TRINE
UNIVERSITY

COURSE SYLLABUS

COURSE TITLE: NETWORK SECURITY

TERM & YEAR: SPRING 2017

COURSE & SECTION NUMBER: INF 343.01

TIME & PLACE: TR 2:00-3:15 PM @ BEST 215

INSTRUCTOR: Bill Barge

OFFICE LOCATION/HOURS: Best Hall 202B
MWF 9:00-10:30 AM; TR 9:30-11:00 AM
MW 2:00-3:30 PM; or by appointment

OFFICE PHONE: 260-665-4298

EMAIL: bargeb@trine.edu

COURSE DESCRIPTION: Introduction to network security, including concepts and theory of security policies, access control methods, site security, network security, system security, user security, application security, and managing security functions through cryptographic services, protocols, authentication, authorization, and access control technologies.

PREREQUISITES: INF 303

REQUIRED TEXT: CompTIA Security+, Third Edition (SY0-401) by David L. Prowse. ISBN 978-0-7897-5333-5.

REFERENCES: OSI Model

OTHER MATERIALS: Wireshark network analyzer software (http://www.wireshark.org/) and other open source software, as required.

LEARNING OUTCOMES: Upon completion of this course, the student should be able to:

1. Explain encryption algorithms that provide confidentiality
2. Explain hashing algorithms that provide integrity
3. Explain authentication, including perimeter security
4. Compare and contrast the four factors of authentication including something you know, something you have, something you are, and something you know
5. Explain transaction logs as a method of non-repudiation
6. Demonstrate the security of wired and wireless networks
7. Describe the importance of redundancy and disaster recovery as they relate to availability
8. Create a risk assessment to create the security policies and procedures necessary to protect a computer network

COURSE REQUIREMENTS:

ATTENDANCE/PARTICIPATION:

You are expected to attend class. You are also expected to be on time, in your seat and ready to go, at the beginning of class. Not all knowledge needed for this class will be out of the book. Some topics will be covered only in class lectures while other topics may be clarified through class discussions. Assignments will be assigned and explained in class. If you miss a class, it is your responsibility to get notes from another student before or after class – not during class. Remember, an excused absence excuses you from class; it does not excuse you from learning the material. Test attendance is mandatory!

GRADING/EVALUATION:

The grade for this course shall be based upon quizzes, assignments, labs, exams, and a final project. The homework assignments are based on materials from the text. The labs will use the open-source software Wireshark to illustrate key concepts from selected chapters. The research project will allow the student to put together all of the concepts from this course into a comprehensive security policy project.

The final course grade will be based on: Labs (30%), Project & Presentation (10%), Exam #1 (30%), Exam #2 (30%).

The grading scale for the course is:

A = 90 to 100
B = 80 to 89
C = 70 to 79
D = 60 to 69
F = 59 and below

ASSIGNMENTS & EXAMS

NO LATE ASSIGNMENTS/WORK WILL BE ACCEPTED. It is in your best interest not to fall behind in the work in this class, and you will not be able to perform well on the exams if you do not do the assignments. You can always turn an assignment in early.

If you miss an exam, you must contact me within 24 hours of the exam with the reason or receive a 0% on the exam. Do not expect your coach to contact me – it is your responsibility. Once you begin an exam, you will need to complete the exam in one sitting. If you need to leave the room, you will need to hand in your exam.

Exams will have a time limit of no more than 80 minutes. Why the time limit? To put everyone on a level playing field. Some students cannot stay (and neither can your instructor) because they have another class/activity immediately after this class. On my part, I will do my best to construct exams that can be completed in the time period.

All grades will be posted to Moodle. The Moodle grade book is the official grade book for the course. It is your responsibility to check Moodle to verify your grade has been posted correctly. It is also your responsibility to verify the grading of assignments and exams. If a grade was calculated or posted incorrectly, please let me know ASAP. You must have the retuned assignment/exam with you when you talk with me. I try to be as consistent as possible when grading. If you have a question about a grade, you must contact me within 7 days after the assignment/exam is returned. **No point adjustments will be made after those 7 days**.

OTHER POLICIES:

ACADEMIC MISCONDUCT
The University prohibits all forms of academic misconduct. Academic misconduct refers to dishonesty in examinations (cheating), presenting the ideas or the writing of someone else as one's own (plagiarism) or knowingly furnishing false information to the University by forgery, alteration, or misuse of University documents, records, or identification. Academic dishonesty includes, but is not limited to, the following examples: permitting another student to plagiarize or cheat from one's own work, submitting an academic exercise (written work, printing, design, computer program) that has been prepared totally or in part by another, acquiring improper knowledge of the contents of an exam, using unauthorized material during an exam, submitting the same paper in two different courses without knowledge and consent of professors, or submitting a forged grade change slip or computer tampering. The faculty member has the authority to grant a failing grade in cases of academic misconduct as well as referring the case to Student Life.

PLAGIARISM
You are expected to submit your own work and to identify any portion of work that has been borrowed from others in any form. An ignorant act of plagiarism on final versions and minor projects, such as attributing or citing inadequately, will be considered a failure to master an essential course skill and will result in an F for that assignment. A deliberate act of plagiarism, such as having someone else do your work, or submitting someone else's work as your own (e.g., from the Internet, fraternity file, etc., including homework and in-class exercises), will at least result in an F for that assignment and could result in an F for the course.

ELECTRONIC DEVICES:
Use of electronic devices including smart watches and cell phones is prohibited during exams or quizzes unless directly allowed by the instructor.

DIGITAL MEDIA DEVICES
Our learning environment, including classrooms and public lecture halls, should be free from disruptions from personal communication and media devices. In such settings, cell phones and all other such devices must be turned off. Camera cell phones must be turned off in locker rooms and other such private places. The use of a computer in the classroom is a privilege, not a right. The student must understand (and resist) the temptation to "surf the 'net" or engage in ANY activity not related to the classroom topic and discussion. Violations of the Trine University Information Technology Security Policy may result in disciplinary action by the University.

ADDITIONAL INFORMATION:

E-MAIL
Every message you send to the instructor (directly or via the course site) must have the course name and/or number in the subject line. If the subject of the email is not readily identified as having to do with a specific course I am teaching or another official function, e.g., advising, it will be deleted.

Your complete name needs to be in the message. I will never remember who is slimjim500@ hotmail.com. I will probably not be able to respond if you don't include first and last name. The subject of the communication must be clear, otherwise I cannot respond. "*Re: your message"*, doesn't tell me much. The contents of the message must be clear. Including the original message in the reply is a good idea. I typically work with up to 150 students, advisees, and other personnel in multiple courses any given semester. "*I did what you said but still don't understand step 2"* doesn't give me enough information to respond.

If a subject does not clearly indicate the course name and/or number, the sender might be blocked. When a sender is blocked, all their messages are blocked until the sender is unblocked. If you think you might have been blocked, phone or visit me to initiate the unblocking procedure. Unfortunately, due to a large amount of spam and unwanted emails, blocking is necessary. The same works in reverse. Many emails or attachments I send are blocked or filtered by software on your end (companies and universities are notorious for blocking wanted email).

MOODLE
All assignments are available in Moodle and will be submitted via Moodle. The Moodle gradebook is the official gradebook for the course. NO LATE ASSIGNMENTS WILL BE ACCEPTED. Assignments submitted after the due date will receive no credit.

COURSE CALENDAR/SCHEDULE:

Week	Description
1	Introduction, Syllabus, Networking Basics, Communication Media, OSI & TCP/IP, Local Area Networks, System Security Services & Mechanisms Chapter 1 Introduction to Security
2	Chapter 2 Computer Systems Security **Lab #1 Wireshark (Ticked Off Developer) – Thursday, January 26th**
3	Chapter 3 OS Hardening and Virtualization Chapter 4 Application Security **Lab #2 Challenge Group/Tool Due – Thursday, February 2nd**
4	Chapter 5 Network Design Elements Chapter 6 Network Protocols & Threats **Lab #3 Wireshark (Operating System Fingerprinting) – Thursday, February 9th**
5	Chapter 7 Network Perimeter Security **Lab #4 Wireshark (Operation Aurora) – Thursday, February 16th**
6	Chapter 8 Securing Network Media and Devices **Lab #5 Wireshark (ARP Cache Poisoning) – Thursday, February 23rd**
7	Chapter 9 Physical Security and Authentication Methods
8	**Exam #1 (Chapters 1-9) Tuesday, March 7th**
9	**SPRING BREAK – March**
10	Chapter 10 Access Control Methods and Models **Lab #6 Wardriving Due – Thursday, March 23rd**
11	Chapter 11 Vulnerability and Risk Assessment Chapter 12 Monitoring & Auditing
12	Chapter 13 Encryption & Hashing Concepts **Lab #7 Wireshark (Remote Access Trojan) – Thursday, April 6th**
13	Chapter 14 PKI and Encryption Protocols
14	**Lab #8 Challenge – Tuesday or Thursday depending on group schedule** **Lab #9 PKI Due – Thursday, April 20th**
15	Chapter 15 Redundancy & Disaster Recovery Chapter 16 Policies, Procedures, and People **Lab #10 Wireshark (Ann Tunnels Underground) Due – Thursday, April 27th**
16	**Lab #11 RSA Due – Tuesday, May 2nd** **Exam #2 (Chapters 10-16) – Thursday, May 4th**
17	**Project & Presentations – Wednesday, May 10th @ 8:00-10:00 AM**