INLS 690-263: Information Security and Assurance (Practical Elements of Information Security Assessment) - Spring 2018

Instructor: Jos Purvis (josp@mail.unc.edu)
Class Sessions: Thursday evenings, from 17:45 to 20:30 (5.45 to 8.30 PM), Manning Hall Room 117
Office Hours: Before and after class Thursdays, and by appointment

Welcome to class! It's important to know first and foremost that the syllabus is a **living document**: the most current copy of it is always on the course page in Sakai, so **always** check there first. I will do my absolute best to announce any syllabus changes, particularly if they affect due dates or assignment content.

Course Summary

Hands-on, practical review of current security tools and concepts. Students will walk section by section through a complete security review from soup to nuts, using each area as an excuse to delve into security technology and management as well as connecting technical reviews of packets and software to the IT processes that control them. Students should leave comfortable with the use of common security tools, with identifying and prioritizing the risks present in an IT system, and with presenting their findings to a non-technical audience.

Contacting Your Instructor

The absolute best way to reach me is email: either josp@email.unc.edu or jos@unc.edu works just fine, and it goes to my mobile as well as my laptop. I try to respond to everything I get within 24 hours; if you haven't heard from me outside of that time, feel free to give me a nudge as I may have missed it. I will be setting up a Slack channel for class and will provide details on that for everyone once it's set up. You can also call or text my cell at +1.919.794.8533, but this is really for **emergencies** only.

Expectations

You should expect the course to be a mix of technical and theoretical—it's important to discuss the macro and the micro level, after all! Since this is a graduate course, I'm expecting graduate-level writing and discussions:

- Write in clear, well-formed English, free from typos and grammatical issues;
- When making assertions, use references or citations to support your point, and cite them correctly;
- Stick with quality over quantity, particularly in weekly writing exercises.

Class is conducted as a graduate seminar: we'll be dividing our time in class between

lecture, discussions, and lab or technical work. I promise I won't hold class any longer than required to cover material for the week, but in exchange I ask that you do your level best to attend every week on time so that we can start promptly and cover what we need to.

Grading

Grading Breakdown

Grading for the course will be broken down as follows:

- 25% - Weekly assignments
- 25% - Section Tests
- 25% - Technical projects
- 15% - Final Exam
- 10% - Class participation

Due Dates and Delays

Every assignment in this course will come with a due date. Unless otherwise specified, assignments are due by NOON (12 PM Eastern) on their due date. Exceptions will absolutely be granted under mitigating circumstances, but this is a **great deal** more likely to happen if you contact me as soon as you think you will have an issue. When in doubt, speak up early! Late assignments without an extension will be accepted up to 72 hours past the due date, with a late penalty of 10 points per day past the due date. The technical assignments are intended to be challenging and to include a fair amount of work, so plan to start work early, work steadily, and speak up if you're having issues: I'm here to help you succeed at this!

Requirements

Students should meet have basic familiarity with the following topics:

- Elementary concepts of IP addressing;
- Use of the Linux command line.

Students will require a working computer for class and/or assignments, but may run MacOS, Windows, or Linux as desired.

Assignments

All assignment information, including reading assignments, will be in Sakai as well as emailed to everyone when assigned.

Tech

We will have periodic technical, hands-on assignments in the form of projects or labs to complete. Sometimes these will simply be a continuation of lab work done in class, while other times they'll be separate. These will include a combination of hands-on technical work and writing about the work.

Writing

As a technology professional, you'll be expected to stay abreast of new developments in

technology and security, and to be able to explain these to non-technical (or less technical) people. To that end, I will sometimes assign a *short* writing assignment. These should be written and turned in using Sakai; you are welcome to write them in a document (Word format or PDF) and submit that as an attachment, or to simply paste your assignment into Sakai directly.

Reading

I'll be assigning reading from the textbook for most weeks; this should be done before class. You don't need to memorize it by any means, but I'm going to be writing lectures with the assumption that you've done the reading and will expect you to keep up.

Schedule

Week 1 (10 Jan)

- Introductions
- Security Concepts: Risk Management, Controls, Audits, Assessments

Week 2 (17 Jan)

- Auditing Linux & Windows: Baselines and System Hardening

Week 3 (24 Jan)

- Auditing Linux & Windows: Patching and Access Control

Week 4 (31 Jan)

- Auditing Linux & Windows: Anti-malware and attack prevention
- **Test 1 Scheduled**

Week 5 (7 Feb)

- Auditing Networks: TCP/IP Fundamentals, Network Packet Analysis

Week 6 (14 Feb)

- Auditing Networks: Firewall Concepts from ACLs to Statefulness

Week 7 (21 Feb)

- Auditing Networks: Intrusion Detection and Prevention

Week 8 (28 Feb)

- Auditing Networks: Wireless LANs

Week 9 (7 Mar)

- **NO CLASS**
- **Test 2 Scheduled**

SPRING BREAK (14 Mar)

Week 10 (21 Mar)

- Auditing Physical Security

Week 11 (28 Mar)

- Auditing Data Management: Data storage and Databases

Week 12 (4 Apr)

- Auditing Data Protection: Fundamentals of Cryptography

Week 13 (11 Apr)

- Auditing Data Protection: Applied Cryptography in SSH and PKI

Week 14 (18 Apr)

- Topic TBD
- **Test 3 Scheduled**

Week 15 (25 Apr)

- Class wrap-up: Finals prep, review, questions, final discussions

Final Exam: 30 Apr