Introduction to Information Security Syllabus

Course:	INLS 490-248
Instructor:	Patrick Hodges
Email:	pjhodges@live.unc.edu
Course Sites:	unc.phodges.pw and uncinls490fa17.slack.com
Office Hours:	Before and after class, and otherwise as requested
Course Prerequisites:	INLS 161
Location:	Manning 117, Tuesday 6:00-8:45pm

Target Audience:

Course is targeted at students who have little to no exposure to security concepts who want to understand how information security impacts individuals and organizations.

Course Description:

Students will learn about many of the current issues facing businesses as well as how to prevent and discuss these issues and controls in depth. Focus will be placed upon preventing loss of information and protecting networks. Students should be able to understand any security control, describe its usage and rationale, as well as test and verify these controls are working as expected. By understanding offensive and defensive tools as well as gaining a wider knowledge of computer security they should be able to understand how computers, networks, policy, and controls can be used to secure information. Students will use controlled virtual machines to investigate and mitigate issues with attention paid to potential abuses of systems and the knowledge of legal aspects around remotely accessing computers. In conjunction with discussion of new and recent news regarding exploits or data loss, these lessons will allow students to discuss trending topics or niches of interest for research. Students will focus on controls and quantifiable protection methods rather than understanding all technical nuance of the attacks used to compromise.

Course Requirements:

Students will need to think critically about security and controls as well as participate in labs using virtual machines to explore security tools and techniques. Students will need a laptop and VMware Workstation Player software to complete lab assignments.

Grades:

Class Participation & Forum posts	25%
Projects & Papers	35%
Exams	30%
Quizzes	10%
Homework	0%

Course Policies:

Students will adhere to university academic integrity agreement and attend all classes on time. Please let me know if you are unable to make class as we will move quickly through material in order to allow more time for interactive labs and new material. Late work will be accepted with a 20% penalty per day. All work should be submitted through group discussion forum or electronically via email or Sakai. Students are allowed to use the internet during assignments and group projects, but not during exams.

Disclaimer:

Any of this is subject to change, but I will alert you to any changes and make announcements on the course site. Please see the site page for any news or updates regarding class cancellations or other immediate, class-wide concerns.

Dates:

Week 1	Class Thursday only 1/12 Introduction and VM Install
Week 2	Lesson 1: Basics and Foundations
Week 3	Lesson 2: History, OSI Model, Networking
Week 4	Top 20 Intro Lab 1 Project 1 Assigned
Week 5	Lesson 3: CIA Triangle and Incident Response DBIR Overview
Week 6	Lesson 4: Securing Yourself Project 1 Due
Week 7	Midterm Exam
Week 8	Lesson 5: Securing Your Network Project 2 Assigned

Week 9	Lesson 6: Application of Security Topics
Week 10	Spring Break
Week 11	Lesson 7: Securing Yourself Online Project 2 Due Paper Assigned
Week 12	Lesson 8: Usability vs. Security
Week 13	Threat Modelling and Risk Assesment
Week 14	Lesson 9: Wrap up and Top 20 Review Paper Due
Week 15	Final Exam Prep and Post Survey
Exam Date	TBA

Class Participation & Forum Posts:

This course is highly interactive and I encourage (and require) class participation for students to be engaged with the course material. There is a group Slack channel and we will have prompts once per class. Students are required to make 2 substantive posts per week and engage with other students regularly to receive full credit (2 responses to others and 2 posts of your own for a total of 4 Slack messages). We may not cover one lesson per class period, so you still need to post 4 times per week reflecting what material we covered, the suggested discussion prompts are only a starting point for your discussions. Discussion topics should include: citation or site with external information and a brief analysis or opinion on the source. Do not simply paraphrase the source, connect it to something we discussed in class or a control. Feel free to use current events or historic records or any other credible source.

Students are also expected to present to the class at least twice during the semester during the class opening (maximum of 3 people per session). This allows students to present about a topic of interest: anything from an expansion on something learned from last class, to unanswered questions, to timely news, or discussion about a tool used. These mini-presentations should take about 5-10 minutes and show students' understanding of recent material, a topic of interest, or a discussion of recent events in news and security.

Projects & Papers:

There will be term papers, longer projects, and lab reports that will need to be completed. They will encompass a wide variety of topics and allow you to show your technical knowledge and how this impacts security as a whole. Papers will need to be submitted electronically via email and not be links to Google docs or similar. Please use PDF formatting and use whatever citation/ writing style you chose. I will not dictate a single style, but please know that part of these reports is overall professionalism and the style, tone, and layout of your papers will be taken into account for your grade in addition to the content.

Quizzes:
Pop quizzes will be given at random, no makeup will be offered. They may cover lecture topics, homework material, or lab techniques. They are to ensure you are keeping up with homework and ensure you are prepared for the exam and future labs that build on previous information.

Midterm & Final Exams:
Exams will be cumulative and students will not be allowed to use the internet. Exams will have a technical and then analytical portion that will demonstrate mastery of both. This means a technical portion using your computer and then a writing portion. Network usage will be monitored for honor code infractions.

Homework:
There will be small assignments, usually technical or reading based in nature, that will be assigned throughout the course. However, you will need these programs and knowledge of their use for labs and exams.

Honor Code:
This course is taught in alignment with the UNC honor code, which all students agree to uphold. More information can be found at: https://studentconduct.unc.edu/faculty/honor-syllabus. This means that for tests, exams, quizzes, and other situations where usage of external resources (internet, chat, or thoughts/ideas not your own) you will refrain from using said external resources. In addition, this means that all concepts, ideas, or words that are not your own need to be cited in some consistent manner. Please let me know if you have any questions regarding this or any other policy related to this class.