CSC 568: Ethical Hacking & Penetration Testing

Dr. Lisa Lancor
lancorl1@southernct.edu
(203) 392-5890

Prerequisites: CSC 555 (*Principles of Information Security*) and CSC 565 (*Computer Networks)*
These prereqs are waived this semester only.

Meeting Times: Tuesday: 5:00pm – 7:30pm in JE 139B

Catalog Description: Principles of network & system penetration, using the same methods as hackers, are explored with the purpose of finding and fixing security vulnerabilities and ensuring the security of information assets. Legal and ethical issues associated with penetration testing are emphasized. The lab-intensive exercises are used to gain practical experiences in areas such as scanning and enumeration, access and exploitation, escalating privileges, malware, buffer overflows, and other relevant topics.

Learning Objectives: Upon successful completion of this course, students will be able to:

1. Explain the rationale for penetration testing including the regulatory and legal requirements.

   Measurement: *Students will be evaluated on homework submissions and exam questions that pertain to the need legal and federal regulations*

2. Analyze the different phases of hacking with an emphasis on recommending strategies for securing information assets at each phase of attack.

   Measurement: *Students will be evaluated on homework submissions and laboratory assignments that pertain to the various attack vectors that are used during different phases of a hack. For example, students will be required to analyze a particular hacking activity and determine the goal of the hacker (e.g. information gathering, escalation of privileges). Based on their findings, they will be required to recommend what assets are at risk and how these assets can be better protected.*

3. Demonstrate the use of various security tools in penetration testing and explain how such tools can be abused by hackers.

   Measurement: *Students will be evaluated on their laboratory activities (through observation) and their laboratory report submissions that will* *require student to use various security tools commonly used by professional penetration testers.*

4. Explain how exploits and vulnerabilities are discovered and the proper procedure for reporting them for proper patching.

   Measurement: *Students will be required to present at least one in-depth report on a particular exploit of their choosing. They must describe the vulnerability and the associated technology upon which the exploit was based, as well as report on who found the vulnerability, how it was discovered (if possible) and the reporting mechanism that was used to notify the security community.*

5. Explore new and emerging security threats and use these to explain the critical need for lifelong learning by security professionals.

   Measurement: *Students will be required to present at least two weekly "Security in the News" or "Breach of the Week" reports describing a vulnerability or exploit that is no more than 30 days old. Their report must not only describe the vulnerability but also classify it under common security classifications (eg. malware, Denial of Service, Advanced Persistent Threats (APTs), etc.)*

Organization: This course will meet once a week for 150 minutes. Normally, the first half of the class will cover the fundamentals of the chosen topic and the second half of the class will provide you with an opportunity to apply what you have learned by completing hands-on laboratory assignments. In addition, a significant amount of learning will take place outside of the classroom through homework and lab preparation assignments.

Obey The Law!!: Don’t disrupt networks or enter computer systems without the explicit written permission of the owners. The hacking skills taught in this course are only safe and legal when used on your own computers, or on computers you have permission to use. If you break the law, you face possible criminal prosecution and prison time, and neither your instructor nor SCSU will be able to save you. In addition, if you commit any computer crime you shall immediately receive a final grade of F in this course and will be banned from using all computer science computer labs. If a situation arises where you are uncertain about the ethics involved, please talk to me.

Attendance: Due to the amount of information covered in each class, attendance to all classes is mandatory and students are responsible for all material presented in class. Missing classes will certainly influence your final grade, therefore attendance **will** be taken at each class. **You are responsible for the material covered in any class**

that you miss!! If you miss a lab assignment, you are expected to make it up (quickly, before the lab drive gets wiped).

Homework: All homework and laboratory assignments must be handed in on time to be considered for full credit. Without an extension granted by the professor, late assignments will be deducted 15% of the total value of the homework. Lateness is defined as any assignment not handed in by midnight on the assigned due date.

Academic Honesty & Collaboration Policy: Honesty is an absolute on all projects and examinations. You are required to compose your own unique solution to each problem and each project. You cannot use any code or work written by anyone inside or outside of this class and turn it in as your own. With that being said, in this course, you will learn just as much (or more) from your interaction with other students as you will from me. Your peers are a valuable resource so you shouldn't overlook them when you need help. Feel free to discuss homework assignments and projects with other students and exchange ideas about how to solve them. There is however, a thin line between collaboration and cheating. While we encourage collaboration, we do not tolerate any form of cheating. Cheating involves the plagiarism of someone else's work and turning it in as your own. To avoid crossing the line, give credit to others when you use their ideas. This is common in scientific literature and something you should get into the habit of doing. If you use an idea that was developed by someone else or jointly with some group, be sure to make a note of that in a homework write-up.

Examinations or assignments which, in the determination of the instructor, have been copied, will be given a grade of zero, and expulsion from the class and/or university may result. If not expelled from the class/university, all homework assignments handed in thereafter will require an oral exam with the instructor. Any repeated incidence of academic misconduct will result in immediate expulsion from the course with the grade of an "F". **Please be aware that the student who offers his/her work to another student will receive the same penalty.**

Presentations: At least two presentations will be made to the class that describes either an assigned topic or a topic of your choosing in the field of information security.

Research Project: Each student is required to complete a semester-long research project in ethical hacking and penetration testing. A project proposal must be written and approved by Dr. Lancor. The project need not be entirely technical; some discussion of societal impact or other issues is acceptable. However, there must be some technical (hands-on) component of the project. Once approved, the final project will be formally written up and presented to the class. The proposal is due on October 28th and the final project is due Dec 16th.

Grading Policy: Students will be evaluated based on one written exam, class presentations, homework assignments, numerous laboratory assignments and a final, end-of-the-semester project. There is no final exam in this course.

Homework & Laboratory Assignments	40%
Midterm Examination	20%
Presentations	15%
Final Project	25%

Makeup exams **will not** be given. However, in ***very*** unusual circumstances, the professor may make an exception.

Course Outline:

1. Introduction to Ethical Hacking & Pen-Testing
    a. What is it and why do we need it?
    b. Legal and Ethical Issues
    c. Professional Certifications
    d. Understanding the Pen-Tester Workflow
    e. Pitfalls & Limitations in Pen-Testing

2. Pre-test Planning
    a. Setting up an effective infrastructure
    b. Establishing grounds rules with target organizations

3. Reconnaissance: Learning about a Target's Infrastructure
    a. What can be discovered about a target organization?
        - Mining Blogs, Search Engines, Social Networking sites, DNS queries, etc
    b. Countermeasures to Reconnaissance

4. Scanning & Enumeration
    a. Understanding Scanning & Enumeration
    b. Common Scanning Tools & Techniques
        - Port Scans, Banner Grabbing, DNS Zone Transfers, etc.
    c. Null Sessions and Shares
    d. Countermeasures to Scanning & Enumeration

5. Gaining Access and Exploitation
    a. Vulnerability Assessments
    b. Security Alerts & Reports
    c. Vulnerability Scanners: e.g. Nessus, Nexpose
    d. Password Cracking Attacks
    e. Malware
    f. Buffer Overflows
    g. Countermeasures to Exploitation

6. Escalating Privileges & Maintaining Access
   a. Pivoting & Escalating privledges
   b. Enumeration from the inside
   c. Covert Channels
   d. Backdoors, Rootkits
   e. Covering track

- **This syllabus represents the intended structure of the course for the semester. It may be changed by the professor via an announcement made during class.**

- **If you are a student with a documented disability, the University's Disability Resource Center (DRC) determines appropriate accommodations through consultation with the student. Before you may receive accommodations in this class, you will need to make an appointment with the DRC, located in EN C-105. To speak with me about other concerns, such as medical emergencies or arrangements in case the building must be evacuated, please make an appointment ASAP.**

- **SCSU is highly committed to providing you with an educational experience that is academically and socially enriching. In line with this mission, we enforce Title IX of the Education Amendment of 1972 which prohibits acts of sexual misconduct (sexual harassment, sexual assault, dating violence, domestic violence and stalking) at educational institutions. To report sexual misconduct students should contact University Police at (203) 392-5375 or 911, and/or Pamela Lassiter, Office of Diversity and Equity, at (203) 392-5491and/or Christopher Piscitelli, Office of Judicial Affairs, at (203) 392-6188. For advocacy and further information including your Title IX rights and reporting procedures visit the Sexual Assault Resource Team (S.A.R.T.) website at http://www.southernct.edu/SART. Please contact Catherine Christy, Women's Center and S.A.R.T. Coordinator, at (203)392-6946 for assistance or with any questions regarding support and advocacy.**