CS 499/ISA 564: Security Laboratory – Spring 2019

- **Who** – Ben Greenberg
  - Email – bgreenbe_at_gmu.edu
  - Office Hours – By appointment only
- **What** – See above
- **When/Where** – Tuesday 4:30-7:10 in Innovation Hall 223
- **Why** – Pick one or more from the following:
  - Required class
  - Fit my schedule
  - Needed a 400-level CS class and desperately wanted to avoid taking CS471
  - 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 cyber security
  - 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 buffer overflows and other software vulnerabilities, shellcode, code injection techniques, return-oriented programming, Metasploit, malware, malware analysis, reverse-engineering, PCAP analysis, 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, as well as basic networking knowledge. 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 and CS455 Computer Communications and Networking (or equivalent knowledge)
- Strong systems programming knowledge including C and x86 assembly
- Good understanding of operating system internals (system calls, run-time memory organization)
- Basic knowledge of computer networking, TCP/IP protocols, Wireshark and PCAP analysis
- A laptop powerful enough to run virtualization software and run two simultaneous virtual machines

Grading
- 6 Lab Assignments – 75% (12.5% each by the virtue of math)
- Research Project – 25%
- Grade Scale – The usual, without that +/- crap (A: 90+, B: 80-89, C: 70-79, D: 60-69, F:59-)

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 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. 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

Labs are due two weeks after they are assigned. Late submissions will be accepted for up to one week after the due date with a 20% penalty. Submissions made after the due date are FINAL. 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 20% 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. Labs submitted before the due date will usually receive prompt feedback that students can use to make revisions to improve their grades.

Class Schedule

Week and Date	Course Lectures and Assignments
Week 1 January 22	Lecture 0: Introduction **Research Project assignment**
Week 2 January 29	Lecture 1: Software Vulnerabilities and Shellcode **Lab 1 assignment: Buffer Overflows and Shellcode**
Week 3 February 5	No lecture: Open lab day for Lab 1
Week 4 February 12	Lecture 2: Code Injection and Exploitation **Lab 1 due at Midnight** **Lab 2 assignment: Advanced Exploitation**
Week 5 February 19	No lecture: Open lab day for Lab 2
Week 6 February 26	Lecture 3: Network and Security Tools **Lab 2 due at Midnight** **Lab 3 assignment: Wireshark and Metasploit**
Week 7 March 5	No lecture: Open lab day for Lab 3
Week 8 March 12	No class: Spring Break (and there was much rejoicing) **Lab 3 due at Midnight**
Week 9 March 19	Lecture 4: Malware Analysis and Reverse Engineering **Lab 4 assignment: Malware Analysis and Reverse Engineering**
Week 10 March 26	No lecture: Open lab day for Lab 4
Week 11 April 2	Lecture 5: Network Hunting and C2 **Lab 4 due at Midnight** **Lab 5 assignment: Network Hunting and C2**
Week 12 April 9	No lecture: Open lab day for Lab 5
Week 13 April 16	Lecture 6: Advanced Malware **Lab 5 due at Midnight** **Lab 6 assignment: Advanced Malware**
Week 14 April 23	No lecture: Open lab day for Lab 6
Week 15 April 30	Lecture 7: Careers in Cyber Security **Lab 6 due at Midnight**
Week 16 May 7	No class: Reading Days (because you've suffered enough)
Week 17 May 14	No class: Exam Period (the only thing exams test is my patience) **Research Project due at Midnight**