CprE 532: Information Warfare

Spring 2024

Instructor:

Dr. Doug Jacobson, 371 Durham dougj@iastate.edu
Phone: (515) 294-8307

Textbook: Hacking Exposed (6th or 7th edition)

Class Discord Server: Link will be posted in the class announcements

Course web site: We use Canvas for course notes, slides, homework, and assignment submission.

Goal:

This course is intended to provide students with hand-on experience in installing, configuring, and testing state-of-the-art security software and hardware. Methods of attack will be examined to better understand how to detect and prevent attacks.

Prerequisite: CprE 531 or CprE 530

Course Length: 45 hours in 15 weeks, 2 seventy five minute meetings per week

Course Description:

Computer Systems and network security: implementation, configuration, testing of security software and hardware, network monitoring. Computer attacks and countermeasures. Emphasis on laboratory experiments.

Course Learning Objectives:

Upon completing this course a student will:

- Understand the ethics of using hacking tools
- Be able to describe the TCP/IP network protocols and the effect of an open network protocol on security
- Be able to snoop traffic from a network and decode the data
- Be able to describe methods to counter traffic attacks like snooping, spoofing, redirection, and flooding.
- Understand the importance of passwords and methods to select good passwords
- Be able to crack passwords and understand the importance of authentication
- Understand the issues of social engineering when used to discover passwords

- Be able to describe a centralized key distribution center and its uses in authentication
- Be able to use one-time passwords, Kerberos, and other authentication systems.
- Understand the issues of anonymous email and email forgery, email privacy.
- Understand and be able to use an encrypted email system
- Understand the relationship of public and private keys to email and the uses of a Public Key Infrastructure
- Be able to identify the security problems with standard terminal based protocols like telnet, ftp, NFS, and web.
- Be able to identify solutions to the security problems with telnet, ftp, NFS, and web traffic.
- Understand how secure protocols like SSH, SSL, and VPN's operate and how they can be used to enhance security.
- Be able to develop a plan to attack a network of computer systems and then be able to develop a plan of countermeasures.
- Understand the use of firewalls and the strengths and weaknesses of a firewall
- Be able to read and identify information in log files for possible security violations
- Be able to use screening routers and software filters to defend a computer system from attack.
- Be able to use probe software to determine the weaknesses of a computer system.
- Understand how intrusion detection system operate and how they can be used to detect attacks

Major Topics:

- Introduction & Ethics
- Network Protocols
- Traffic attacks and defenses
- Authentication attacks and defenses
- eMail Attacks and defenses
- Terminal Services, NFS, and X
- WEB
- Intrusion detection
- Firewalls
- Screening Routers
- Link encryption
- Encryption tools
- Trapping a hacker
- Probe software
- Security management

Method of Instruction:

The course is taught using lectures which are also videotaped to the off campus students. The course also has a strong laboratory component where the students connect to the lab remotely to carry out experiments. The labs range from using tools (both attack tools and defend tools) to looking at network protocols. The largest lab is the attack and defend lab where the students try to break into a small company designed by the faculty. The students must detail the attack plan and then provide a detailed description of how to defend against the attacks.

In a field of cutting-edge technological engineering students will be required to be creators of knowledge and inventors of processes, not simply users of information. This requirement will make students move beyond being knowledgeable about the content and into the higher realms of analyzing situations, designing systems, and evaluating results. To accomplish these cognitive goals, the emphasis in the classroom will be on the student. Student-centered classrooms will enhance student learning by helping them understand the content on the basis of real-world experiences, engaging them in interactive learning situations, and providing problem-based projects from which they will learn.

Grading:

35% Exam 1
35% Exam 2
30% Labs/ homework/ in-class

Requirements:

Internet access (VPN, ftp, www)

CprE 532 **Tentative Schedule Spring 2024**

Class		Date	Topics
1	Tues	16-Jan	Introduction & Adversarial Thinking - Virtual Class
2	Thurs	18-Jan	Adversarial Thinking - Virtual class
3	Tues	23-Jan	Adversarial Thinking
4	Thurs	25-Jan	Network Protocols
5	Tues	30-Jan	Find the target
6	Thurs	1-Feb	Network scanning
7	Tues	6-Feb	Network scanning
8	Thurs	8-Feb	enumeration
9	Tues	13-Feb	Authentication
10	Thurs	15-Feb	Authentication
11	Tues	20-Feb	Authentication attacks
12	Thurs	22-Feb	Authentication defenses
13	Tues	27-Feb	Authentication defenses
14	Thurs	29-Feb	**Test 1**
15	Tues	5-Mar	Web Attacks
16	Thurs	7-Mar	Web Attacks
	Tues	12-Mar	Spring Break
	Thurs	14-Mar	Spring Break
17	Tues	19-Mar	Remote access
18	Thurs	21-Mar	Firewalls
19	Tues	26-Mar	Firewalls
20	Thurs	28-Mar	Hacking a system
21	Tues	2-Apr	Email
22	Thurs	4-Apr	Email
23	Tues	9-Apr	Network protection
24	Thurs	11-Apr	Intrusion detection
25	Tues	16-Apr	Intrusion Prevention
26	Thurs	18-Apr	Data Loss Protection
27	Tues	23-Apr	Trapping a hacker
28	Thurs	25-Apr	Encryption tools
29	Tues	30-Apr	Forensics
30	Thurs	2-May	**Course wrap-up**
			Final exam Format TBD