USC
SCHOOL OF
ENGINEERING

Introduction to Ethical Hacking

ITP 325 (3 Units)

Description and Objective

Over the past 20 years, computer security has grown from an obscure concept to a daily news headline. On a seemingly daily basis, major news sources have stories about information security breaches, hacker break-ins, and identity thefts. Digital information is now among the most valuable assets to companies. Everything from patents, confidential company secrets, employee and customer information, even the financial data of the company is kept in a digital state. Once information started to become digital, a new type of criminal was born to steal this information: the hacker.

Today, criminal hacking has become one of the most profitable industries for organized crime. Due to profitability and low risk of computer crime, there is a need for effective training and education on the methodologies to secure these critical infrastructures. The best person to secure these critical infrastructures is an ethical hacker.

The ethical hacker is a person who is trained in the art of attacking computer infrastructure for the purposes of testing, auditing, and preemptively securing these infrastructures. The significant difference between the ethical hacker and the criminal hacker is that the ethical hacker is staying within the legal bounds of the region by being under a specific contract with the owner of the computer. The ethical hacker never attacks a system without permission. The ethical hacker follows a very strict code of ethics to maintain credibility.

This course is designed to introduce students to the fundamentals of ethical 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.

Concepts

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

Prerequisites/ Recommended Preparation	ITP 125x or instructor consent
Instructor	Joseph Greenfield
Contacting the Instructor	joseph.greenfield@usc.edu | 213-740-4604
Lecture/Lab	5:00 – 8:00, Wednesday, OHE 406
Required Textbooks	*Hacking Exposed Windows, Third Edition*. Joel Scambray, Stuart McClure. ISBN: 0-07-149426-X
Web Site	All course material will be on Blackboard at blackboard.usc.edu
Grading	Grading will be based on percentages earned in assignments. Students will have structured labs throughout the semester, to be conducted during the scheduled lab time. In addition, there will be a mid-semester project combining aspects of various portions of the labs. There will also be a final project to be completed in groups. Labs 50% Midterm Project 20% Final Project 30% Total 100%
Grading Scale	The following is the grading scale to be used for the final grades at the end of the semester 93% and above A 90% – 93% A- 87% – 90% B+ 83% – 87% B 80% – 83% B- 77% – 80% C+ 73% - 77% C 70% – 73% C- 67% – 70% D+ 63% – 67% D 60% – 63% D- Below 60% F
Policies	- Projects turned in after the deadline will automatically have 5% deducted per day. Projects will not be accepted after 1 week beyond the project’s deadline - No make-up exams (except for medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule. - It is your responsibility to submit your project on or before the due date. **It is not the responsibility of the lab assistant.** Do **not** turn in anything to your lab assistant!

	- All projects will be digitally submitted through blackboard except where specifically specified. Always keep a backup copy of your labs
Academic Integrity	The use of unauthorized material, communication with fellow students during an examination, attempting to benefit from the work of another student, and similar behavior that defeats the intent of an examination or other class work is unacceptable to the University. It is often difficult to distinguish between a culpable act and inadvertent behaviour resulting from the nervous tension accompanying examinations. When the professor determines that a violation has occurred, appropriate action, as determined by the instructor, will be taken. Although working together is encouraged, all work claimed as yours must in fact be your own effort. Students who plagiarize the work of other students will receive zero points and possibly be referred to Student Judicial Affairs and Community Standards (SJACS). All students should read, understand, and abide by the University Student Conduct Code listed in SCampus, and available at: http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html
Students with Disabilities	Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me (or to your TA) as early in the semester as possible. DSP is located in STU 301 and is open 8:30 a.m. - 5:00 p.m., Monday through Friday. The phone number for DSP is (213) 740-0776.

Introduction to Ethical Hacking

ITP 325 (3 Units)

Course Outline

Week 1 – Defining Ethical Hacking

- Course overview
- What is hacking
- Criminal hacking vs. Ethical hacking
- Review of hacker methodology
- Hackers in the 90s

Reading: Instructor Notes

Week 2 – Computer Laws and Hacker Ethics

- Overview of local, state, and federal computer crimes laws
- Ethical hackers code of ethics
- Overview of closed lab environment
- Media perception of hackers today

Reading: Instructor Handouts

Week 3 – Overview of Security Basics

- Security fundamentals
- Limitations and accountability
- Overview of different operating systems
- Review of networking fundamentals (TCP/IP and OSI)

Reading: Chapter 1 + Instructor Notes
Lab 1: Setting up the virtual machines for the lab

Week 4 – Windows From a Hacker's Perspective

- Windows 2000, XP, and Vista
- Users and Groups
- SIDs
- Access control lists (ACLs)
- Windows authentication
- Domains and workgroups
- Applications and services

Reading: Chapter 2
Lab 2: Setting up virtual servers

Week 5 – Footprinting and Scanning

- Dangers of search engines
- Port scanning
- Ping sweeps
- Banners and OS detection

Reading: Chapter 3
Lab 3: Port scanning

Week 6 – Enumeration

- Mapping the entire windows system
- Mapping the entire windows network
- Misconfigurations
- Active directory
- Detecting vulnerabilities in a system

Reading: Chapter 4
Lab 4: Enumerating windows systems

Week 7 – Hacking Windows Services

- Researching vulnerabilities
- Finding programs to exploit vulnerabilities
- Escalating attacks and "owning" systems

Reading: Chapter 5
Lab 5: Hacking a windows system

Week 8 – Midterm project preparation

- Assigning teams and roles
- Planning for the wargames simulation
- Prepping defense and attacks

Reading: Chapter 7

Week 9 – MIDTERM: WARGAMES

Week 10 – Escalation and Post Exploit Actions

- Transferring hacker toolkits
- Remote control and remote shells
- Password extraction
- Rootkits

Reading: Chapter 8
Lab 6: Cracking Windows Passwords

Week 11 – System Defense

- Patches and updates
- Local security policies
- Security templates
- Users and groups
- Defense software

Reading: Chapter 12 and Appendix A
Lab 7: Securing a windows workstation

Week 12 – Email, Viruses, and Worms

- E-mail threats
- Detecting phishing scams
- Trojans, Viruses and Worms
- Antivirus software

Reading: Instructor Notes
Lab 8: Spoofing e-mail

Week 13 – Vulnerability Assessment and Event Logs

- Vulnerability assessment tools
- Understanding automated reports
- Understanding event logs

Reading: Instructor Notes
Lab 9: Nessus

Week 14 – The Human Element

- Social Engineering 101
- Training personnel about security
- Interviewing and Interrogating

Reading: Instructor Notes
Final Projects assigned

Week 15 – Conclusion

- Conclusion to the course

FINAL PROJECTS ARE DUE ON THE DAY
OF THE SCHEDULED FINAL EXAM
Please see the schedule of classes for the exact date