## Objective
Upon completing this course, students will:
- Understand the fundamentals of information security
- Learn the basics of securing a workstation
- Understand basic networking and security technologies
- Understand the relationship between security and management
- Have a motivation to learn and improve their awareness and understanding of computers and security

## Concepts
This course is designed to be an introductory course in information and computer security. This course starts with an analysis of threats to information integrity. Students will then get an introduction to security mechanisms and policies. Students will learn how security infrastructure will integrate with the rest of the business and IT infrastructure, through the use of hands-on projects.

## Prerequisites/Recommended Preparation
None

## Instructor
Joseph Greenfield

## Contacting the Instructor
joseph.greenfield@usc.edu | 213-740-4604

## Office Hours
3:00 – 5:00 Monday
2:00 – 3:30 Tuesday & Thursday

## Office Location
OHE 412

## Lecture
5:00 – 6:20 Monday, OHE 406

## Lab
6:30 – 7:50 Monday, OHE 406

## Recommended Textbooks
CISSP All-in-One Exam Guide, 5th Edition
Shon Harris
ISBN: 0-07-1602178

## Web Site
All course material will be on Blackboard at blackboard.usc.edu

## Additional Resources
Think like a computer scientist (Python Resource):
http://openbookproject.net/thinkcs/python/english2e/

Beginners Guide to Python:
http://wiki.python.org/moin/BeginnersGuide
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, students will work in groups to prepare a 20-minute presentation on a topic of their choosing. The presentations will be conducted during the last few weeks of class.

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labs</td>
<td>30%</td>
</tr>
<tr>
<td>Presentation/Project</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm</td>
<td>15%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>25%</td>
</tr>
<tr>
<td>Participation</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

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 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 Information Security
ITP 125 (2 Units)

Course Outline

Week 1 – Introduction, Computer Security, Ethics
- Course overview
- What is a hacker?
- I’m being hacked!?!?
- Hacker methodology
- Ethics and Computer Law
Reading: Learning With Python, Chapters 1 & 2

Week 2 – HOLIDAY

Week 3 – Networking
- OSI 7-layer model
- Overview of networked systems
- Wireless and Wired networking
Reading: Learning With Python, Chapters 3 & 4

Week 4 – TCP/IP
- Modern networking
- TCP Ports
- Handshaking
Reading: Learning With Python, Chapters 5 & 6

Week 5 – Physical Security
- Mechanical security
- Surveillance systems
Reading: Learning With Python, Chapters 7 & 9

Week 6 – Operating Systems
- Processes
- Multitasking
- Memory management
- OS Architecture
- Client/Server Architecture
Reading: Chapter 24
Lab 5: Your First Hack!!!
**Week 7 – Hashing & Cryptography**
- One-way hashes
- Authentication
- Message digests
- Attacks on hashes
- PKI
**Reading:** Chapter 19

**Week 8 – Information Gathering**
- Google Hacks
- Information gathering techniques
- Searching
**Reading:** Chapter 20

**Week 9 – MIDTERM**

**Week 10 – Threats, Attacks and Exploits**
- Basic threat vectors
- Buffer overflows
- SQL injection
- Post-exploit access
**Reading:** TBA

**Week 11 – Social Engineering**
- Introduction to Social Engineering
- Phishing
- Human behavior and psychology
**Reading:** TBA

**Week 12 – Lockdown and Defense**
- Workstation security
- Server security
- Database security
- Perimeter defense
**Reading:** TBA

**Week 13 – Information Security and Policy Management**
- Information Security Policy
- AUPs
- Protecting the organization
**Reading:** TBA
**Week 14** – Incident Response
- Responding to being hacked
- Introduction to forensics
- Triage and containment

**Reading:**  TBA

**Week 15** – Conclusion
- Review for the final exam
- Conclusion to the course