CS 499/ISA 564: Security Laboratory – Spring 2017

- **What** – See above
- **When/Where** – Tuesday 4:30-7:10 in ENGR 1505
- **Who** – Ben Greenberg
  - Email: bgreenbe_at_gmu.edu
  - Office Hours: After class
- **Why** – Pick one or more from the following:
  - Required class
  - Fit my schedule
  - Wanted to become a l33t h4xx0r
  - Needed an elective – threw a dart at the board, or rolled a die, or used some other RNG
  - Sounded super spiffy and neato keen
  - Considering making the terrible life choice of a career in InfoSec
  - CowboyNeal told me to do it

Course Description

This course strives to provide students with a practical understanding of real-world security threats, tools, techniques and procedures through the use of instructional laboratory assignments. Topics will include malware, shellcode, remote code exploitation, malware analysis, reverse-engineering, and command and control. This course is intended for students who already possess a strong knowledge of low-level computer programming including C and x86 Assembly. Students will learn how to leverage these skills to attack some of the most challenging problems in the realm of cyber security.

Prerequisites

- CS367 Computer Systems and Programming or CS531 Fundamentals of Systems Programming.
- Strong programming knowledge including C, Python, and x86 Assembly.
- Good understanding of operating system internals (system calls, run-time memory organization)
- Topics covered will include: Malware, shellcode, buffer overflows, heap sprays, code injection, ROP, C2, Metasploit, reverse engineering, PCAP analysis, RCE. Students should possess at least a cursory understanding of these topics (without the use of Google/Wikipedia) or expect a steep learning curve throughout the course.

Grading

- Lab Assignments 70%
- Research Project 20%
- Class Participation 10%
- Readings 0% (These are optional and purely for your edification. They provide additional background and context for topics that will be covered in class and those related but not directly covered. Read at your discretion)

Honor Code

Students are expected to read and adhere to the GMU Honor Code and CS Department Honor Code.

Disability Statement

If you have a documented learning disability or condition that may affect academic performance you should make sure this documentation is on file with the Office of Disability Services and discuss your accommodation needs with me.

Student Support Resources

Information on GMU student support services can be found at the Student Support Resources on Campus page.

Attendance/Absence Policy

In this course students will be treated like adults (being an actual adult is, strictly speaking, optional). Attendance will not be taken. Students are expected to make responsible decisions regarding class attendance and bear in mind that class participation is 10% of the grade. Excuses for absences with good reasons (medical/family emergency, hangover, up too late playing video games, etc.) can be conveyed to me via email.

Late Assignment Policy

Late lab submissions will be given a 10% penalty for each day they are late. Students who cannot make the submission deadlines should email me as far in advance as possible with a well-formulated excuse punctuated by excessive groveling and accompanied by a story of tragic woe describing how you struggled valiantly to complete the assignment on time but the myriad evil forces of life conspired to stymie you at every turn. Note that I will not be watching over Blackboard like a leering gargoyle eagerly waiting to strike that 10% off your lab grade should it be submitted at 12:01AM. Just submit it before I wake up the following day and shake off my morning grumps enough to check for it.

Class Schedule

Week and Date	Course Lectures and Assignments
Week 1 January 24	Lecture 1: Introduction **Research Project assignment**
Week 2 January 31	Lecture 2a: Malware and Shellcode **Lab 1 assignment: Buffer Overflows and Shellcode**
Week 3 February 7	Lecture 2b: Malware and Shellcode continued
Week 4 February 14	Lecture 3a: Code Injection and Exploitation **Lab 1 due at Midnight** **Lab 2 assignment: Remote Exploitation**
Week 5 February 21	Lecture 3b: Code Injection and Exploitation continued
Week 6 February 28	Lecture 4: Metasploit and other Offensive Security Tools **Lab 2 due at Midnight** **Lab 3 assignment: Metasploit and Armitage**
Week 7 March 7	Lecture 5: The Cyber Kill Chain and the Bigger Picture **Lab 3 due at Midnight**
Week 8 March 14	No class – Spring Break (and there was much rejoicing)
Week 9 March 21	Lecture 6a: Malware Analysis and Reverse Engineering **Lab 4 assignment: Malware Analysis and Reverse Engineering**
Week 10 March 28	Lecture 6b: Malware Analysis and Reverse Engineering continued
Week 11 April 4	Optional class: No lecture, work on Lab 4 **Lab 4 due at Midnight**
Week 12 April 11	Lecture 7: Network Hunting and C2 **Lab 5 assignment: Network Hunting and C2**
Week 13 April 18	Lecture 8a: Advanced Malware
Week 14 April 25	Lecture 8b: Advanced Malware continued **Lab 5 due at Midnight** **Lab 6 assignment: Analyzing Advanced Malware**
Week 15 May 2	Lecture 9: Careers in Cyber Security
Week 16 May 9	Optional class: No lecture, work on Lab 6 **Lab 6 due at Midnight** **Research Project due at Midnight**
Week 17 May 16	No class – Exam Week (because you've suffered enough)