Fall 2013

CEG 4420/6420-01: Host Computer Security

Prabhaker Mateti
Wright State University - Main Campus, prabhaker.mateti@wright.edu

CEG 4420/6420: Host Computer Security

Syllabus

Catalog Description: This course introduces security hardening of a single system, and how to protect it when connected to a network. It explains how malware can compromise security and privacy from the moment a machine is powered on until shut down. Topics include Privilege Escalation, Buffer Overruns, Network Packet Mangling, Session Hijacking, Firewalls, and ethics. Lab work uses tools such as nmap and Kali (BackTrack) Linux. **Prerequisites**: CEG 4350

Source Material

There is no required text book this term.

Home Page
http://www.cecs.wright.edu/~pmateti/Courses/4420 Please visit often this page for announcements, and info on notes.

Simson Garfinkel, Gene Spafford, and Alan Schwartz
Practical Unix and Internet Security, 3rd edition (2003), O'Reilly & Associates; ISBN: 0596003234. A *recommended* text book. Errata Previous Editions: http://www.oreilly.com/catalog/puis/errata/
http://proquest.safaribooksonline.com.ezproxy.libraries.wright.edu:2048/ book/ networking/ security/0596003234

Charles P.Pfleeger, Shari Lawrence Pfleeger,
Security in Computing, Fourth Edition, Prentice Hall, 2006, ISBN-10: 0-13-239077-9. A *recommended* text book.
http://proquest.safaribooksonline.com.ezproxy.libraries. wright.edu: 2048/ book/networking/security/0132390779

Attendance

Full attendance is expected.

Course Content

Lab work is a significant part of this course. The ordering of lectures, in contrast to the course content topics listed below, is largely due to this influence.

The topics are described at some length because they may be too unfamiliar to you. The numbers in parens are a rough estimate of the number of (75-minute) lectures on each topic.

Intro (1)

Well Known Security Breaches. The most famous incidents. The Internet Worm, 1988. Current events. Terminology: E.g., Intruder v. Hacker v. attacker v. cracker. Course overview.

System Administration (2)

Linux setup. The initial boot can be a significant source of insecurity. The sequence of events from initial power-on cold booting to shut down of a computer system. Standard Unix processes: `init, getty, inetd, rpc.*` etc. Introduction to network setup. TCP/IP refresher. Virtual machines.

Applied Cryptography (1)

Understanding computational infeasibility. Message digests. Digital certificates. Man-in-the-Middle attacks.

TCP/IP Exploits (2)

Modern operating systems are internally organized as a networked collection of servers, even when not connected to other

machines. Service and node authentication. Probing a Host for Weakness. Remote Trojans. Causing service denials. Denial of Service Attacks. Distributed coordinated attacks. Sniffing. Spoofing. Secure shell. Secure Socket Layer (SSL). Virtual Private Networks (VPN). IPv6.

Authentication (3)

User Authentication: /etc/passwd, /etc/shadow files. One time passwords. Semi-permanently assigned password, and a response token generated by credit-card-sized electronic authenticators. Two-factor authentication. Cracking of passwords.

System Hardening (8)

Escalation of privileges. Denial of Service (DoS). Virus, Worms, and Trojan Horses. The structure of a computer virus. Manipulation of executable binaries. Anti-virus programs. Configuring properly. Hardening an OS. Re-design of OS for security. NSA's Security Enhanced Linux. Absense of Root kits, unauthorized services, Backdoors. Honey pots. Prevention and detection of malware.

Secure Software Development (6)

Buffer Overflow Exploitation. Software development techniques that are resistant to bug exploits. At the high-level, code structure, least privilege, and narrow interfaces, and at the low-level, checking for buffer overruns, being ultra careful in writing setuid programs, untrusted paths, race conditions, environment, etc. Type-safety, source code analysis, assertions and invariants. Prevention and detection of race conditions.

System Audit (2)

Detection and Documentation of (possible) Intrusions. Penetration testing. Logging facilities. Intrusion Detection Systems (IDS). Intrusion Prevention Systems (IPS). Forensics.

Ethical and Legal Issues (2)

We will discuss topics such as: Why Hackers Do The Things They Do? Is it OK to harden the PC of a neighbor without permission? It is required that you sign our statement of ethics.

Exams 20 + 30%

There will be two exams contributing 20% and 30% to the final grade. The mid term is scheduled around the sixth week, and the final during the exam week as set by the Registrar.

Laboratory Experiments 48%

The laboratory experiments contribute 48% to the final grade. I expect to give 12 experiments worth 4% each. Lab reports must be submitted by midnight on the due date posted. I will accept up to two lab reports late but each within 48 hours. The subject matter of these experiments is included in the exams.

All lab work must be, with a couple of exceptions, conducted within the Operating Systems and Internet Security (OSIS) Lab. No other WSU facilities are allowed.

In this course, a lab rarely involves writing your own programs. It generally will require you to build an executable after suitable reconfiguration using tools such as make. The source code tree will be given to you. The code is in C/C++, Java, or in (one or two cases) ASM code.

Most experiments are to be performed by the student individually with a few that are best learned when there is a pair of students. These labs must be work done *solely by you (and your partner)*, except for the parts I provided you with.

Discussion 2%

Active participation in the group discussions is expected.

Homework Assignments

There are no homework assignments to be turned in.

CEG 6420

Students enrolled in CEG 6420 are required to do an additional task. This quarter the task is to (i) learn and write a technical summary in a few pages on one of the topics below, (ii) sketch a new lab experiment based on that topic, and (iii) carry out that experiment and submit a lab report as usual. Your article and lab experiment should look like one of those already included in the course. If a topic beyond this list interests you, let us consider it.

1. Linux Intrusion Detection Systems.
2. Intrusion Detection and Logging using Linux Snort
3. Hardening a well-known Linux distribution, e.g., Kali or Knoppix

---