USC Viterbi
School of Engineering
Information Technology Program

ITP 325: Ethical Hacking and Systems Defense

Units: 3
Spring 2019
Day/Time: Thursday 6:00PM – 9:00 PM

Class Location: OHE 406

Instructor: Caesar J. Sedek
Office: OHE 406
Office Hours: Before class and by appointment
Contact Info: sedek@usc.edu
All Emails Should Have a Response By One Business Day

Teaching Assistant(s): TBA, See Blackboard
Office: OHE 406
Office Hours: As announced.
Contact Info:

IT Help: Viterbi Information Technology
Hours of Service: Monday-Friday 8AM – 9PM
Contact Info: Phone: 213-740-0517; Email: engrhelp@usc.edu

Program Mission: The goal of the Digital Forensics and Cyber Security program at USC is to develop the critical thinking, analytical reasoning, and technical writing skills that are necessary to effectively work in a junior level digital forensic or cyber security analyst role. This is accomplished through utilizing industry standard tools and techniques to investigate labs and cases based upon real-world investigations and intrusions. Students will study various areas of cyber investigations, including digital evidence gathering, reporting, examinations, and court presentations. Students will study cyber security tenants of risk analysis, remediation, as well as penetration testing and network security design.

Course Description

Over the last 30 years, computer security has grown from something whispered in basements and USENET to daily news headlines. Information security breaches have become so commonplace that the public has become numb to the revelation of major attacks, despite digital information being so valuable for both an individual and a company or organization.

Today, cybercrime is more profitable than the global illegal drug trade. Due to its profitability and low risk, there is a need for effective training and education on the methodologies to secure critical infrastructure, whether it is a financial institution's databases or a nuclear power generator. The best person to secure these systems is an ethical hacker.

An ethical hacker is someone who is trained in the art and methodologies of attacking computer systems for the purposes of testing, auditing and securing the infrastructure. The ethical hacker stays within the legal bounds by being under a specific contract with the owner of the system. An ethical hacker never attacks a systems without permission. An ethical hacker follows a very strict code of ethics to maintain credibility.

This course is designed to introduce students to the fundamentals of hacking and becoming an ethical hacker. The course focuses on the code of conduct and ethics of attacking systems. The course also teaches the mindset of the criminal hacker and evolution of the hacker. Students also gain fundamental understanding and education on the elements of compromising computer systems for the explicit purposes of securing them from criminals. The course makes a very clear distinction between criminal hacking and ethical hacking, and only teaches the latter. The course then focuses on some fundamentals of system defense, including configurations and software to prevent unauthorized system access.

Learning Objectives

Upon completing this course, students will:

- Understand the core foundations of ethics in regards to computer security
- Learn about the hacker mindset and the history of hackers
- Understand basic networking and security technologies
- Gain a basic understanding of security policy
- Learn about basic system defense infrastructure

Prerequisite(s): ITP 125 or Instructor's consent; ITP 357, EE 450 or a willingness to learn networking quickly; Python scripting (125 equivalent)

Course Notes

Course is letter graded, with any and all materials available on Blackboard (blackboard.usc.edu). Labs will be conducted in the security lab (OHE 406) during assigned class or lab time.

Technological Proficiency and Hardware/Software Required

You will need a computer (laptop preferred) capable of running multiple virtual machines within VirtualBox. You will need administrative rights to this computer.

Required Readings and Supplementary Materials

- The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy 2nd Edition
  Refereed in syllabus as **BHPT**
  Patrick Engebreston
  ISBN: 0124116442
  https://www.amazon.com/Basics-Hacking-Penetration-Testing-Second/dp/0124116442
- Penetration Testing: A Hands-On Introduction to Hacking

Referred to in syllabus as **PT**
Georgia Weidman
ISBN: 1593275641
https://www.amazon.com/Penetration-Testing-Hands-Introduction-Hacking/dp/1593275641

- Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
  Referred to in syllabus as **VP**
  TJ O'Connor
  ISBN: 1597499579
- All course materials will be posted on Blackboard - http://blackboard.usc.edu
- Readings exist in the syllabus
- Codecademy – Python - https://www.codecademy.com/tracks/python
- Piazza – http://piazza.com/ (you will receive an invitation via e-mail or you can join the class section)
- USB Rubber Ducky
  - https://hakshop.com/collections/physical-access/products/usb-rubber-ducky-deluxe
- Supplemental material available from Cybrary.it

Description and Assessment of Assignments

The assignments will be a combination of in-class and out-of-class laboratory exercises. They will typically involve some form of procedural work (we will provide instructions), with some reflection on the work performed including researching processes and procedures performed. All laboratory exercises will be graded on a point-scale, typically between 10 and 20 points.

Grading Breakdown

	% of Grade
Lab Assignments	45
Class Participation/Attendance	5
CTF Report	25
Final Exam	20
Total	100

Grading Scale

Course final grades will be determined using the following scale

A	93-100
A-	90-92
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

Grading Policies

The lab assistants, graders, and instructors will do their best to return assignments graded to students within one week of the submission. Certain assignments that are longer in length, including exams, case reports, and final projects, may require more time.

The grading rubric is posted. There is no curve, and grades are based on performance in the class. While we understand the importance of grades and maintaining a high GPA, we cannot hand out high marks without justified performance in the class. Do not rely upon an expectation of a guaranteed minimum final grade in this class regardless of its impact on your overall GPA, financial situation, familial situation, or the fate of the galaxy.

The instructor is the ultimate authority over any grade for any assignment, exam or class.

University policy states that no extra credit may be afforded to individual students without the same opportunity made available to everyone in the class. Should there be extra credit in the class, it will be made available to the entire class. Do not ask the instructor for additional extra credit.

Grades will be posted on Blackboard and it is your responsibility to ensure that the grades online are accurate and to follow your progress in the class.

Assignment Policies

The labs will be posted on Blackboard under the "Assignments" or "Labs" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link. Do not email your assignments to the instructor, lab assistants, or graders. TurnItIn may be utilized for some assignments, and you must make sure that you have fully submitted the assignment (usually a two step process).

Unless otherwise noted, all lab assignments are due at the beginning of class the next class period, unless otherwise modified by Blackboard announcement and/or email from the instructor and/or Lab Assistants. Some assignments (typically longer in length) will have a due date on 11:59:59 PM on the Friday or Sunday of the following week. Do not expect a timely response from the lab assistants, graders, or instructors if emailed after normal business hours particularly on the date the assignment is due.

If you join the class after the semester has started, you will have two weeks from the date of enrollment to complete all assignments due before you joined the class unless a written extension is granted from the instructor, typically via email.

It is your responsibility to submit your assignments on or before the due date and verify it has been successfully submitted. Late submissions will not be accepted.

The lab assistants and graders are not authorized to grant an extension on any assignment. Any extensions must be requested of the instructor in writing and confirmed in writing. If you ask for an extension on the day the assignment is due, without expressing an emergency such as being kidnapped and taken to Mexico, it will probably not be granted.

Certain assignments will require a paper submission, and you may be asked to submit them to the main ITP office. There have been previous allegations of student rudeness to the ITP Staff. If the staff complains about you being rude, you will have 25% automatically deducted from your assignment. Don't be rude.

The instructor and lab assistants reserve the right to not answer certain questions about the lab assignment. This is normally due to the nature of the question being directly related to the learning objectives of the lab. You are encouraged to use online resources to further your understanding of the material to successfully answer questions related to the lab assignment (in other words, use your research skills).

All lab assignments have been tested by the instructor and/or lab assignments. Due to the nature of certain software packages and configurations in the lab, the assignments may or may not work as intended. You are encouraged to ask questions if something appears to not work correctly. However, there are certain instances where things are intended to not work correctly and the instructor and lab assistant will indicate as such. When in doubt, do a little research.

Exam Policies

Please review the schedule of classes for the Final Exam schedule. Should you have a scheduling conflict with the final exam, you must contact the instructor and coordinate an alternative time by the end of Week 3. Any requests made after Week 3 are not guaranteed to be accommodated.

Per USC policy, Final Exams must be scheduled during the assigned final examination schedule. It is your responsibility to arrange your travel after the scheduled date of the final exam.

All students are required to participate in the final exam and/or project. Failure to take the final exam and/or submit a final project will result in an automatic failure in the class.

No make-up exams (except for documented medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule. Missing your alarm is not an emergency. A documented medical event (car accident with documentation), family emergency (death in the family), or alien abduction can be considered emergencies.

Contacting the Instructor, Lab Assistants or Graders

When emailing the lab assistants, graders or instructor, please be sure to include your full name, student ID, class name and number, and class section (day and time) in the email.

Emails sent to the lab assistants or graders will be responded to within two business days. The instructor will endeavor to respond to emails within two business days. Do not email anyone with the expectation of an immediate response within the hour. Please do not complain when we have not responded to your email ten minutes before the assignment deadline.

Questions regarding individual clarification or regrade must be made through email to both the grader (if there is one) and the instructor. When requesting a regrade, the instructor has the prerogative to alter a grade higher or lower based upon a review of the entire assignment. Be absolutely certain before requesting a regrade of any assignment or exam – if you are going to roll the dice, be certain of your gamble.

Questions about lab assignments should be submitted through the class discussion board (typically Piazza). This will have a faster response rate. Do not post code or answers on Piazza.

The instructor will post his/her regular office hours on blackboard. You may request a meeting with the instructor outside of normal office hours. Should you go to the instructor's office outside of normal office hours or outside of a scheduled meeting, do not expect the instructor to be able to meet with you. We do have other responsibilities outside of the class.

Attendance Policy

You are expected to be in class, on time, and distraction free. As this class meets once a week and as it is lecture and lab any student who misses more than two classes is in danger of failing the course. Please see the instructor immediately if you have missed at least two class meetings.

This is a lab-based class. Certain class sections will be lecture, lab, or a combination of lecture and lab. Attendance is vital to success in the class, and punctuality is vital to success in your professional careers. The lab assistants will be taking attendance for every class meeting. If you anticipate missing a class due to an event, please email the lab assistants and instructor prior to the start of class. If you are sick, we want you to get better and not infect your fellow classmates – please email the lab assistants and instructor. Should you miss a class with a lab assignment, contact the lab assistants to determine available times to come to the lab and finish your assignment.

Writing Skills

A significant portion of the cyber security and digital forensics curriculum involves communicating what was discovered by writing professional quality reports. These reports are held to standards that are expected by professionals in industry who are writing reports for clients, attorneys, judges and juries. It is expected that the reports will be written with correct spelling, grammar and language nuances of the American English language. A component of each report grade will be based on writing style, grammar and word choice. These reports must be accessible to technical and non-technical readers alike.

If you are not a native English speaker and writer, it is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional careers. Writing assistance is also available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center. Additional writing assistance is also available from the Viterbi Writing Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with University standards, plagiarism of any type will not be tolerated.

Additional University policies follow the course schedule.

ITP 325 - Course Schedule

Subject to Change Throughout The Semester
(In other words, guaranteed to change)

For some readings, you may need to copy and paste the link together, if it runs onto a second line

Week 1 – Week of January 7 – Introduction and Ethics

- Ethical Hacking
- Ethics
- Engagements and Reports

Lab/Homework

Lab 1 - Ethics

Reading

1. BHPT, Chapter 1
2. PT, Chapter 0, 1
3. VP, Chapter 1

Week 2 – Week of January 14 – Review of Everything

- Number systems
- Networking
- TCP/IP
- Subnetting

Lab/Homework

Lab 2 – Programming Review

Reading

None. If you are confused about the review, go to Cybrary.it for additional video lectures about networking and TCP/IP.

Week 3 – Week of January 21 – Reconnaissance

- OSINT
- Passive vs Active recon
- Common tools for recon

Lab/Homework

Lab 3 – Recon lab

Reading

1. BHPT, Chapter 2
2. PT, Chapter 5

Week 4 – Week of January 28 – Google Hacking and Doxing

- Google Hacking
- Doxing Introduction

Lab/Homework

Lab 4 - Doxing Lab

Reading

None

Week 5 – Week of February 4 – Social Engineering

- Human Tendancies
- Social Engineering
- Social Engineering Toolkit

Lab/Homework

Lab 5 – Kali and SET

Reading

1. PT, Chapter 11

Week 6 – Week of February 11 - Scanning

- Scanning Process
- Ping sweep
- Port Scans
- Nmap

Lab/Homework

Lab 6 - Nmap

Reading

1. BHPT, Chapter 3
2. PT, Chatper 6

Week 7 – Week of February 18 – Exploitation, Part 1

- Understanding exploitation
- Buffer overflows

Lab/Homework

Lab 7 – Exploitation

Reading

1. BHTP, Chapter 3
2. PT, Chapters 2, 4, 8

Week 8 – Week of February 25 – Exploitation, Part 2

- Exploitation Frameworks
- Metasploit in-depth

Lab/Homework

Lab 8 – Metasploit

Reading

3. BHTP, Chapter 3
4. PT, Chapters 2, 4, 8

Week 9 – Week of March 4 – Exploitation, Part 3

- Anti-forensics
- Evasion techniques

Lab/Homework

Lab 9 – Antiforensics and A/V Evasion

Reading Before Next Class

1. PT, Chapter 12

Week 10 – Week of March 10 - Spring Break

Week 11 – Week of March 18 – Post-Exploitation

- Meterpreter
- Armitage

Lab/Homework

Lab 10 – Armitage

Reading Before Next Class

1. BHPT Chapter 6

2. PT, Chapter 13

Weeks 12 – 14 – CTF / WARGAMES

Week 15 – Week of April 22 – Course Conclusion

- Careers in Info Sec
- Certifications
- Conferences

Lab/Homework

Exam Review & Final Lab Completion

Reading Before Next Class

n/a

Final Exam

According to Final Exam Schedule found at classes.usc.edu – Normal Classroom

Statement on Academic Conduct and Support Systems

Academic Conduct:

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences that can include expulsion. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Support Systems:

Student Counseling Services (SCS) – (213) 740-7711 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention. engemannshc.usc.edu/counseling

National Suicide Prevention Lifeline – 1 (800) 273-8255
Provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week. www.suicidepreventionlifeline.org

Relationship and Sexual Violence Prevention Services (RSVP) – (213) 740-4900 – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender-based harm. engemannshc.usc.edu/rsvp

Sexual Assault Resource Center
For more information about how to get help or help a survivor, rights, reporting options, and additional resources, visit the website: sarc.usc.edu

Office of Equity and Diversity (OED)/Title IX Compliance – (213) 740-5086
Works with faculty, staff, visitors, applicants, and students around issues of protected class. equity.usc.edu

Bias Assessment Response and Support
Incidents of bias, hate crimes and microaggressions need to be reported allowing for appropriate investigation and response. studentaffairs.usc.edu/bias-assessment-response-support

The Office of Disability Services and Programs
Provides certification for students with disabilities and helps arrange relevant accommodations. dsp.usc.edu

Student Support and Advocacy – (213) 821-4710
Assists students and families in resolving complex issues adversely affecting their success as a student EX: personal, financial, and academic. studentaffairs.usc.edu/ssa

Diversity at USC
Information on events, programs and training, the Diversity Task Force (including representatives for each school), chronology, participation, and various resources for students. diversity.usc.edu

USC Emergency Information
Provides safety and other updates, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible. emergency.usc.edu

USC Department of Public Safety – UPC: (213) 740-4321 – HSC: (323) 442-1000 – 24-hour emergency or to report a crime.
Provides overall safety to USC community. dps.usc.edu