WAYNE STATE UNIVERSITY
COLLEGE OF ENGINEERING

Computer Science Department

CSC 5991
Cyber Security Practice

Winter 2016
0000 PERN
M W 11:00 A.M. – 12:20 P.M.
http://www.cs.wayne.edu/fengwei/16sp-csc5991/index.html

Instructor:
Name: Dr. Fengwei Zhang
Office location: 5057 Woodward Ave; Suite 14109.3
Phone: 313-577-1648
Email: fengwei@wayne.edu

Office Hours: Monday, Wednesday 12:20 PM - 1:20 PM

Course Description:

This course provides hands-on experience in playing with security software and network systems in a live laboratory environment, with the purpose of understating real-world threats. The course will take both offensive and defense methods to help student explore security tools and attacks in practice. It will focus on attacks (e.g., buffer overflow, heap spray, kernel rootkits, and denial of service), hacking fundamentals (e.g., scanning and reconnaissance), defenses (e.g., intrusion detection systems and firewalls). Students are expected to finish intensive lab assignments that use real-world malware, exploits, and defenses.

Credit Hours:
3 Credit Hours

Perquisite:
CSC 4290 (Introduction to Computer Networking), CSC 4420 (Computer Operating Systems), and CSC 5270 (Computer Systems Security); or permission of the instructor.

Text(s) Book:

No textbook is required for this course. We will cover these topics using the provided slides, papers, and online material.

Computer Programs:

You should have your own computer to take this class, on which you will install either VMware Workstation for Windows or Linux, or VMware Fusion for Mac.

Course contents:

Weeks	Topics	Readings	Slides & Labs
Week 1, 01/11	Course overview	VMware software and Microsoft products through Dreamsp WSU. [Link] Kali Linux with nmap, Wireshark, and Metasploit. [Link]	
Week 1, 01/13	Lab 1: Packet Sniffing and Wireshark	Wireshark: Network protocol analyzer. [Link] TCPDump and LibPCAP. [Link] Packet Sniffing Basics. In Linux Journal. [Link]	
Week 2, 01/18	No Class	Holiday -- Martin Luther King Day	
Week 2, 01/20	Lab 1: Packet Sniffing and Wireshark		
Week 3, 01/25	Lab 2: Buffer Overflow	Smashing the Stack for Fun and Profit. Aleph One. In Phrack Volume 7, Issue 49. [Link] Local Stack Overflow (Basic Module). [Link] Debugging Under Unix: gdb Tutorial. [Link]	
Week 3, 01/27	Lab 2: Buffer Overflow		
Week 4, 02/01	Lab 2: Buffer Overflow		
Week 4, 02/03	Lab 2: Buffer Overflow		
Week 5, 02/08	Lab 3: Scanning and Reconnaissance	Nmap: the Network Mapper - Free Security Scanner. [Link] Nmap man page. [Link] OpenVAS: Open Vulnerability Assessment System. [Link] Setting up OpenVAS on Kali Linux. [Link] NESSUS: Vulnerability Scanner. [Link] ZMap: Fast Internet-Wide Scanning and its Security Applications. Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. In UsenixSecurity'13. [Link] Souce Code. [Link]	
Week 5, 02/10	Lab 3: Scanning and Reconnaissance		
Week 6, 02/15	Lab 4: Metasploit Framework	Metasploit Framework Project Page. [Link] Metasploitable2 (Linux). [Link] Armitage: Cyber Attack Management for Metasploit. [Link]	
Week 6, 02/17	Lab 4: Metasploit Framework		
Week 7, 02/22	Lab 4: Metasploit Framework		
Week 7, 02/24	Lab 4: Metasploit Framework		

Week 8, 02/29	Lab 5: Malware and Kernel Rootkits	Understanding the Linux Kernel, 3rd Edition. Daniel Bovet and Marco Cesati. [Link] Windows Internals, 6th Edition. David A. Solomon. [Link] SPECTRE: A Dependable Introspection Framework via System Management Mode. Fengwei Zhang, Kevin Leach, Kun Sun, and Angelos Stavrou. In DSN'13. [Link] Heap Taichi: Exploiting Memory Allocation Granularity in Heap-Spraying Attacks. In ACSAC'10. [Link]	
Week 8, 03/02	Lab 5: Malware and Kernel Rootkits		
Week 9, 03/07	Lab 5: Malware and Kernel Rootkits		
Week 9, 03/09	Lab 5: Malware and Kernel Rootkits		
Week 10, 03/14	No class	Holiday -- Spring Break	
Week 10, 03/16	No class	Holiday -- Spring Break	
Week 11, 03/21	Lab 6: Denial of Service (DOS)	Understanding Denial-of-Service Attacks. US-CERT. [Link] Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants). Aleksandar Kuzmanovic and Edward W. Knightly. In ACM SIGCOMM'03. [Link]	
Week 11, 03/21	Lab 6: Denial of Service (DOS)		
Week 12, 03/28	Lab 6: Denial of Service (DOS)		
Week 12, 03/30	Lab 7: Wireless Exploitation & Defenses	How to Hack Wi-Fi: Cracking WPA2-PSK Passwords Using Aircrack-Ng. [Link] Security of the WEP Algorithm. [Link]	
Week 12, 03/21	Lab 7: Wireless Exploitation & Defenses		
Week 13, 03/21	Lab 7: Wireless Exploitation & Defenses		
Week 14, 04/06	Lab 8: Firewalls & Intrusion Detection Systems (IDS)	The Snort Project. Users Manual. [Link] The Linux Firewall iptables [Link] [Link]	
Week 14, 04/11	Lab 8: Firewalls & Intrusion Detection Systems (IDS)		
Week 15, 04/18	Lab 8: Firewalls & Intrusion Detection Systems (IDS)		
Week 15, 04/20	Final Project Presentations		
Week 16, 04/25	Final Project Presentations		

Course Learning Objectives:

This course offers an in depth experience of real-world threats and defenses. Upon successful completion of this class, the student will gain experience in:

- Understanding on real-world security vulnerabilities, exploits and defenses.
- Having hands-on labs in network and system security experiments.
- Learning knowledge of practical security problems and their solutions.

Assessment:

Topics	**Grade**
Class Participation	100
Lab 1: Packet Sniffing and Wireshark	80
Lab 2: Buffer Overflow	80
Lab 3: Scanning and Reconnaissance	80
Lab 4: Metasploit Framework	80
Lab 5: Malware and Kernel Rootkits	80
Lab 6: Denial of Service (DOS)	80
Lab 7: Wireless Exploitation	80
Lab 8: Firewalls & Intrusion Detection Systems (IDS)	80
Team Project	260
Total	1000

Grading Scale:

The grades for the course will be based upon the percentages given below

A	90 - 100%	C	70 - 73%
A-	87 - 89%	C-	67 - 69%
B+	84 - 86%	D+	64 - 66%
B	80 - 83%	D	60 - 63%
B-	77 - 79%	D-	57 - 59%
C+	74 - 76%	F	0 - 56%

Religious Holidays:

Because of the extraordinary variety of religious affiliations of the University student body and staff, the Academic Calendar makes no provisions for religious holidays. However, it is University policy to respect the faith and religious obligations of the individual. Students with

classes or examinations that conflict with their religious observances are expected to notify their instructors well in advance so that mutually agreeable alternatives may be worked out.

Student Disabilities Services:

- If you have a documented disability that requires accommodations, you will need to register with Student Disability Services for coordination of your academic accommodations. The Student Disability Services (SDS) office is located in the Adamany Undergraduate Library. The SDS telephone number is 313-577-1851 or 313-202-4216 (Videophone use only). Once your accommodation is in place, someone can meet with you privately to discuss your special needs. Student Disability Services' mission is to assist the university in creating an accessible community where students with disabilities have an equal opportunity to fully participate in their educational experience at Wayne State University.
- Students who are registered with Student Disability Services and who are eligible for alternate testing accommodations such as extended test time and/or a distraction-reduced environment should present the required test permit to the professor at least one week in advance of the exam. Federal law requires that a student registered with SDS is entitled to the reasonable accommodations specified in the student's accommodation letter, which might include allowing the student to take the final exam on a day different than the rest of the class.

Academic Dishonesty - Plagiarism and Cheating:
Academic misbehavior means any activity that tends to compromise the academic integrity of the institution or subvert the education process. All forms of academic misbehavior are prohibited at Wayne State University, as outlined in the Student Code of Conduct (http://www.doso.wayne.edu/student-conduct-services.html). Students who commit or assist in committing dishonest acts are subject to downgrading (to a failing grade for the test, paper, or other course-related activity in question, or for the entire course) and/or additional sanctions as described in the Student Code of Conduct.

- **Cheating:** Intentionally using or attempting to use, or intentionally providing or attempting to provide, unauthorized materials, information or assistance in any academic exercise. Examples include: (a) copying from another student's test paper; (b) allowing another student to copy from a test paper; (c) using unauthorized material such as a "cheat sheet" during an exam.
- **Fabrication:** Intentional and unauthorized falsification of any information or citation. Examples include: (a) citation of information not taken from the source indicated; (b) listing sources in a bibliography not used in a research paper.
- **Plagiarism:** To take and use another's words or ideas as one's own. Examples include: (a) failure to use appropriate referencing when using the words or ideas of other persons; (b) altering the language, paraphrasing, omitting, rearranging, or forming new combinations of words in an attempt to make the thoughts of another appear as your own.
- **Othe**r forms of academic misbehavior include, but are not limited to: (a) unauthorized use of resources, or any attempt to limit another student's access to educational resources, or any attempt to alter equipment so as to lead to an incorrect answer for subsequent users; (b) enlisting the assistance of a substitute in the taking of examinations; (c)

violating course rules as defined in the course syllabus or other written information provided to the student; (d) selling, buying or stealing all or part of an un-administered test or answers to the test; (e) changing or altering a grade on a test or other academic grade records.

Course Drops and Withdrawals:

There will be no in-completes given for the course.

In the first two weeks of the (full) term, students can drop this class and receive 100% tuition and course fee cancellation. After the end of the second week there is no tuition or fee cancellation. Students who wish to withdraw from the class can initiate a withdrawal request on Pipeline. You will receive a transcript notation of WP (passing), WF (failing), or WN (no graded work) at the time of withdrawal. No withdrawals can be initiated after the end of the tenth week. Students enrolled in the 10th week and beyond will receive a grade. Because withdrawing from courses may have negative academic and financial consequences, students considering course withdrawal should make sure they fully understand all the consequences before taking this step. More information on this can be found at:
http://reg.wayne.edu/pdf-policies/students.pdf

Student services:

- The Academic Success Center (1600 Undergraduate Library) assists students with content in select courses and in strengthening study skills. Visitwww.success.wayne.edu for schedules and information on study skills workshops, tutoring and supplemental instruction (primarily in 1000 and 2000 level courses).
- The Writing Center is located on the 2nd floor of the Undergraduate Library and provides individual tutoring consultations free of charge. Visit http://clasweb.clas.wayne.edu/writing to obtain information on tutors, appointments, and the type of help they can provide.

Class recordings:

Students need prior written permission from the instructor before recording any portion of this class. If permission is granted, the audio and/or video recording is to be used only for the student's personal instructional use. Such recordings are not intended for a wider public audience, such as postings to the internet or sharing with others. Students registered with Student Disabilities Services (SDS) who wish to record class materials must present their specific accommodation to the instructor, who will subsequently comply with the request unless there is some specific reason why s/he cannot, such as discussion of confidential or protected information.

Other issues

- Foods and drinks are not allowed during the lecture or lab hours.
- Cell phones and other two-way communication devices: Students are expected to turn off their devices or turn them to the silent mode when they come to the lecture or to the lab. If a device is used in any way in the lab, you will receive a verbal warning first and then you will be asked to leave immediately.