Spring 2020

IT 430-002: Ethical Hacking for System Administrators

Stanley Senesy

IT 430
Ethical Hacking for Administrators
Syllabus

Instructor: Stan J. Senesy (senesy@njit.edu)

Office: NJIT Newark, GITC rm. 3803. (973)596-5288.

Office hours: Posted on Moodle

Text: Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2014 ISBN: 978-1593275648

Schedule: Section 002 - Tuesday, Thursday 10:00 – 11:20 am, GITC 1202
Section 004 - Tuesday, Thursday 2:30 – 3:50 pm, GITC 1202

Course Description

This course will explore the various means that an intruder has available to gain access to computer resources. We will investigate weaknesses by discussing the theoretical background behind, and whenever possible, actually performing the attack. We will then discuss methods to prevent/reduce the vulnerability.

What is ethical hacking? The threat to systems is one that is continuously changing and evolving. It is not sufficient that a System Administrator harden a system based upon the threats that are currently known. Typically, one must think out of the box with the mentality that in order to catch a thief, you need to think like a thief. The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within **legal limits**.

The quote the certification guide, an Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. **Hacking is a felony in the United States and most other countries.** Only when it is done by **request** and under a **contract** between an Ethical Hacker and an organization, it is considered legal. The most important point is that an Ethical Hacker **has authorization** to probe or attack the target. Illegal or unethical use of the techniques discussed in class will result in immediate dismissal from the course and potentially other consequences.

Learning Objectives

Weekly assignment documents will list the learning objectives for that week during the course. Please use them to help you prepare for the assignments and assessments that occur throughout the course. Overall learning objectives, their level and applicable timeframe include:

- (synthesis) develop a comprehensive test plan utilizing penetration testing (weeks 1 through 3)
- (application) conduct passive and active reconnaissance (week 5)
- (synthesis) integrate social engineering into the testing scenario (week 4)
- (application) identify application weaknesses using vulnerability scanners (weeks 6 through 13)
- (analysis) analyze and strengthen password complexity (week 9)
- (analysis) assess vulnerabilities of wireless networking protocols (week 10)
- (application) conduct buffer overflow exploits (week 14)

Prerequisite

IT 340 – Core administration skills learned in this course are required for IT 430 and will not be covered during this class. **You should not take IT 430 unless you have successfully completed IT 340.**

Course Computing Requirements

You must have access to, and administrative rights on, a computer that meets the NJIT minimum baseline computer system standards in order to complete this course. A lab computer is not sufficient. You can find a listing of the minimum computing requirements at http://ist.njit.edu/compreq/faq.php

We will be using vCloud to create and administer virtual instances of various operating systems. We will cover the configuration of your computer during the first week of class.

Please note that students are responsible for the administration/maintenance of their own computer. This includes any software loaded onto it for this course. While I will provide help with problems when I have time available, responsibility for resolving problems remains with the student.

Grading:

Homework/Labs/Quizzes	25%
Project	20%
Midterm	20%
Final Exam	35%

Grades will be computed on a straight scale out of 100 possible points: 90-100=A, 87-89=B+, 80-86=B, etc.

Lectures

I tend to use PowerPoint slides for the main points in my presentations, augmented with board-work when necessary. You can find a copy of the slides that I'll use on the course Moodle board at:

http://moodle.njit.edu

You'll need your UCID and password to login. There is a tutorial on the login screen that you should use if this is your first experience with Moodle.

Labs

You will be assigned an activity each week and given time to complete it in class. These are not 'take-home' assignments, they must be completed during the lab session.

Students who miss class due to an emergency or other legitimate excuse will not have that week's work counted against them, once the reason for the absence has been validated.

Project

There will be a semester-long group project that will allow groups to research deeply into an aspect of penetration test and/or hacking. Details of the project will be discussed once the course begins.

Assessment

The midterm and final will constitute a significant portion of your overall grade. Exam dates and times are listed in the syllabus schedule. The exams will contain information from the text, as well as lectures. The final will be cumulative.

If you miss an exam, the Dean of Students will validate your emergency and will contact me regarding rescheduling. If you have a schedule conflict that will cause you to miss an exam, please inform me immediately so that we can arrange an alternate date for you to complete the test.

Collaboration

You are encouraged to work together with your classmates in order to help your high-level understanding of the material presented in the course. Any solutions to assignments/exams/projects presented for credit must be work created **on your own**. Plagiarism, cheating, or any other anti-intellectual behavior will be dealt with as per the NJIIT Code of Academic Integrity. You can find a copy of the Code here:

https://www.njit.edu/policies/sites/policies/files/academic-integrity-code.pdf

Academic Policies (Please Read This Carefully)

Late work will be marked down according the following scale. The timestamp in Moodle will determine how late your work was (no exceptions):

0 – 24 hours = (-10) points
24 - 48 hours = (-20) points
48 – 72 hours = (-30) points
72 – 96 hours = (-40) points
> 96 hours = no credit

If you 're-submit' homework, the later timestamp will be used to determine if it is late. Once I've graded your work, you cannot modify it and turn it in again.

If you have an emergency (hospitalization, military service, or anything defined as an emergency by the University) please contact the office of the Dean of Students. I will not accept your doctors note, etc. They will validate it and get back to me at which point I will remove the late penalty from your work. Grades will not be posted until after the 96 hour period has expired.

I do not offer 'extra credit' assignments. Every student has an equal opportunity to earn the grade they'd like in the course. The overall point spread is broad enough that doing poorly on a single assignment or quiz should not significantly affect your grade.

I do not curve individual assignments. If, at the end of the course I determine that a curve is justified, then I will curve ALL final grades (either positively or negatively) equally. Grading scales are applied consistently across the entire class - no exceptions.