Introduction to Practical Cyber Operations Fundamentals

CIS 4930/CIS 5930, Spring 2020

Department of Computer Science, Florida State University

Class time and location

Tuesday, Thursday 2:00-3:15pm, Room 151, Love Building.

Instructors

- Coordinator: Mike Burmester, Email: burmester@cs.fsu.edu
- Instructors:
  - Dr Xiuwen Liu liux@cs.fsu.edu
  - Logan Anderson lja16@my.fsu.edu()
  - Nicholas Meier nlm15@my.fsu.edu ()
  - Dillon Prendergast djp15@my.fsu.edu()
- Office: 268 Love Building (LOV); Phone: (850) 644-6410
- Office Hours: Burmester: Monday and Wednesday, 1:45-2:30pm, and by appointment. Anderson/Meier/Prendergast: Day: Time: Place

Class Home Page

www.cs.fsu.edu/~burmeste/pcs.htm

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, we will send emails using email addresses in the Blackboard system and please make sure that your email address on record is current.

Rationale

Computers and communication technologies have been incorporated into many applications and have fundamentally changed many aspects of the human activities. Unfortunately, the changes have 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. 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. Due to the proactive nature of hackers and malicious users and weak links in securing systems (such as phishing email and social engineering attacks target unsuspecting users), it is unavoidable that some computers will be infected by malware and some will be infiltrated and compromised; according to a new study, 38.3% of all users were attacked while their owners were online and in total, 23% of all computers were attacked at least once in 2014. When such activities are sensed, cyber security professionals must act quickly and accurately as shut downing all the servers can affect many normal users while not stopping cyber-attacks as early as possible

can have serious consequences in terms of data and other losses. Furthermore, nullifying such attacks can involve many practical cyber security skills that are not covered in security courses. In addition, to prevent such attacks, one may have to understand offensive techniques used by malicious groups. This course is designed to cover the basic principles and techniques for solving cyber-attacks, covering cryptography, web, binary reversing, binary exploitation, forensics, and firmware analysis with the emphasis on practical skill development and problem solving in the context of the cyber Catch-The-Flag (CTF) competitions so that you can develop the skills and techniques that are ready to be used.

Course Description

This course covers fundamental problems, principles, and practical problem solving techniques in cryptography, web, binary reversing, binary exploitation, forensics, and firmware analysis; many of the techniques will be demonstrated and practiced using commonly used and customized tools using Python. It also involves opportunities to solve new CTF challenges and develop new tools to help solve such problems.

Prerequisites

CDA 3100 – Computer Organization I; having a good understanding of instruction set architectures (registers, instruction encoding and decoding, and memory organization) and basic data types, data structures, function calls (calling conventions), and memory layout of programs; be able to understand x86 and other assembly (assuming that instruction reference manuals are available); having a general understanding of computer security; familiarity with the UNIX environment.

Course Objectives

Upon successful completion of this course of study, the student will gain proficiency in:

- Recognizing common weaknesses in implementations of cryptographic algorithms
- Performing cryptanalysis of substitution and commonly used ciphers
- Identifying common web application vulnerabilities
- Utilizing SQL injection to exploit vulnerable web applications
- Analyzing binary programs in x86

- Identifying and exploiting buffer overflow vulnerabilities in binary executables
- Identifying and exploiting string format vulnerabilities in binary executables
- Developing and using shellcode as a binary exploitation technique
- Developing scripts in Python for solving various cybersecurity problems
- Analyzing common file formats (ELF, PE, and PDF files)
- Recovering hidden or deleted information from disk images

Textbook and Course Materials

There is no required textbook for this course and we will provide lecture slides, written notes, and worked out examples from previous relevant CTF competitions. The following books can be helpful to understand some of the basic concepts thoroughly.

Recommended reading: "Hacking: The Art of Exploitation, 2nd Edition" by Jon Erickson**:** this is a book with accurate and detailed descriptions and commands of common vulnerabilities and corresponding exploits. It is an excellent book for understanding buffer overflow vulnerabilities, string format vulnerabilities, and shellcode, and other exploitation development.

"**The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws**" by Dafydd Stuttard and Marcus Pinto. The book provides a comprehensive and thorough coverage of web security mechanisms, and web vulnerabilities.

"**Information Security**," 2nd Edition, (ISBN 978-0-470-62639-9), Wiley, 2011, by Mark Stamp. The book provides a good coverage on commonly used cryptographic algorithms and cryptanalysis techniques, and security protocols.

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

Student Responsibilities

Attendance is required for this class. Unless you obtain prior consent of the instructors, 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.

As this course will cover certain techniques to exploit and 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 ten homework assignments (most of them involve solving CTF problems) will be given along the lectures and they need to be done individually and turned in. There will be a CTF competition-style final in the last week of the classes and the write-ups are due during the final exam week.

Grading Policy

Grades will be determined as follows:

Assignment	Points	Assignment	Points
Assignments	65 %	Term Project	10%
Practice CTF	10 %	Final CTF	15 %

Two of the submitted assignments with the lowest grade will be dropped.
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
$93 \leq S$	A	$80 \leq S < 83$	B-	$67 \leq S < 70$	D+
$90 \leq S < 93$	A-	$77 \leq S < 80$	C+	$63 \leq S < 67$	D
$87 \leq S < 90$	B+	$73 \leq S < 77$	C	$60 \leq S < 63$	D-
$83 \leq S < 87$	B	$70 \leq S < 73$	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

- **Week 1: Introduction to CTF / Python**
  - Fundamentals
    - Course structure, Linux environment, virtual machines, example CTF challenges and write-ups, basic Python
- **Week 2: Introduction to Python programming for CTF**
  - Fundamentals
    - Overview of practical cyber security skills, Python programming examples for solving practical cyber problems
    - Python programming for networking and other manipulations, Case studies of selected CTF competitions
  - Practice
    - Overview of problems from CTF competitions
    - Python programming examples for solving practical cyber problems
- **Week 3: Web exploitation I**
  - Fundamentals
    - Web security fundamentals
  - Practice
    - Web security problems from CTF competition archives
- **Week 4: Web exploitation II**
  - Fundamentals
    - Common vulnerabilities and attacks on web applications, SQL injection, cross-site scripting
  - Practice
    - Common web vulnerabilities from CTF competition archives
- **Week 5: Forensics I**
  - Fundamentals
    - Encodings, File formats, and File Carving
    - Memory Forensics on Windows and Linux
    - Volatility & Sleuthkit
    - Passwords & Password Cracking
  - Practice
    - In-Class examples & Forensics problems from CTF competitions
- **Week 6: Forensics II**
  - Fundamentals
    - Steganography
    - Network Forensics
    - Wireless
    - OSINT
  - Practice
    - In-Class examples & Advanced Forensics problems from CTF competition archives
- **Week 7: C Basics I**

- Fundamentals
  - Program structure, Basic data types, Variable types, Operator types, control statements, input and output pointing to data, using functions, play with strings.
- Practice
  - Examples and exercises. C-Built-in Functions, C-Useful resources.

• Week 8: C Basics II / Reverse engineering I

- Fundamentals
  - Structured data types, working with files, bits manipulation, pre-processors
  - Binary program reversing in x86
- Practice
  - Examples and exercises.
  - Binary program analysis problems from CTF competition archives

• Week 9: Reverse engineering II

- Fundamentals
  - Advanced reversing techniques and dynamic analysis
- Practice
  - Reversing problems from CTF competition archives

• Week 10: Binary Exploitation I

- Fundamentals
  - Buffer overflow vulnerability exploitation
  - String format vulnerability exploitation
- Practice
  - Buffer overflow exploitation problems from CTF competition archives
  - String format exploitation problems from CTF competition archives

• Week 11: Spring break; no class

• Week 12: Binary Exploitation II

- Fundamentals
  - Advanced Stack-based exploitation, Shellcode
- Practice
  - Shellcode problems from CTF competition archives
  - Pwntools usage examples from CTF competition archives

• Week 13: Cryptography I

- Fundamentals
  - Substitution cipher, one-pad cipher, symmetric key encryption, and cryptanalysis
- Practice
  - Substitution and symmetric key encryption problems from CTF competition archives

• Week 14: Cryptography II

- Fundamentals
  - Public key encryption, hashing, and cryptography algorithms in applications and protocols
- Practice
  - Public key encryption, hashing, and secure protocol problems from CTF competition archives

• Week 15: Practice CTF

- **Week 16: Final CTF Competition**
  - The final CTF competition is scheduled from 3:15pm, April 16th to 2:00pm, April 23rd, 2018.
  - You must be available during that weekend to participate in the final CTF competition that counts as the final exam for this class even though the write-ups are due by the scheduled final exam time.
  - Fundamentals
    - Solving CTF problems
  - Practice
    - Solving CTF problems
- **Final Exam Week**
  - Final CTF write-ups due, Thursday, April 30th, 9:30am

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/Academics/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.

Accommodation for Disabilities

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. This should be done during the first week of class. 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 advance notice.
