USF Sarasota-Manatee - New Undergraduate Course Proposal Form

1. **College/School Contact Information**

Tracking Number	Date & Time Submitted	
3	2010-03-29 17:13:37	
Discipline	College/School	Budget Account Number
Information Technology	Arts & Sciences	380700004
Contact Person	Phone	Email
S.Lodwig	941-228-4671	slodwig@sar.usf.edu

2. **Course Information**

Prefix	Number	Full Title
CIS	4369	Ethical Hacking

Is the course title variable? N
Is a permit required for registration? N
Are the credit hours variable? N

Credit Hours	Section Type	Grading Option
3.0	Class Lecture (Primarily)	Regular
Total Clock Hours	Abbreviated Title (30 characters maximum)	
45	Ethical hacking	

5. Prerequisites
   Programming Course and a Math Course
6. Corequisites
   none
7. Co-Prerequisites
   none
8. Course Description
   Provides an understanding of computing, networking, exploitation techniques, used for IT security. In testing, a legal ethical hacker tries to penetrate a system, finds its weakest link and analyzes ways to correct security flaws.
9. **Justification**

   (This section is critical since the APC members will make their decision based on the information provided here. The information should be in the following outline form.)

   A. Indicate how this course will strengthen the Undergraduate Program. Is this course necessary for accreditation or certification?

As I.T. students apply their knowledge by constructing systems and networks to deliver information to business functions, they must be cognizant of the threats and vulnerabilities to these systems, and how to develop effective countermeasures for these. This course helps provide a basic understanding of computing, networking, and programming concepts, as well as exploitation techniques, as they relate to computer security. In security testing, an ethical hacker with legal permission attempts to penetrate a system to find its weakest link and then analyze ways to correct the security flaws. Ethical hacking relies on a combination of creativeness, expansion of knowledge bases of best practices, legal issues, and client industry regulations as well as known threats and the breadth of the target organization's security presence or point of risk. This course ought to be a requisite part of any I.T. certificate in Information Security. While this course does not prepare a student for a particular certification, such as the EC-Council's "Certified Ethical Hacker", the student would still benefit from the class and have the foundation on which to pursue such a certification.

B. What specific area of knowledge is covered by this course which is not covered by courses currently listed?

Teaches penetration testing methods which are not covered in other I.T. security coursework.

C. What is the need or demand for this course? (Indicate if this course is part of a required sequence in the major.) What other programs would this course service?

Ethical Hacking is another key course in the Information Security suite. It enables the future Information Security Expert stay one step ahead of the hacker by viewing the system to be secured thru the eyes of a hacker.

D. Has this course been offered as Selected Topics/Experimental Topics course? If yes, what was the enrollment?

Ethical hacking has been offered as Special Topics for the last three Fall semseters (2007-2009), with a consistently increasing enrollment (10 initially to 31 last fall)

E. How frequently will the course be offered? What is the anticipated enrollment?

Once a year. We expect the enrollment to incerase given the IT Program is among the fastest growing ones at this campus.

F. Do you plan to drop a course if this course is added? If so, what will be the effect on the program and on the students? (If dropping/deleting a course please complete the nonsubstantive course change form.)

No, we do not plan to drop another course.

G. What qualifications for training and/or experience are necessary to teach this course? (List minimum qualifications for the instructor.)

The Instructor teaching these courses is highly qualified with a CISSP certification. This certification is the highest and most prestigious of the Information Security certifications. The instructor is also working full-time in the Information Security area.

10. **Other Course Information**

A. Objectives / Outcomes

The student will understand - • General computer organization and architecture • Basic programming concepts • Ethical hacking methodology • Generalized exploit techniques • Buffer overflows, heap overflows, and format string vulnerabilities • Basic networking concepts • Networking vulnerabilities and countermeasures • Basic assembly language and shellcoding • Countermeasures for security vulnerabilities

B. Major Topics

Security trends, Security Services, Threats, General hacking methodology. Networking concepts, Footprinting, Scanning. OSI Model, Sockets, Lower Layers, Network Sniffing. Network-based attacks, Denial of service, Spoofing / injection. TCP/IP Hijacking, Port Scanning Basic programming concepts, Pseudo-code, Control Structures Memory Segmentation, Buffer overflows Generalized Exploit Techniques Command shells, Heap and other overflows, Format strings. Assembly and shellcoding Developing countermeasures - System Daemons, Log Files, Nonexecutable Stack, Randomized Stack Space Basic cryptography, Password cracking Hacking Wireless Networks, WEP cracking OS specific vulnerabilities

C. Examples of Course Textbooks and Course Readings

Hacking: The Art of Exploitation, 2nd Edition, by Jon Erickson. Publisher: No Starch Press. Pub Date: January 15, 2008.

11. **Syllabus**

Please submit an electronic copy of your syllabus to Rhonda Moraca, moraca@sar.usf.edu.

UNIVERSITY OF SOUTH FLORIDA

ETG 4930 Ethical Hacking
Fall, 2009

Course Abstract: The purpose of this course is to 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 to find its weakest link and then analyze ways to correct the security flaws. Ethical hacking relies on a combination of creativeness, expansion of knowledge bases of best practices, legal issues, and client industry regulations as well as known threats and the breadth of the target organization's security presence or point of risk.

Outcomes of this course: The student will understand:

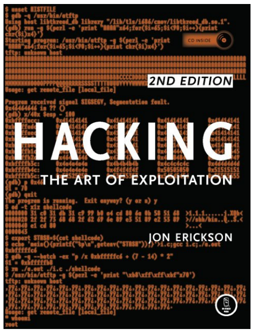
- General computer organization and architecture
- Basic programming concepts
- Ethical hacking methodology
- Generalized exploit techniques
- Buffer overflows, heap overflows, and format string vulnerabilities
- Basic networking concepts
- Networking vulnerabilities and countermeasures
- Basic assembly language and shellcoding
- Countermeasures for security vulnerabilities

As time permits, we may also explore:

- Encryption and basic password cracking
- Wireless attacks and countermeasures

Class Format: Undergraduate course meeting Thursdays 6-8:50 p.m. via Elluminate. This class will be taught completely online. There will be a number of hands-on exercises using the tools on the CD included with the textbook.

Office Hours: Email me anytime at: jrasmuss@cse.usf.edu. I am also often available on Google talk: Jeremy.rasmussen@gmail.com. Office phone: (813) 972-6845.



Required reading:
Hacking: The Art of Exploitation, 2nd Edition
by Jon Erickson
Publisher: No Starch
Pub Date: January 15, 2008
Print ISBN-13: 978-1-59-327144-2

Whitehatters Computer Security Club (WCSC): If you are serious about information security and want more hands-on learning outside the classroom environment, consider joining WCSC. The purpose of the club is to promote learning about computer security and participate in organized Capture the

Flag (CtF) events. The club meets bi-weekly on Fridays at 5 p.m. in the Marshall Center, USF Tampa campus. **For more info**: www.whitehatters.org

Whitehatter Patrick Vincens developed a hacker training Web site as part of his Honors College studies. It is located at: http://proving-grounds.usf.edu. The site can only be accessed from on USF campus. It is a good site to try out to begin thinking like a hacker.

Course instructor: Mr. Jeremy Rasmussen. Manager, Information Security Solutions (ISS) group, Sypris Electronics, LLC, Tampa. M.S. Engineering Management (USF, 1994); B.S. Computer Science (USF, 1991); Certified Information Systems Security Professional (CISSP), 2000. About 17 years of experience in secure communications systems and information assurance product development. My group performs network vulnerability assessments, forensic incident response, product vulnerability analysis, penetration testing / red teaming, develops security policy, and delivers security awareness training. Besides this class, I have also taught "Cryptography and Network Security" and "Digital Forensics and Investigations" through the IT Dept. of the Arts & Sciences College at USF Sarasota.

Grading format:

Hands-on exercises, Quizzes, and Class Participation	34%
Test #1	33%
Test #2	33%
Total	**100%**

Please note these very important class rules:

1. **Assignments are due by the beginning of class on the due date assigned.** I will not accept any late assignments unless you have specifically made arrangements with me **beforehand**. For example, emailing me at the end of the semester to request turning in all of your missed homework because you had some illness will ***not*** work.
2. **Academic honesty is mandatory.** Cheating on exams is grounds for expulsion from the class and receiving a double F, which will brand your academic career in infamy forever. If you turn in work that references someone else's work and do not properly attribute it, this is plagiarism. It is also grounds for receiving a double F in the course. This includes, for example, downloading source code from the Internet without giving credit. If you borrow some freeware to use in a project, and the freeware is copyrighted, you may not remove the header information and insert your own as if it were original code. This is unethical and grounds for dismissal from the class.
3. **New university-standard policy** which doesn't affect us much because we are already 100% on-line: "In the event of an emergency, it may be necessary for USF to suspend normal operations, During this time, USF may opt to continue delivery of instructions through methods that include, but are not limited to Blackboard, Elluminate, and Skype and email messaging and/or an alternate schedule. It's the responsibility of the student to monitor Blackboard site for each class for course specific communication, and the main USF, College, and department websites, emails, and MoBull messages for important general information."

Most students are highly motivated to learn and do not need to be informed of these things, but the 5% or so that want to get a free grade without doing any work need to be made aware of these rules. If you do not think you can abide by these (in my opinion, completely reasonable) rules, please do not take this course!

Class philosophy: Ethical hacking is a very hands-on discipline. While there is a fair amount of information to be covered, most people learn this subject matter by being involved and engaged in activities. For this reason, this class will employ a number of hands-on exercises. There will be a class-participation session each week in which we will discuss current topics (news, relevant issues) in ethical hacking. Students are expected to do some self-study outside the class to be prepared to make a contribution in class.

Course Schedule (tentative, subject to change – changes will be announced in class and official announcements will be posted on MyUSF):

Week 1: 8/27/09

- Class intro
- Security trends
- Security Services
- Threats
- General hacking methodology

Reading: TBD.

Week 2: 9/3/09

- Networking concepts
- Footprinting
- Scanning

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Chapter 0x400. NETWORKING
Section 0x410. OSI Model
Section 0x420. Sockets
Section 0x430. Peeling Back the Lower Layers
Section 0x440. Network Sniffing

Week 3: 9/10/09

- Network-based attacks
- Denial of service
- Spoofing / injection

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Section 0x450. Denial of Service
Section 0x460. TCP/IP Hijacking
Section 0x470. Port Scanning
Section 0x480. Reach Out and Hack Someone

Week 4: 9/17/09

- Basic programming concepts, part 1.

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Chapter 0x100. Introduction
Chapter 0x200. Programming
Section 0x210. What Is Programming?
Section 0x220. Pseudo-code

Section 0x230. Control Structures
Section 0x240. More Fundamental Programming Concepts

Week 5: 9/24/09

- Basic programming concepts, part 2.

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Section 0x250. Getting Your Hands Dirty
Section 0x260. Back to Basics
Section 0x270. Memory Segmentation
Section 0x280. Building on Basics

Week 6: 10/1/09

- Buffer overflows

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Chapter 0x300. EXPLOITATION
Section 0x310. Generalized Exploit Techniques
Section 0x320. Buffer Overflows

Week 6: 10/1/09

- Command shells
- Other overflows
- Format strings

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Section 0x330. Experimenting with BASH
Section 0x340. Overflows in Other Segments
Section 0x350. Format Strings

Week 7: 10/8/09

- Assembly and shellcoding
- **Test #1** – online via MyUSF (Blackboard)

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Chapter 0x500. SHELLCODE
Section 0x510. Assembly vs. C
Section 0x520. The Path to Shellcode

Week 8: 10/15/09

- Assembly and shellcoding, part 2

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Section 0x530. Shell-Spawning Shellcode
Section 0x540. Port-Binding Shellcode
Section 0x550. Connect-Back Shellcode

Week 9: 10/22/09

- Developing countermeasures

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Chapter 0x600. COUNTERMEASURES
Section 0x610. Countermeasures That Detect
Section 0x620. System Daemons
Section 0x630. Tools of the Trade
Section 0x640. Log Files
Section 0x650. Overlooking the Obvious
Section 0x660. Advanced Camouflage
Section 0x670. The Whole Infrastructure
Section 0x680. Payload Smuggling
Section 0x690. Buffer Restrictions
Section 0x6a0. Hardening Countermeasures
Section 0x6b0. Nonexecutable Stack
Section 0x6c0. Randomized Stack Space

Week 10: 10/29/09

- Basic cryptography

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Chapter 0x700. CRYPTOLOGY
Section 0x710. Information Theory
Section 0x720. Algorithmic Run Time
Section 0x730. Symmetric Encryption
Section 0x740. Asymmetric Encryption
Section 0x750. Hybrid Ciphers

Week 11: 11/5/09

- Password cracking

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Section 0x760. Password Cracking

Week 12: 11/12/09

- Hacking Wireless Networks
- WEP cracking

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Section 0x770. Wireless 802.11b Encryption
Section 0x780. WEP Attacks

Week 13: 11/19/09

- Additional topics – probably Operating System specific vulnerabilities

Reading:
Hacking: The Art of Exploitation, 2nd Edition
Chapter 0x800. CONCLUSION

Week 14: 11/26/09

- Other topics – OS specific vulnerabilities

Reading:
Hand-outs, TBD.

Week 15: 12/3/09

- Other topics
- **Test #2** – online via MyUSF (Blackboard)

Reading:
Hand-outs, TBD.