Offensive Computer Security

CIS 5627, Spring 2018
Department of Computer Science, Florida State University

Class time and location

TBA

Instructor

- Instructor: Xiuwen Liu (pronounced as Shu-wen Lea-l)
- Email: liux@cs.fsu.edu (most effective way to contact me)
- Home page: http://www.cs.fsu.edu/~liux
- Office: 166 Love Building (LOV); Phone: (850) 644-0050
- Office Hours: TBA and by appointments.

Class Home Page

http://www.cs.fsu.edu/~liux/courses/offensivesec/index.html.
This web site contains the up-to-date information related to this class such as news, announcements, assignments, lecture notes, and useful links to resources that are helpful to this class. Besides the web pages, Blackboard will be used to communicate changes and updates and post grades for this class; in particular, I will send emails using email addresses in the Blackboard system and please make sure that your email address on record is current.

Rationale

With affordable desktop and laptop computers, large storage devices (e.g., hard drives), hardware, wide availability of the high speed internet connections, and more recently Internet-capable 3G and 4G smartphone and similar devices, the earth becomes highly connected that almost everyone can reach any other one on the planet as long as they are connected to the Internet. The unprecedented connectivity has unleaded unique potentials of computer technology (e.g., huge storage spaces and fast computing), leading to new services that were not imagined ten years ago. Not only our daily life activities heavily rely on the Internet, and government and the critical infrastructures we take for granted rely on the intended behaviors of computers and the underlying network. Unfortunately, the high connectivity has also created new problems, from spyware to steal data, computer viruses and worms to destroy data, to network-enabled weapons, to cyber wars that can disable companies and even countries (such as Stuxnet). All these problems are related to computer security. Due to its paramount importance, computer security is not just one academic research area. Many security products are installed on typical computers; in the United States, there are multiple federal agencies dedicated to computer security; the computer security is a multi-billion industry that is estimated to grow steadily (just click https://www.google.com/#q=computer+security+industry+growth and see). Computer security related issues have been widely recognized in software development companies. As computer security techniques evolve continuously along with product improvements and new service opportunities, computer security is and will remain to be an important and valuable area in the perceivable future with new career opportunities; in recent years, computer security has enjoyed a zero and low unemployment rate (see http://www.techjournal.org/2011/07/information-security-analysts-unemployment-rate-zero/ and http://www.bls.gov/oes/current/oes151122.htm). Due to the complexity of networked systems at typical organizations, securing such systems is much more than installing antivirus products, vulnerability scanning, and firewall and network parameter configurations; zero-day vulnerabilities and their exploitations render all existing antivirus products ineffective and active development of malicious cyber activities posts new threats constantly to the Internet and cyber space. To better secure systems against such attacks, offensive computer security, also called penetration testing, has evolved to be an effective way to evaluate and enhance the security of computer systems. Developing effective penetration testing is an exciting and challenging endeavor and can have a significant impact on the operations of companies by avoiding potentially costs due to cyber incidences.

Course Description

This course covers fundamental problems, principles, and techniques in offensive computer security, including various buffer overflow techniques (stack and heap overflow techniques), format string techniques, basic networking techniques, shellcode development (including port-binding shellcode, and connect-back shellcode), web application exploitation (via SQL injection, cross-site scripting), software reverse engineering, fuzzing techniques, social engineering techniques, and then commonly used tools for penetration testing with an emphasis on their principles and fundamental techniques. Additionally, as offensive computer security relies on many interdependent components, this course will also cover real world policy (legal) and implementation issues in penetration testing. It also involves opportunities to develop fully working exploitations by implementing and demonstrating such exploitations on virtual machines.

Prerequisites

CDA 3100 – Computer Organization I; have a good understanding of operating systems and computer networking models; have a good understanding of basic data types, data structures, function calls, and memory layout of programs; be able to read and understand C programs; be able to understand x86 assembly and write short x86 assembly programs; have a good understanding of basic encryption algorithms, hashing algorithms, and a general understanding of computer security.

Course Objectives

Upon successful completion of this course of study, the student will be able to:

- Identify common buffer overflow vulnerabilities
- Exploit stack buffer overflow vulnerabilities
- Identify common format string vulnerabilities
- Exploit common format string vulnerabilities
- Write shell-spawning shellcode
- Write port-binding shellcode
- Write connect-back shellcode
- Reverse engineer x86 binaries
- Perform fuzzing to identify vulnerabilities
- Develop social engineering techniques
- Identify SQL injection vulnerabilities
- Exploit SQL injection vulnerabilities
- Identify cross-site scripting vulnerabilities
- Exploit cross-site scripting vulnerabilities
- Identify web application vulnerabilities
- Exploit web application vulnerabilities
- Effectively report and communicate the flaws

- Incorporate new offensive techniques documented in research papers
- Conduct penetration testing

Textbook and Course Materials

Required textbooks: "Hacking: The Art of Exploitation, 2nd Edition" by Jon Erickson**;** this is the main textbook. **"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"** by Dafydd Stuttard and Marcus Pinto**;** we will mainly cover several chapters from this book (mainly Chapters 2, 3, 7, 9, and 12).

In addition to the textbooks, papers and notes from the literature will be distributed along the lectures.

Student Responsibilities

Attendance is required for this class. Unless you obtain prior consent of the instructor, missing classes will be used as bases for attendance grading. Excused absences include documented illness, deaths in the family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. These absences will be accommodated in a way that does not arbitrarily penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness. In case that it is necessary to skip a class, students are responsible to make up missed materials. Participation in in-class discussions and activities is also required. All submitted assignments and projects must be done by the author(s). It is a violation of the Academic Honor Code to submit other's work and the instructor of this course takes the violations very seriously.

University Attendance Policy - Excused absences include documented illness, deaths in the family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. These absences will be accommodated in a way that does not arbitrarily penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

As this course will cover certain techniques to break down known systems in order to demonstrate their vulnerabilities, it is **illegal**, however, to practice these techniques on others' systems. The students will be liable for their behaviors and therefore consequences.

Assignments and Projects

About six homework assignments will be given along the lectures and they need to be done individually and turned in. There will be hands-on projects, where the full exploitation cycles must be implemented and demonstrated in virtual machine environments. There will be a midterm exam and a final exam.

Grading Policy

Grades will be determined as follows:

Assignment	Points	Assignment	Points
Class Attendance & Participation	10 %	Midterm Exam	15 %
Homework Assignments	30 %	Hands-on Project	10 %

Research Paper Reading Assignment	5 %	Term Project	10%
Final Exam (cumulative)	20 %		

Grading will be based on the weighted average as specified above and the following scale will be used (S is the weighted average on a 100-point scale):

Score	Grade	Score	Grade	Score	Grade
$93 \le S$	A	$80 \le S < 83$	B-	$67 \le S < 70$	D+
$90 \le S < 93$	A-	$77 \le S < 80$	C+	$63 \le S < 67$	D
$87 \le S < 90$	B+	$73 \le S < 77$	C	$60 \le S < 63$	D-
$83 \le S < 87$	B	$70 \le S < 73$	C-	$S < 60$	F

Late Penalties

Assignments are due at the beginning of the class on the due date. Assignments turned in late, but before the beginning of the next scheduled class will be penalized by 10 %. Assignments that are more than one class period late will **NOT** be accepted.

Submission and Return Policy

All tests/assignments/projects/homework will be returned as soon as possible after grading but no later than two weeks from the due date.

Tentative Schedule

Here **Art** refers to the "Hacking: The Art of Exploitation" and **Web** refers to the "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws".

- Week 1: Introduction (**Art**: Chapter 0x100 and other sources)
  - General introduction to offensive computer security, penetration testing, and hacking
  - Steps in penetration testing and offensive computer security (see http://www.pentest-standard.org/index.php/Main_Page)
  - Fundamental principles and techniques to exploitation development
- Week 2: C programs: vulnerabilities (**Art**: Chapter 0x200)
- Weeks 3-4: General vulnerabilities and exploitations (**Art**: Chapter 0x300)
- Week 5: Networking (**Art**: Chapter 0x400)
- Weeks 6-7: X86 assembly programing and reverse engineering (**Art**: Chapter 0x500)
- Week 8: Shellcode development (**Art**: Chapter 0x500)
- Week 9: Midterm exam
- Weeks 10-11: Web application exploitation (**Web**: Chapters 2, 3, 8, 9, 10, 12, and 13)
- Week 12: Fuzzing and social engineering (from the literature and other sources)
- Week 13: Post Exploitation (**Art:** Chapter 0x600)
- Week 14: Case studies of exploitation tools (from the literature and other sources)
- Week 15: Summary and physical security (locking picking)
- Week 16: Final exam (cumulative)

Academic Honor Code

The Florida State University Academic Honor Policy outlines the University's expectations for the integrity of students' academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process. Students are responsible for reading the Academic Honor Policy and for living up to their pledge to "...be honest and truthful and...[to] strive for personal and institutional integrity at Florida State University." (Florida State University Academic Honor Policy, found at http://fda.fsu.edu/academic-resources/academic-integrity-and-grievances/academic-honor-policy.)

Assignments/projects/exams are to be done individually, unless specified otherwise. It is a violation of the Academic Honor Code to take credit for the work done by other people. It is also a violation to assist another person in violating the Code (See the FSU Student Handbook for penalties for violations of the Honor Code). The judgment for the violation of the Academic Honor Code will be done by the instructor and a third party member (another faculty member in the Computer Science Department not involved in this course). Once the judgment is made, the case is closed and no arguments from the involved parties will be heard. Examples of cheating behaviors include:

- Discuss the solution for a homework question.
- Copy programs for programming assignments.
- Use and submit existing programs/reports on the world wide web as written assignments.
- Submit programs/reports/assignments done by a third party, including hired and contracted.
- Plagiarize sentences/paragraphs from others without giving the appropriate references. Plagiarism is a serious intellectual crime and the consequences can be very substantial.

Penalty for violating the Academic Honor Code: A 0 grade for the particular assignment /exam and a reduction of one letter grade in the final grade for all parties involved for each occurrence. A report will be sent to the department chairman for further administrative actions.

Americans With Disabilities Act

Students with disabilities needing academic accommodation should: (1) register with and provide documentation to the Student Disability Resource Center; and (2) bring a letter to the instructor indicating the need for accommodation and what type. Please note that instructors are not allowed to provide classroom accommodation to a student until appropriate verification from the Student Disability Resource Center has been provided. This syllabus and other class materials are available in alternative format upon request.

For more information about services available to FSU students with disabilities, contact the:

Student Disability Resource Center
874 Traditions Way
108 Student Services Building
Florida State University
Tallahassee, FL 32306-4167
(850) 644-9566 (voice)
(850) 644-8504 (TDD)
sdrc@admin.fsu.edu
http://www.disabilitycenter.fsu.edu/

Additional Information

Free Tutoring from FSU - On-campus tutoring and writing assistance is available for many courses at Florida State University. For more information, visit the Academic Center for Excellence (ACE) Tutoring Services' comprehensive list of on-campus tutoring options at http://ace.fsu.edu/tutoring or contact tutor@fsu.edu. High-quality tutoring is available by appointment and on a walk-in basis. These services are offered by tutors trained to encourage the highest level of individual academic success while upholding personal academic integrity.

Syllabus Change Policy: Except for changes that substantially affect implementation of the evaluation (grading) statement, this syllabus is a guide for the course and is subject to change with