Offensive Computer Security (CIS4930 / CIS5930)

Spring 2014

Class time and location:
Monday Wednesday (Will never meet Friday) from 3:35PM - 4:50 PM
in room HCB 0216. *However, most classes will be virtual (i.e. hosted online).*

Instructors:

Instructor: W. Owen Redwood
Email: redwood@cs.fsu.edu (most effective way to contact me).
Home page: http://ww2.cs.fsu.edu/~redwood/
Office: 010 Love Building (LOV)

Instructor: Professor 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.

Teaching Assistant: Abdullah Raiaan
Email: raiaan@cs.fsu.edu
Office: 100A Carrouthers (MCH).
Office Hours (tennatively): Tuesday / Thursdays 4PM-5PM.

Class Home Page:
http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/
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:
The primary incentive for an attacker to exploit a vulnerability, or series of vulnerabilities is to achieve a return on an investment (his/her time usually). This return need not be strictly monetary—an attacker may be interested in obtaining access to data, identities, or some other commodity that is valuable to them. The field of penetration testing involves authorized auditing and exploitation of systems to assess actual system security in order to protect against attackers. This requires thorough knowledge of vulnerabilities and how to exploit them. Thus, this course provides an introductory but comprehensive coverage of the fundamental methodologies, skills, legal issues, and tools used in white hat penetration testing and secure system administration.

Required Textbooks:

1. Erickson, Jon. "Hacking: The Art of Exploitation, 2nd Edition"
2. Stuttard, Dafydd; Pinto, Marcus. "The Web Application Hacker's Handbook, 2nd Edition".

Suggested Textbooks:

The following textbooks are suggested for any student who seeks advanced resources to supplement the knowledge presented in this course:

Sikorski, Michael. "Practical Malware Analysis".
Kozoil, Jack. "The Shellcoder's Handbook: Discovering and Exploiting Security Holes".
Seacord, Robert C. "Secure Coding in C and C++, Second Edition".

Prerequisites:

This is a *highly* technical class. We expect students to have a strong technical background before taking this course. Students who have not taken a security class before or whom are otherwise unfamiliar with computer security will not be able to complete this class. Specifically, students should satisfy at least **two** of the following:

1) Assembly code (Intel X86 preferred)
2) Knowledge of Computer Security basics
   For undergraduates (at least CIS 4360 or CNT4406)
   For graduates (at least CIS5370, CNT5412, CNT5415, or CIS 5371)
3) Familiarity with operating system kernel/internals (windows or linux)
4) Familiarity with command line operation of Windows AND Linux

Course Objectives:

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

- Have found their own 0-day vulnerability and ethically disclosed it.
- Know how to identify software flaws discovered through binary and source code auditing
- Know how to reverse engineer x86 binaries
- Know how to exploit software flaws (such as injection flaws, buffer overflows)
- Know how to perform network and host enumeration, as well as OS and service fingerprinting
- Know how to perform network vulnerability analysis, penetration and post exploitation
- Know how to effectively report and communicate all of the above flaws

Grading:

All homework, projects, and assignments are individual work only. No collaboration is allowed. Discussion of material is encouraged, but discussion of answers is prohibited.

- Homeworks: 55%
- Midterms: 30%
- Final Exam: 15%

This class will involve regular homeworks that will assess the student's knowledge of materials on a weekly basis. Homeworks will often expose students to tools related to subjects, and require the student to use the tools to solve problems. Sometimes they can be small projects. If students do not have access to personal computers that can run the tools, then access to the SAIT security lab will be provided.

Extra Credit:
1) Involvement in CTF's (see https://ctftime.org/ for a CTF schedule)

Calendar:

Red text indicates required reading for the lecture. Orange text indicates supplemental material that has been handpicked for additional understanding, but will not be tested upon. ***HAOE refers to the textbook Hacking:the Art of Exploitation, and WAHH refers to the textook The Web Applications Hacker's Handbook****. Below is the proposed course calendar, but note that it is subject to change:*

Week 1 (Jan 6,8) Overview Week 1:

Jan 6: Introduction lecture (ethics and overview)
- Reading: 0x200 up to 0x260 (HAOE)

Jan 8: Essential C Security 101
What you absolutely need to know about secure coding in C. C is everywhere.
- Reading: 0x260 up to 0x280 (HAOE)

Homework 1: Basics

Week 2 (Jan 13, 15) Overview Week 2: C and Code Auditing

Jan 13: Essential C Security 102
- Reading: 0x280 up to 0x300 (HAOE) and 0x350 up to 0x400

Jan 15: Code Auditing
- Read https://gist.github.com/neuromancer/a53891db0ac199f43a1a/

Homework 2: Code Auditing

Week 3 (Jan 20, 22) Overview Week 2: Permissions and *Intro to Vulnerability Research*

Jan 20:Holiday - No class

Jan 22: The Permissions Spectrum; Windows / Linux & Rootkits / Intro to Vulnerability Research
Basics to an OS, Kernel vs user space, system calls, unix permissions, ruid vs euid etc…

- No reading assigned

Homework 3: Permissions, Windows, Linux, Rootkits questions (tennative)

Week 4 (Jan 27, 29): Reverse Engineering Workshop Week

Jan 27: Guest Lecturer: Mitch Adair on Reverse Engineering

- Read Chapter 1 from "Reversing: Secrets of Reverse Engineering". Read via the preview feature on amazon: http://www.amazon.com/Reversing-Secrets-Engineering-Eldad-Eilam/dp/0764574817

Supplementary video: "Primer on Assembly" http://www.securitytube.net/video/208

Jan 29: Guest Lecturer: Mitch Adair on Reverse Engineering (Continued)

- No reading assigned

Read "**Constant Insecurity**: Things you didn't know about Portable Excutable File Format", 2011 Blackhat presentation by Mario Vuksan & Tomislav Pericin (Reversing Labs):http://www.reversinglabs.com/sites/default/files/pictures/PECOFF_BlackHat-USA-11-Slides.pdf

Homework 4: Reverse Engineering

Week 5 (Feb 3, 5): Fuzzing Week

Feb 3: Fuzzing 101
Automated software testing, software exploration, and bug hunting.

- Read: Differential Testing for Software (http://www.cs.dartmouth.edu/~mckeeman/references/DifferentialTestingForSoftware.pdf)
- Read Adaptive Random Testing (http://www.utdallas.edu/~ewong/SYSM-6310/03-Lecture/02-ART-paper-01.pdf)
- Read: Attaching the Rocket to the Chainsaw https://www.cert.org/blogs/certcc/2013/09/putting_the_rocket_on_the_chai.html

Feb 5: Exam #1 Review

Exam 1 will cover all topics up to and including Fuzzing

Week 6 (Feb 10, 12) MIDTERM #1 and Exploit Development

Feb 10: MIDTERM EXAM #1

Feb 12: Exploitation Development 101
Fuzzing overview, environment variables, stack attacks, buffer overflow, nop-sleds

- Read 0x300 up to 0x340 in HAOE

Homework 5: Fuzzing & Exploitation development related

Week 7 (Feb 17, 19) Exploit Development

Feb 17: Exploitation Development 102
Writing Shellcode (linux),
DEP, N^X, ASLR, Stack (/GS) cookies
Ways attackers can bypass executable security mechanisms

- Read 0x500 up to 0x540 in HAOE (Writing shellcode)
- Read 0x6A0 up to 0x700 in HAOE

<This class got delayed to Feb 24. Schedule needs to be updated!!>Feb 19: Exploitation Development 103
Advanced Techniques, Polymorphic shellcode,

- Read 0x680 up to 0x6A0 in HAOE

Homework 6: Exploit homework

Week 8 (Feb 24, 26): Networking

Feb 24: Networking 101
Wireshark, Nmap, nc, Hubs vs switches vs routers, manufacturer default logins / backdoors... ARP & dns (dnssec), proxies, weak IP vs strong IP model (RFC 1122)

- Read: 0x400 up to 0x450 in HAOE
- Supplementary video: Hacking Routers http://www.youtube.com/watch?v=Zazk0plSoQg&feature=relmfu

Feb 26: Networking 102
Wrapping up essential networking concepts

- Read 0x450 up to 0x500 (HAOE) (27 pages)
- Read 0x540 through 0x550 (HAOE) (11 pages)
- Read Chapter 1 (WAHH) (15 pages)
- **Homework 7: Networking Questions**

Week 9 (March 3, 5): Web Application Hacking Week

March 3: Web Hacking 101:
We begin our coverage of web application security, architecture, common vulnerabilities, and attack techniques

- Reading: Chapters 2-3 of WAHH
- Reading: Open Web Application Security Project (OWASP) Top 10 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Related Reading: PHP A Fractal of Bad Design http://me.veekun.com/blog/2012/04/09/php-a-fractal-of-bad-design/

March 5: Web Hacking 102:
Web application hacking continued

- Reading: Chapters 9 of WAHH
- Related video (Advanced SQLi): http://www.youtube.com/watch?v=rdyQoUNeXSg&feature=relmfu

Homework 8: SQLi / XSS exploitation

Week 10 (March 12, 14)

SPRING BREAK (No Class this week**)**

Week 11 (March 17, 19):

March 17: Web Hacking 103:
SSL, The flaws of the certificate authority infrastructure, CA breaches / history, trust agility [convergence], and SSL Strip [http://www.thoughtcrime.org/software/sslstrip/].

- Read Chapter 10 in WAHH
- Related Video: https://www.youtube.com/watch?v=Z7Wl2FW2TcA ([black hat] SSL and the future of Authenticity).
- Related Video: https://www.youtube.com/watch?v=lt7uW6vDk00 Whitfield Diffie and Moxie Marlinspike talk about certificate authorities, DNSSEC, SSL, dane, trust agility, and etc.

March 19: Web Hacking 104 / Exploitation 104
IDS / IPS ,Web Application Firewalls. Connect back shellcode. Encoded / Polymorphic shellcode

- Read Chapter 12 in WAHH
- Read 0x550 in HAOE
- Related Video (IDS/IPS Detection, Evasion, VOIP hacking): http://www.youtube.com/watch?v=tJsNu0VRKYY&feature=related

---

Week 12 (March 24, 26) Advanced Exploitation Topics

March 24: Guest Lecturer: Jordan Wiens on JIT Exploitation
Coverage of JIT Exploitation techniques and mitigations.

- Read Chapter 13 in WAHH

March 26: Midterm #2 Review / Intro to ROP
Return Oriented Programming (ROP) Chains

- **Reading: The ROPC (part 1) blog post here: http://gdtr.wordpress.com/2013/12/13/ropc-turing-complete-rop-compiler-part-1/**

Week 13 (March 31, April 2) Advanced Exploitation & Midterm2

March 31: Guest Lecturer: Devin Cook on Return Oriented Programming

- **Reading: The ROPC (part 2) blog post here:**
- **http://gdtr.wordpress.com/2014/01/01/ropc-turing-complete-rop-compiler-part-2-language/**

April 2nd: MIDTERM EXAM #2

Homework 9: ROP exercises

Week 14 (April 7, 9) Start of special topics

April 7: Metasploit, Armitage & Cortana

-Now we learn how to use the tools.

- **Related Resource: Metasploit Megaprimer http://www.securitytube.net/groups?operation=view&groupId=10**

April 9: Post Exploitation 101 (Meterpreter):
-Coverage of post-exploitation activity

- Read 0x640 up to 0x670 in HAOE (log files through advanced camouflage),
- Related Video (post exploitation): Tactical Post Exploitation by Carlos Perez https://www.youtube.com/watch?v=gNUhK6G8EQ4
- Related video: Covert Post Exploitation https://www.youtube.com/watch?v=PTYYlHYBF0Q&feature=related

---

Week 15 (April 14, 16)

April 14: Forensics and Incident Response
-Using Volatility to inspect intrusion activity.

April 16: Advanced Malware Techniques: - Xiuwen
-Packers, red pills, blue pills, rootkits, anti reverse engineering/debugging, and binary patching

Homework 10: Volatility

Week 16 (April 21, 23)

April 21: Physical Security Assessment
Lockpicking (hands on), physical-access attacks, physical emanation security, and shielding, and biometrics.

April 23: Social Engineering

Week 17 (April 28 - May 2)

Final Exam Week

May 6: Grades Due & Available Online

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 Academic Honor Policy, found at http://dof.fsu.edu/honorpolicy.htm)

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/ quiz/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 accommodations should: 1) register with and provide documentation to the Student Disability Resource Center (SDRC), and 2) bring a letter to the instructor indicating the need for accommodation and what type. This should be done within 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 Assistant Dean of Students:

Student Disability Resource Center
97 Woodward Avenue, South.
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/