CIS 4204 Ethical Hacking
Spring, 2015

Instructor: Shane Hartman  
E-Mail: shartman@sar.usf.edu

Office:  
Office Telephone:  
Office Hours:

PREREQUISITES: COP 2030 and MAD 2104

COURSE DESCRIPTION: provide a basic understanding of computing, networking, programming concepts, and exploitation techniques, as they relate to computer security. In security testing, an ethical hacker with legal permission attempts to penetrate a system or systems to find a weak link and then analyze ways to correct the security flaws. Ethical hacking relies on a combination of creativeness, expansion of knowledge based on best practices, legal issues, and client industry regulations as well as known threats and the breath of the target organization’s security presence or point of risk

COURSE TOPICS: Indicate the subject content that the course will cover.

1. Article and Industry Research and Discussion
2. Hacking and Counter Hacking Based Skill Practice

COURSE OBJECTIVES: The objectives are the goals of the course. They are the intended results or consequences of instruction, curricula, or activities.

1. General computer organization and architecture
2. Ethical Hacking methodology
3. Generalized exploit techniques
4. Basic network concepts
5. Networking vulnerabilities and countermeasures
6. Develop skills and techniques for writing a research paper.

COURSE STUDENT LEARNING OUTCOMES: Course outcomes are statements that describe what students will be able to demonstrate at the end of the course. They provide the evidence that student learning took place.

Upon completion of this course, students will be able to:

1. Understand computer systems threats
2. Understand the advisory and counter measures
3. Employ basic practice security principles to computer systems and infrastructure

TEXT AND MATERIALS:

**CANVAS USE:**
The class syllabus is posted in Canvas, an online course management system. In this class Canvas will be used for all aspects of the course: lectures, assignments, and examinations.

**COMPUTER LAPTOP USE (suggested)**
USFSM requires all students to have laptops that can be brought with them to class.
- Students are required to use their laptops to complete the assignments.

**PLAGIARISM SOFTWARE (if applicable)**
Instructors are encouraged to use the “TURNITIN” application via Canvas whenever possible to assist students in avoiding plagiarism. If used instructors must include the following statement in the course syllabus:

The University of South Florida has an account with an automated plagiarism detection service which allows student assignments be checked for plagiarism. I reserve the right to ask students to submit their assignments to Turnitin through Canvas. Assignments are compared automatically with a database of journal articles, web articles, and previously submitted papers. The instructor receives a report showing exactly how a student’s paper was plagiarized.

PLEASE REMOVE YOUR NAME FROM THE BODY OF YOUR PAPER AND REPLACE IT WITH YOUR USF ID#. ALSO REMOVE YOUR NAME FROM THE FILE NAME AND REPLACE IT WITH YOUR USF ID# (e.g., “U12345678 Essay 1.docx”) BEFORE SUBMITTING IT TO TURNITIN.

Pursuant to the provisions of the Family Educational Rights and Privacy Act (FERPA), students are requested to maintain confidentiality as a way to keep their personal contact information (i.e. name, address, telephone) from being disclosed to vendors or other outside agencies. By your submission, you are also agreeing to release your original work for review for academic purposes to Turnitin.

**GRADING, EVALUATION AND ATTENDANCE POLICIES:**
A. USFSM policy requires that all students receive a graded assignment or examination prior to the semester’s drop/withdraw date
B. Specifically state the value of and the manner in which each assignment in the syllabus will be evaluated or graded.
C. A precise description of the grading process, e.g. use of plus or minus grading, use of straight A,B,C,D and F system, point system with delineations of grades for accumulation of a stipulated number of points, etc.
D. Attendance policy to include make up of missed work.

**USFSM AND USF SYSTEM POLICIES**
A. **Academic Dishonesty**: The University considers any form of plagiarism or cheating on exams, projects, or papers to be unacceptable behavior. Please be sure to review the university’s policy in the USFSM Catalog, the USF System Academic Integrity of Students, and the USF System Student Code of Conduct.

B. **Academic Disruption**: The University does not tolerate behavior that disrupts the learning process. The policy for addressing academic disruption is included with Academic Dishonesty in the USFSM Catalog, USF System Academic Integrity of Students, and the USF System Student Code of Conduct.

C. **Contingency Plans**: In the event of an emergency, it may be necessary for USFSM to suspend normal operations. During this time, USFSM may opt to continue delivery of instruction through methods that include but are not limited to: Canvas, Elluminate, Skype, and email messaging and/or an alternate schedule. It’s the responsibility of the student to monitor Canvas site for each class for course specific communication, and the main USFSM and College websites, emails, and MoBull messages for important general information. The USF hotline at 1 (800) 992-4231 is updated with pre-recorded information during an emergency. See the Campus Police Website for further information.

D. **Disabilities Accommodation**: Students are responsible for registering with the Office of Students with Disabilities Services (SDS) in order to receive academic accommodations. Reasonable notice must be
given to the SDS office (typically 5 working days) for accommodations to be arranged. It is the responsibility of the student to provide each instructor with a copy of the official Memo of Accommodation. Contact Information: Disability Coordinator, 941-359-4714, disabilityservices@sar.usf.edu, http://usfsm.edu/disability-services/

E. Fire Alarm Instructions: At the beginning of each semester please note the emergency exit maps posted in each classroom. These signs are marked with the primary evacuation route (red) and secondary evacuation route (orange) in case the building needs to be evacuated. See Emergency Evacuation Procedures.

F. Religious Observances: USFSM recognizes the right of students and faculty to observe major religious holidays. Students who anticipate the necessity of being absent from class for a major religious observance must provide notice of the date(s) to the instructor, in writing, by the second week of classes. Instructors canceling class for a religious observance should have this stated in the syllabus with an appropriate alternative assignment.

G. Sexual Misconduct/Sexual Harassment Reporting: USFSM is committed to providing an environment free from sex discrimination, including sexual harassment and sexual violence (USF System Policy 0-004). The Counseling and Wellness Center is a confidential resource where you can talk about incidents of sexual harassment and gender-based crimes including sexual assault, stalking, and domestic/relationship violence. This confidential resource can help you without having to report your situation to either the Office of Student Rights and Responsibilities (OSSR) or the Office of Diversity, Inclusion, and Equal Opportunity (DIEO), unless you request that they make a report.

Please be aware that in compliance with Title IX and under the USF System Policy, educators must report incidents of sexual harassment and gender-based crimes including sexual assault, stalking, and domestic/relationship violence. If you disclose any of these situations in class, in papers, or to me personally, I am required to report it to OSSR or DIEO for investigation. The Deputy Coordinator for USFSM is Mary Beth Wallace, AVP for Student Enrollment, Engagement and Success, 941-359-4330 or marybeth@sar.usf.edu.

Campus Resources:
Counseling Center and Wellness Center 941-487-4254
Victim Advocate (24/7) 941-504-8599

List of off-campus resources:
Hope of Manatee: 941-755-6805
Safe Place & Rape Crisis Center (SPARCC) – Sarasota: 941-365-1976
First Call for Help- Manatee: 941-708-6488
Sarasota & North Port 941-366-5025
Manatee Glens: 941-782-4800

H. Web Portal Information: Every newly enrolled USF student receives an official USF e-mail account. Students receive official USF correspondence and Canvas course information via that address.

GENERAL INSTRUCTION FOR STUDENTS (suggested)
A. If you miss class or have circumstances preventing you from doing your work contact me immediate for support and remediation.

B. Academic Support Services:
Information Commons provides students with individual and group study spaces, computers, printers, and various media equipment for temporary use. Information Commons is staffed with a librarian, learning support faculty, tutors, and technology and e-learning specialists. Students challenged by the rigors of academic writing, mathematics, or other course content are urged to contact their professors early in the semester to chart out a plan for academic success, and/or regularly use the tutoring services provided by the Learning Support Services, which are provided at no cost to students.
Course Schedule (tentative, subject to change):

**Week 1 – Introduction to Ethical Hacking**
- Class Intro
- Hacking History
- Ethical Hacking
- Threats

**Week 2 – TCP/IP Primer**
- TCP
- IP
- UDP
- Packets
- 3 Way Handshake

**Week 3 – Footprinting**
- Gathering Information
- Whois
- Tracert and TTL

**Week 4 – Scanning**
- Test 1
- Ping Sweeps
- Scanning Tools
- Port Scanning

**Week 5 – Enumeration**
- NetBIOS
- Active Directory
- SNMP Enumeration
- DNS Zone Transfer

**Week 6 – Hacking Windows**
- Privilege Escalation
- Cracking Passwords
- Data Execution Prevention

**Week 7 – Hacking Unix**
- Quest for Root
- Vulnerability Mapping
- Services

**Week 8 – Network Devices and Hardware**
- Mid-Term
- Discovery
- Fingerprinting

**Week 9 – Hacking Code**
- Buffer Overflows
- Input Validation
- Vulnerabilities
- Exploits

**Week 10 – Wireless Hacking**
- Wireless Type
• Service Set Identifier (SSID)
• Wired Equivalent Protocol (WEP)
• Wireless Application Protocol (WAP)

Week 11 – Web Server Hacking and Web Application Vulnerabilities
• IIS Attacks
• Apache Attacks
• Spidering

Week 12 – SQL Injection Vulnerabilities
• Test 2
• SQL Injection Testing and Attacks
• Types of Attacks
• SQL Injection Prevention and Remediation

Week 13 – Firewalls, Intrusion Detection Systems, and Honeypots
• Firewall Types and Configurations
• Intrusion Detection Systems (IDS)
• Honeypot Applications

Week 14 – Social Engineering
• Social Engineering
• Human-Based Social Engineering
• Computer-Based Social Engineering
• Identity Theft

Week 15 – Viruses, Worms, and Trojans
• Viruses
• Spyware
• Spambots
• Worms

Week 16 – Final Exams