Introduction to Practical Cyber OperaTions Fundamentals

CIS 4930, Spring 2025
Department of Computer Science, Florida State University

Class time and location

Tuesday, Thursday 4:50-6:05pm, Room 2401, Health and Wellness Center (HWC).

Instructor and Supporting Team

- Instructor
  - Dr. Xiuwen Liu
  - Email: liux@cs.fsu.edu (most effective way to contact me; starting the subject line with "CTFSp25:" to be properly sorted and searched)
- Supporting team members
  - They will present and share how they solve CTF challenges
- **Offices**: 332A Love Building (LOV); Phone: (850) 644-0050
- **Office Hours:** Xiuwen Liu: Tuesday and Thursday, 3:00-4:00pm, and by appointments. In case that I am not in my office during my office hours, please look for me in 352 LOV.

Class Home Page

The class uses the Canvas as the web site; it contains the up-to-date information related to this class such as news, announcements, email communications, assignments, lecture notes, and useful links to resources that are helpful to this class.

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 last year. 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 security challenges, covering cryptography, web, binary reversing,

binary exploitation, forensics, and selected topics 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 selected topics; many of the techniques will be demonstrated and practiced using commonly used and customized tools using Python. It also involves solving new CTF challenges and develop new tools to help solve such problems.

Prerequisites

CDA 3100 – Computer Organization I and COP 3330 - Data Structures, Algorithms, and Generic Programming I Highly recommended; 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 web technologies and applications; having a general understanding of computer security and web security; familiarity with the UNIX environment; proficient in programming and being able to learn how to program in Python and use tools quickly.

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
- 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)

Textbook and Course Materials

There are no required textbooks for this course, and we will provide lecture slides, written notes, and worked out examples from previous relevant CTF competitions. However, the following books can be helpful for understanding some of the basic concepts more 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. The related web site, https://portswigger.net/web-security, is a great resource to learn updated web security vulnerabilities and exploits.

"**Information Security: Principles and Practice," 3rd Edition,** by Mark Stamp; the book provides a good coverage on commonly used cryptographic algorithms and cryptanalysis techniques, and security protocols.

"Computer Security: A Hands-on Approach," by Wenliang Du (3rd Edition; ISBN: 978-17330039-5-7); 2nd Edition (ISBN: 978-1733003902)); the book centered around hands-on labs and it is very helpful to learn the concepts and fundamentals. The labs and slides are available from https://seedsecuritylabs.org.

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

Student Responsibilities

Attendance is required for this class. In case that it is necessary to skip a class, a student is required to notify the instructor beforehand; the absence is excused if it is allowed by the University Attendance Policy (see below). In both excused and unexcused cases, the students are responsible for making 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 (see below) 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 exploit and break down known systems to demonstrate their vulnerabilities, it is **illegal**, however, to practice these techniques on systems where permission has not been granted. 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 an in-person practice CTF (up to two members on a team) on April 19th, 2025 from 9:00am to 1:00pm. 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
Homework Assignments	50 %	Practice CTF	15 %
Final CTF	25 %	Paper Reading Assignment - How AI Tools Can Solve CTF Problems.	10%

Two of the homework assignments with the lowest grades 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 / Security Fundamentals

- Class organizations
- Fundamentals
  - Course structure, Linux environment, virtual machines, example CTF challenges and write-ups, basic files, binaries, data structures, dynamic approaches to identifying important information.

• 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: Reverse engineering I**
  - Fundamentals
    - Binary program reversing in x86 and x64
  - Practice
    - Examples and exercises.
    - Binary program analysis problems from CTF competition archives
- **Week 8: Reverse engineering II**
  - Fundamentals
    - Advanced reversing techniques and dynamic analysis
  - Practice
    - Reversing problems from CTF competition archives
- **Week 9: 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
- **Spring Break Week - March 10th to March 14th; no classes**
  - CMU live picoCTF Competition starts in March, 2025
    - Registrations open on February 1st, 2025 and close on March 13th, 2025
    - Live Competition from March 7th 2025 at 12:00pm ET to March 17th, 2025 at 3:00pm ET.

- **Week 10: Binary Exploitation II**
  - Fundamentals

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

- **Week 11: Cryptography I**
  - Fundamentals
    - Substitution cipher, one-pad cipher, symmetric key encryption, and cryptanalysis
  - Practice
    - Substitution and symmetric key encryption problems from CTF competition archives
  - The live CMU picoCTF Competition ends in March, 2025
- **Week 12: 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 13**: Emerging CTF Challenges
  - Fundamentals
    - GPT4
    - AI tools for solving CTF problems
  - Practice
    - Go over how to solve related challenges
- **Week 14**: Common CTF problem solving strategies
  - Fundamentals
    - Common strategies and algorithms
  - Practice
    - Examples

- **Practice CTF**
  - Individuals or groups of two members
  - Live, in-person competition on April 19th, 2025 from 9:00am to 1:00pm in LOV 307 and nearby classrooms
    - Open to others not in this class

- **Week 15: Final CTF Competition**
  - The final CTF competition is scheduled from 4:50pm on April 22md to 6:05pm on April 24th, 2025.
  - You must be available to participate in the final CTF competition that counts as the final exam for this class even though the write-ups are due at 5:00pm, Friday, May 2nd, 2025.
  - Fundamentals
    - Solving CTF problems
  - Practice
    - Solving CTF problems
- **Final Exam Week**
  - Final CTF write-ups due at 5:00pm, Friday, May 2nd, 2025

- Paper reading assignment, due at 5:00pm, Friday, May 2nd, 2025

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-integrityand-grievances/academic-honor-policy.)

Assignments/projects/exams are to be done individually and the team members and submissions must be the work of the authors. 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:

- Discussing the solution for a homework question.
- Copying programs for programming assignments.
- Using and submitting existing programs/reports on the World Wide Web as written assignments.
- Submitting programs/reports/assignments done by a third party, including hired and contracted.
- Plagiarizing 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 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 advance notice.