USC Viterbi
School of Engineering
Information Technology Program

ITP 499: Advanced Ethical Hacking

Units: 4
Fall 2019
Day/Time: TH 3:30–5:20pm

Class Location: OHE 406

Instructor: Stefan McGregor
Office: OHE 412
Office Hours: See Blackboard (and always by appointment)
Contact Info: sjmcgreg@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

As hackers become more skilled and sophisticated, the onus falls on business owners to ensure that their cybersecurity systems can protect against threats. One of the most important tools that companies can use to defend themselves is to employ penetration testing in which a cybersecurity professional utilizes the same techniques as a criminal hacker to attempt to gain access to the companies' IT systems. These "ethical hackers" use any method that a criminal might use, such as password cracking, viruses or even social engineering approaches in this penetration testing.

Undoubtedly, the most valuable aspect of penetration testing is that it puts the cybersecurity of an IT infrastructure through the same stresses as a real hacking attempt and, therefore, exposes the weaknesses in the system. By having a controlled cybersecurity professional hack into the system means that, instead of learning the hard way through a costly real attack, the errors can be rectified before a malicious hacker attempts to get into the system.

A penetration test, or pen-test, reveals the security areas in which an enterprise must further invest, and provides an outside prespective on an organization's security. It is often the case that a business running its own in-house cybersecurity and computer systems never gets a second opinion of their effectiveness. Many business owners trust their IT professionals to deploy a strong system that is, insofar as is possible, free from weaknesses. Worrying statistics indicate that over 50 percent of small businesses suffer a cyber-attack and, of those that are attacked, as many as 60 percent go out of business within six months.

This course is designed to introduce students to advanced hacking techniques and tactics currently used in modern penetration testing and "red team" operations. The course focuses on hands-on exploitation of system and social engineering attack vectors. We will cover in depth all phases of penetration testing engagement: advanced attack infrastructure setup, user profiling and phishing, host enumeration, advanced lateral movement, sophisticated Active Directory domain enumeration and escalation, persistence (userland, elevated, and domain flavors), advanced Kerberos attacks, data mining, and exfiltration.

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:

- Use multiple information gathering techniques to identify and enumerate targets running various operating systems and services.
- Successfully analyze, correct, modify, cross-compile, and port public exploit code.
- Successfully conduct both remote and client side attacks.
- Accomplish advanced privilege escalation of Windows and Linux systems.
- Learn Active Directory domain privilege escalation tactics.
- Produce penetration testing and red-team reports

Prerequisite: ITP 325 or Instructor's consent;

Recommended Preparation: ITP 357, EE 450 or a willingness to learn networking quickly

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 Hacker Playbook 3: Practical Guide To Penetration Testing
Referred to in syllabus as **BHPT**

Peter Kim
ISBN: 1980901759
https://www.amazon.com/Hacker-Playbook-Practical-Penetration-Testing/dp/1980901759/ref=sr_1_1?keywords=the+hackers+playbook+3&qid=1554431294&s=gateway&sr=8-1

Red Team Field Manual
Referred to in syllabus as **RTFM**

Ben Clark
ISBN: 1494295504
https://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504/ref=sr_1_1?keywords=Rtfm%3A+Red+Team+Field+Manual&qid=1554431388&s=books&sr=1-1

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	80
Class Participation	5
Final Project	15
Total	100

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 a straight 90/80/70/60 scale. 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 that link. Do not email your assignments to the instructor, lab assistants, or graders. TurnItIn may be utilized for some assignments to detect plagiarism. 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 most likely result in failing 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.

Responses to emails sent to the lab assistants or graders will be 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.

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 499 - 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 – Linux Review and Fundamentals

- Linux boot process
- Linux files and directories
- Linux logs
- Advanced linux command usage

Lab/Homework

Lab 1 – Linux command line and Bash scripting

Reading

TBA

Week 2 – Windows Part 1: Review and Fundamentals

- Windows boot process
- Windows files and directories
- Windows command line

News Group

None

Lab/Homework

Lab 2 – Windows Command line

Reading

TBA

Week 3 – Windows Part 2: Enterprise

- Advanced Windows topics
- Active directory familirization
- Windows infrastructure
- PowerShell command line

Lab/Homework

Lab 3 – PowerShell command line lab

Reading

TBA

Week 4 – Tool Familirization

- Command and Control tools
- File transfer methods
- Scanning methods
- Advanced enumeration tools
- Initial access tools

Lab/Homework

Lab 4 – Tool familirization lab & Nessus

Reading

TBA

Week 5 – Social Engineering

- Social engineering introduction
- Different payloads
- Advanced social engineering tactics

Lab/Homework

Lab 5 – Social Engineering tools and toolkits

Reading

TBA

Week 6 – Exploitation, Part 1

- Understanding exploitation
- Review of exploitation from 125 and 325
- Buffer overflows

Lab/Homework

Lab 6 – Exploitation 1

Reading

TBA

Week 7 – Exploitation, Part 2

- Continuation of advanced exploitation
- Network exploitation
- User software exploitation

Lab/Homework

Lab 7 – Exploitation 2

Reading

TBA

Week 8 – Windows Privilege Escalation

- Introduction to windows privilege escalation
- Advanced Windows privilege escalation
- Mimikatz

Lab/Homework

Lab 8 – Windows privilege escalation

Reading

TBA

Week 9 – Linux Privilege Escalation

- Introduction to linux privilege escalation
- Advanced Linux privilege escalation
- Becoming root

Lab/Homework

Lab 9 – Linux privilege escalation

Reading Before Next Class

TBA

Week 10 – Post-Exploitation

- Persistance
- PowerShell Empire
- Cobalt Strike

Lab/Homework

Lab 10 – Post Exploitation lab

Reading Before Next Class

TBA

Week 11 – Domain Privilege Escalation, Part 1

- Introduction to domain privilege escalation
- Domain privilege escalation methods and techniques

Lab/Homework

Lab 11 – Domain privilege escalation lab 1

Reading Before Next Class

TBA

Week 12 – Domain Privilege Escalation, Part 2

- Advanced domain privilege escalation
- Advanced domain privilege escalation methods

Lab/Homework

Lab 12 – Domain privilege escalation lab 2

Reading Before Next Class

TBA

Week 13 – Command and Control Infrastructure

- Introduction to command and control infrastructure
- Setup redirectors & command and control servers

Lab/Homework

Lab 13 – Setup command and control infrastructure

Reading Before Next Class

TBA

Week 14 – Reporting & Scoping & Client Management

- Client management
- Scoping
- Reporting requirements
- Careers in Info Sec
- Certifications
- Conferences

Lab/Homework

Lab 14 – Create a sample report

Reading Before Next Class

TBA

Week 15 – Final Exercise

- Complete penetration testing engagement

Lab/Homework

Final Project

Reading Before Next Class

None

Final Project Description

The final project is due on the University-scheduled date of the final exam. It will consist of a full engagement as a penetration tester against a client enterprise network. Students will be required to apply all of the knowledge gained in the course to

1. Establish a scope for the project
2. Draft a penetration testing plan with multiple attack vectors
3. Successfully execute the penetration of the organization
4. Establish a persistency and foothold
5. Pivot to the objective data
6. Successfully exfiltrate the data
7. Write a penetration testing report
8. Present the report and findings to the client

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