

COURSE DESCRIPTION

| | | | |
|----------------|----------------|--------------------|--|
| Dept., Number | CSC 154 | Course Title | Computer System Attacks and Countermeasures |
| Semester hours | 3 | Course Coordinator | Isaac Ghansah |
| | | URL (if any): | http://gaia.ecs.csus.edu/~ghansahi/ |

Catalog Description

An introduction to network and computer security with a focus on how intruders gain access to systems, how they escalate privileges, and what steps can be taken to secure a system against such attacks. Topics include: Perimeter Defenses, Intrusion Detection Systems, Social Engineering, Distributed Denial of Service Attacks, Buffer Overflows, Race Conditions, Trojans and Viruses. Prerequisite: At least a C- in CSC 138 or CPE 138.

Textbook

Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed, 5th Edition, Osborne McGraw-Hill, 2005.

References

Charles P. Pfleeger, Security in Computing, Third Edition, Prentice Hall, 2003.

Kevin D. Mitnick, William L. Simon, The Art of Deception, Wiley, John & Sons, 2002.

Course Goals

1. To provide experience in analyzing and identifying vulnerabilities in systems or networks.
2. To introduce the computer science student to career paths in Computer and Network Security.
3. To provide experience in performing a security audit of computers and networks.
4. To expose the student to the domains of knowledge and skills required for Information Systems Security.

Prerequisites by Topic

Thorough understanding of:

- TCP/IP and WAN/LAN Technologies.
- How to compile and run programs in Linux and Windows.

Basic understanding of:

- NetBIOS and Windows file sharing.
- Domain Name System (DNS).
- Host and Network Configuration Protocols (ARP, RARP, BOOTP, DHCP).
- Unix operating system and/or Windows operating system.

Exposure to:

- IPv6 and IPsec.

Major Topics Covered in the Course

1. Ethics and Law. (3 hours).
2. Footprinting, Scanning, Enumeration. (9 hours).
3. Computer Systems Attacks. (3 hours).
4. Trojans and Backdoors. (3 hours).
5. Sniffers, Intrusion Detection Systems, Firewalls and Honeypots. (3 hours).
6. Denial of Service. (3 hours).
7. Social Engineering. (3 hours).
8. Session Hijacking. (3 hours).
9. Attacks on Web Servers, Web Applications Vulnerabilities. (3 hours).
10. Introduction to Cryptography. (3 hours).
11. Web Based Password Cracking Techniques. (3 hours).
12. SQL Injection, Buffer Overflows. (3 hours).
13. Viruses and Worms. (3 hours).

Outcomes

Thorough understanding of:

- Three fundamental steps that a hacker performs.
- Software security design flaws.
- Tools hackers use in conducting attacks.

Basic understanding of:

- Host and network intrusion detection systems.
- Tools and methods of protecting computers and networks against hacker attacks.
- Malicious code.
- Legal and ethical practices in security.

Exposure to:

- Security incident investigation.
- Preparation of electronic evidence.

Laboratory Projects

All security-related projects will be in a closed laboratory environment:

1. Download, uncompress and install an Open Software Unix password-cracking program and crack any weak passwords in a test file. (1 week).
2. Use a scanning tool such as “nmap” to scan target system. (2 weeks).

3. Use such a tool as “nessus” to identify security weaknesses and warnings in Windows and Unix target systems. (2 weeks).
4. Configure firewall to filter traffic. (2 weeks).
5. Use tools to overflow a buffer in target systems. (2 weeks).

Estimated Curriculum Category Content (Semester hours)

| <i>Area</i> | <i>Core</i> | <i>Advanced</i> | <i>Area</i> | <i>Core</i> | <i>Advanced</i> |
|-----------------|-------------|-----------------|-----------------|-------------|-----------------|
| Algorithms | | | Data Structures | | |
| Software Design | 0.1 | | Prog. Languages | | |
| Comp. Arch. | | | | | |

Oral and Written Communications

Students will write a paper and give oral presentations on an appropriate security topic.

Social and Ethical Issues

1. Discussions on Federal Laws Section 1029 and Section 1030.
2. Discussions on State of California Penal Code Section 502.

It will be made clear that the students should not use their knowledge and skills with any malicious intent against the university network, any other networks, physical computing resources, or humans. Students will be required to sign an agreement to observe a set of legal and ethical guidelines.

Theoretical Content

The course uses cryptographic algorithms applied to secure communication.

Problem Analysis

Each network attack method will be analyzed in a rigorous manner. Effectiveness of the defensive measures shall be evaluated.

Solution Design

Students will learn how to discover the vulnerabilities and how to develop techniques to protect the networks.