2

Syllabus

CONTENTS

The syllabus describes the course, the teacher's goals, administrative issues, the calendar to be followed, the grading scale, etc. This chapter provides the syllabus used in the Fall 2013 course at Clemson University. I have omitted items that are requirements specific to Clemson University. Each instructor will need to insert the information that is appropriate for their institution.

2.1 Attendance policy

Course meetings mainly follow a seminar, rather than lecture, format. Attendance at course meetings is mandatory, since the seminar format includes in-class discussion. For the discussion, students are expected to have completed the reading assignments in advance. On days when presentations or demonstrations are due, students must be present and properly prepared. Students are expected to wait for 10 minutes, should the professor be late.

2.2 Objectives and outcomes

This course is a project-oriented introduction to computer and network security. Security is a process that maintains well-defined system properties. Students will need to understand security threats and existing security countermeasures. Discussions will identify security holes in current network implementations. A set of challenging assignments has been developed that provide

students with the basic skill sets needed for work in network security. In class discussions will help students prepare their assignments. Ethical and legal aspects of computer security issues are introduced and discussed as a part of the course. The final includes essay questions on these topics. Assignments will include:

- Technical deliverables (system installation, implementation, test, and maintenance).
- Technical reports and design documents.
- Technical presentations.

Students are expected to create and deliver professional quality materials. Graduate students need to implement a security research project and present their results to the class. The security project should be at a level suitable for submission to a professional conference.

2.3 A note on ethics, legal issues and etiquette

In order to develop and maintain secure systems, it is necessary to fully understand system vulnerabilities. This understanding is best attained by mimicking the mindset of potential attackers. This course provides students with facilities and resources for exploring system vulnerabilities. It is expected that any exploits attempted will be carefully designed with a specific purpose in mind. Exploit designs will be documented and delivered to the instructor before implementation occurs. They will involve neither physical access to machines nor vandalism (including destruction of software or hardware infrastructure). Exploits will most often involve violating system confidentiality, consistency, and/or non-repudiation attributes. All attack implementation and testing will be performed solely within the laboratory on the machines provided for that purpose. These machines will remain on an isolated network during this process.

Attacks on operational networks potentially violate existing laws with severe consequences. Illegal activity is not condoned and will be dealt with severely. Red team analysis of systems should be performed with the informed consent of the owners of the system being analyzed and not in connection with this course.

2.4 Resources

This course is project oriented. Students are expected to independently find the resources needed to fulfill their assignments. They will also write a number of reports and present their results. Most lectures will be run as a seminar with the instructor questioning the students. The instructor is available to the students for discussion of design alternatives and as an information resource.

Introduction to Computer and Network Security: Navigating Shades of Gray is the required text.

A number of security-related URL's, videos and other information will be provided. Use of open source tools for system implementation is strongly encouraged. Books worth referring to:

- S. Young and Dave Aitel, *The Hackers Handbook* [13],
- Bob Toxen, *Real World Linux Security: Intrusion Prevention, Detection, and Recovery* [11],
- Kolesnikov and Hatch, *Building Linux VPNs* [8],
- Mike Schiffman, *Building Open source network security tools* [9],
- Michael Donahoo and Kenneth Calvert, *The Pocket Guide to TCP/IP Programming* [5],
- Warren Gay, *Linux Socket Programming by Example* [7],
- John Chirillo, *Hack Attacks Revealed* [4], and
- *Building Secure Software* [12].

2.5 Assignments

Demonstrations and presentations will be done in the lab at times arranged with the instructor. They are a form of oral examination and should be treated accordingly. They will include either individuals or work groups and the instructor. Students are given 10 minutes to present their work and convince the instructor that they fulfilled the assignment.

The graduate section is the same as the undergraduate, except that the graduate students do an independent research project. The project topic is due on October 9. The project will be graded as if it were a conference paper. The last 2 class meetings are an in class seminar on these projects. The papers are due by Nov. 27. If students need guidance, they need to initiate contact with the instructor.

2.6 Grading

(Percentages. For undergraduates, points and percentages are identical. For graduate students, they are quite different.)

- A 90 or above
- B 80 to 89
- C 70 to 79
- D 60 to 69
- F Below 60

Deadlines are fixed. No extensions will be given. No late assignments will be accepted. This means that assignments are due at the start of class. No credit will be given for a late assignment. Printers printing slowly are not an adequate excuse for a late assignment.

Presentations are interactive. Students must be prepared to answer questions from the instructor and other students. Documents must be professionally prepared. Sloppy and poorly written documents will be graded harshly. Students may be asked to re-write the document to make it fulfill professional standards. The documentation is due at the start of class on the due date. Presentations will be given during the week. A sign up sheet will be circulated in class.

Assignment	Group or Individual	Deliverable	Due Date	Points
VPN and sniffer installation, use, and analysis	Individual (pair)	Document and presentation	09/10/13	20
Buffer overflow implementation	Individual	Report and demonstration	10/08/13	20
Graduate research topic	Individual (6490 only)	1 page abstract	10/08/13	10
Polymorphic virus implementation	Individual	Report and demonstration	11/05/13	20
Wireless Security	Individual	TBD	12/03/03	15
Graduate research project	Individual (6490 only)	Report and in-class presentation	11/19/13	40
Class participation	Individual	N/A		15
Final exam	Individual	Examination	12/12/2013	10
Total Undergrad				100
Total Grad				150

TABLE 2.1
Items used in grading with due dates and points.

Date	Due	Reading assignments	Lecture topic
08/27		Syllabus, IEEE Security and Privacy, Chapters 5 and 6	Introduction to course
09/03		Chapter 3	Cryptography basics
09/10	VPN and sniffer	Chapters 7 and 8	Buffer overflow details
09/17		Chapter 1 and 2	Survey of security issues
09/24		Chapter 4	Network attack how to
10/01		Chapter11	Privacy
10/08	Graduate research topic/ Buffer overflow	Chapter 9	Virus execution details
10/15	Fall Break		
10/22			Game console security
10/29		Chapter 10 and 12	Automotive Security
11/05	Virus assignment		Wireless security
11/12		Chapters 13 and 14	Digital Rights Management / Ethics
11/19	Graduate research		Student presentations
11/26			Student presentations
12/03	Wireless assignment		Presentation
12/12	Final at 7:00 PM		

TABLE 2.2
Class schedule.