Offensive Network Security
CIS 4930/5930

Spring 2014

Time & Location

Tuesday,Thursday from 15:35 - 16:50 in LOV 301

Instructors

Instructor: Joshua Lawrence
lawrence@cs.fsu.edu
LOV 167

Advisor: Xin Yuan
xyuan@cs.fsu.edu
LOV 168

Class Terms & Conditions (Disclaimer)

As a student of this class you will adhere to the rules of Florida State University regarding computing rules and not use this class to vandalize and or disrupt normal network operations.

Class Overview

Offensive Network Security (OffNetSec) was created to complement Owen Redwood's Offensive Computer Security (http://www.cs.fsu.edu/~redwood/OffensiveComputerSecrutiy). The goal of OffNetSec is to teach students how to think outside the box when dealing with network protocols.
How can an attacker map a network using known protocols? How can an attacker determine specific communication paths in a network? This class allows students to look deep into known protocols (i.e. IP, TCP, UDP) to see how an attacker can utilize these protocols to their advantage and how to spot issues in a network via captured network traffic.

The first half of this course focuses on known protocols while the second half of the class focuses on reverse engineering unknown protocols. This class will utilize captured network traffic to allow students to reverse the protocol by using known techniques such as incorporating bioinformatics introduced by Marshall Beddoe. This class will also cover fuzzing protocols to see if the server or client have vulnerabilities. Overall, a student finishing this class will have a better understanding of the network layers, protocols, and network communication and their interaction in computer networks.

Main Course Objectives

- How to interact with known network protocols
- How to dissect known protocols
- How to reverse unknown network protocols
- How to fuzz known/unknown network protocols

- How to passively and actively eavesdrop on networks
- How to interact with wireless networks

Tools Taught

- Wireshark/tshark
- nping/nmap/ncat
- Scapy
- Protocol Debugger (PDB) / NetZob
- Terminal Command line tools

Known Protocols Covered

- Ethernet
- ARP
- TCP
- UDP
- DHCP
- HTTP
- SMTP
- DNS

Grading Rubric

- 50% Homework
- 25% Midterm
- 25% Final

Grading Distribution

A-: 86-89; A: 90+
B-: 74-77; B: 78-81; B+: 82-85
C-: 64-66; C: 67-70; C+: 71-73
D-: 52-55; D: 56-59; D+: 60-63
F: 0-51

Extra Credit

Extra credit can be earned by participating in capture the flag (CTF) competitions through the semester. The extra-credit will be applied to the final grade. CTFs will be announced via the class email and n0l3ptr group. Also, visit http://ctftime.org for upcoming CTFs.

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/