safe, appropriate manner. We occasionally have to step over cords for the multimedia cart and/or computer equipment. We also need to watch out for boxes and paper, students' backpacks, etc. During the first few labs, you will be encouraged to build good computing habits, designed to prevent eyestrain, carpal tunnel syndrome, etc.

CAMPUS FOOD AND DRINK POLICY: No eating or drinking is allowed at the computer tables in the lab rooms. Students, who wish to eat or drink in the lecture room, must sign the Statement of Responsibility, an agreement to be responsible for removing cans, bottles, and trash, from the learning environment.

TESTING: There are two testing elements; short Unit Quizzes and three Major tests. All quizzes and tests will be Closed Book, unless notified in advance. **No make-up quizzes or exams will be given!!!!!!**

DUE DATES: Unit quizzes for this material will be given during the first ten minutes of a class meeting. **DE#** indicates the opportunity to present a "Discovery Event" reports for that discovery period.

LABORATORY ASSIGNMENTS: There are 15-17 Laboratory Assignments (**LA**). Laboratory Assignments will be completed in the lab and no makeup will be allowed. Labs are for your own benefit. You can simulate some of the labs using TestOut software in the open lab (on your own time). The default login id and password is your student id. First, you need to login to the network as ITCC and no password to use the software. Make sure you change your password after your first login.

DISCOVERY EVENTS: Extra credit. This option involves classroom presentation of any current event related in the IT field to the subjects learned prior to the upcoming DE. Each student required to choose 2 dates to present 2 independent findings about new technology, improvement to existing technology or PC component. Each presentation should not exceed 10 minutes and presentation style chosen individually. A written presentation must be handed in by each student for each presentation to earn a grade. Valued at 10% of the final grade.

Important: These requirements are cumulative. There are three scheduled periods, as indicated on the *Assignment Schedule*, to make up the two **DE's**. A missed chance for a discovery period is lost and may not be recovered.

Supplementary information: Available on campus, in D257 computer lab by accessing G:\Data\Szabo\ITSY2459. The folder contains class notes, PowerPoint slides, class announcements, the course syllabus, test dates, and other information for the course. Read

Grading and Evaluation Criteria

40% of the grade is based on a midterm and a final examination. Both examinations are cumulative and given in a varied format. An in-class review will be held prior to each examination.

20% of the grade is based on quizzes. Quizzes are announced one day in advance and can vary from three to five questions and that might be in any format.

40% of the grade is based on keeping a project notebook. Students are asked to obtain a small notebook or to use a lab notebook and keep notes on the results of Hands-on Projects and Case Projects at the end of each chapter in the text.

A 90 - 100

B 80 - 89

C 70 - 79

D 60 - 69

F 59 below

INSTRUCTOR DATA: Zoltan Szabo

Office Location: Del Rio Building, D112
Office Hours: By appointment only
Division Office: B101, Phone: 238-6074

Office: (972) 238-6059

E-Mail: zszabo@dcccd.edu

Lab: D257; (972) 238-6317

COURSE OUTLINE and/or ASSIGNMENT SCHEDULE:

LAST DAY TO DROP WITH A "W" Thursday, April 15

Week	Topics	Chapter Readings	Exams
1	Intro Ethical Hacking Overview 1/19, 1/21	Chapter 1	
2	TCP/IP Concepts Review 1/26, 1/28	Chapter 2	
3	Network and Computer Attacks 2/2, 2/4	Chapter 3	
4	Footprinting and Social Engineering 2/9, 2/11	Chapter 4	
5	Port Scanning 2/16, 2/18	Chapter 5	
6	Enumeration 2/23, 2/25	Chapter 6	Mid-term Exam
7	Programming for Security Professionals 3/2, 3/4	Chapter 7	
8	Microsoft Operating System Vulnerabilities 3/9, 3/11	Chapter 8	
9	3/15 – 3/19 SPRING BEAK	OFF	Spring Break
10	Microsoft Operating System Vulnerabilities 3/23, 3/25	Chapter 8	
11	Linux Operating System Vulnerabilities 3/30, 4/1	Chapter 9	
12	Linux Operating System Vulnerabilities 4/6, 4/8	Chapter 9	
13	Hacking Web Servers 4/13, 4/15	Chapter 10	
14	Hacking Wireless Networks 4/20, 4/22	Chapter 11	
15	Cryptography Protecting Networks with Security Devices 4/27, 2/29	Chapter 12 Chapter 13	
16	Business and IA Policy Integration System Auditing (OVAL, nessus, MSBA) Review 5/4, 5/6	Chapter 14 Chapter 15	
17	5/11 Final Exam		Final Exam