Today’s Internet not only features rich applications and always-on connections, it is also notorious for prevalent security threats that affect everyone. Knowledge on computer and network security is hence necessary not only for people working in the field (e.g., an IT support, system administrator, researcher), but also for individuals trying to protect themselves and others. While computer and network security courses have been offered for many decades to equip students, often the courses (especially in the undergraduate level) had to focus more on the theoretical foundation. In other words, students still lack the necessary hands-on experience with many security topics. This was primarily caused by two limiting factors. First, there was a serious lack of well-developed security labs that fit different platforms. Second, there is simply not enough time to cover all aspects of security while providing extensive hands-on labs in one course. Thanks to the fundings from NSF, recently security researchers have been addressing the first limitation by systematically designing various types of high-quality labs that are freely available. Now, to address the second limitation, we design this experimental security course, which covers only selective topics that are relevant to the hands-on labs.

In this course, students will learn fundamentals of computer and network security, some aspects of information systems security such as access control, hacks/attacks, systems and programs security, intrusion detection, cryptography, networks and distributed systems security, and smartphone security. Through extensive hands-on labs, students will build deep understanding on security in practice, and develop the skills necessary to formulate and address the security needs of enterprise and personal environments.

Topics:
In (almost) each week, we will teach one lecture and hold one lab session in class (some labs require two weeks though). The lectures are focused on selective security topics, preparing students with the necessary theoretical foundation to understand and carry out the lab tasks.

Target Audience:
Undergraduate students who have taken IST 451 or master students have taken a security related course before, have learned a programming language (e.g., C, C++, or Java), and know the basics (or willing to learn) of Linux system (e.g., commands, file systems). Students are expected to use their own computers (Windows, Mac or Linux) to run the labs.

Evaluation Methods:
Students will be evaluated through 10+ hands-on lab reports and 3 homework assignments. There will be no exams. Class participations will also be considered.

Book:
Mark Stamp: Information Security Principles and Practice, 2nd edition. (e-textbook available through PSU library) and online lab materials.