

Teaching Hacking at College

Sam Bowne

Computer Networking and Information Technology

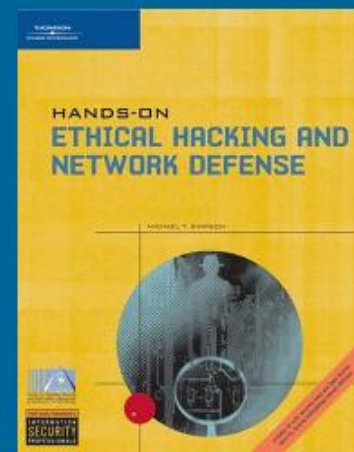
City College San Francisco

New Class at CCSF

CNIT 123: Ethical Hacking and Network Defense

Students learn how hackers attack computers and networks, and how to protect systems from such attacks, using both Windows and Linux systems. Students will learn legal restrictions and ethical guidelines, and will be required to obey them. Students will perform many hands-on labs, both attacking and defending, using port scans, footprinting, exploiting Windows and Linux vulnerabilities, buffer overflow exploits, SQL injection, privilege escalation, Trojans, and backdoors.

Prerequisites: CNIT 106 and 120 or equivalent familiarity with the fundamentals of networking and security.



Hacking is Built into Our Program

Courses Required for the Certificate of Completion in Network Security

Course	Units
CNIT 106 Introduction to Networks	3
CNIT 108 Wireless Networks, Advanced	3
CNIT 120 Network Security	3
CNIT 122 Firewalls	3
CNIT 123 Ethical Hacking	
or CNIT 221 Cisco PIX firewall & Router Sec ...	3
Total Units	15

Why Teach Hacking?

- Lectures aren't enough
- Students need **hands-on labs**
- Practice attack and defense
- Hacking is new and exciting
- Even professional network admins don't know hacking

Isn't Teaching Hacking Dangerous?

- Criminal hackers don't go to college to learn it
- The good guys need to learn it too
- Discussing the issues openly is better than forcing students to learn it outside class

Level of Course

- Prerequisites: **Network+** and **Security+**
- No programming
 - We don't create exploits
- We just use existing tools, like "script kiddies"
- Each project shows **vulnerability, attack, and defense**

The Hacking Lab

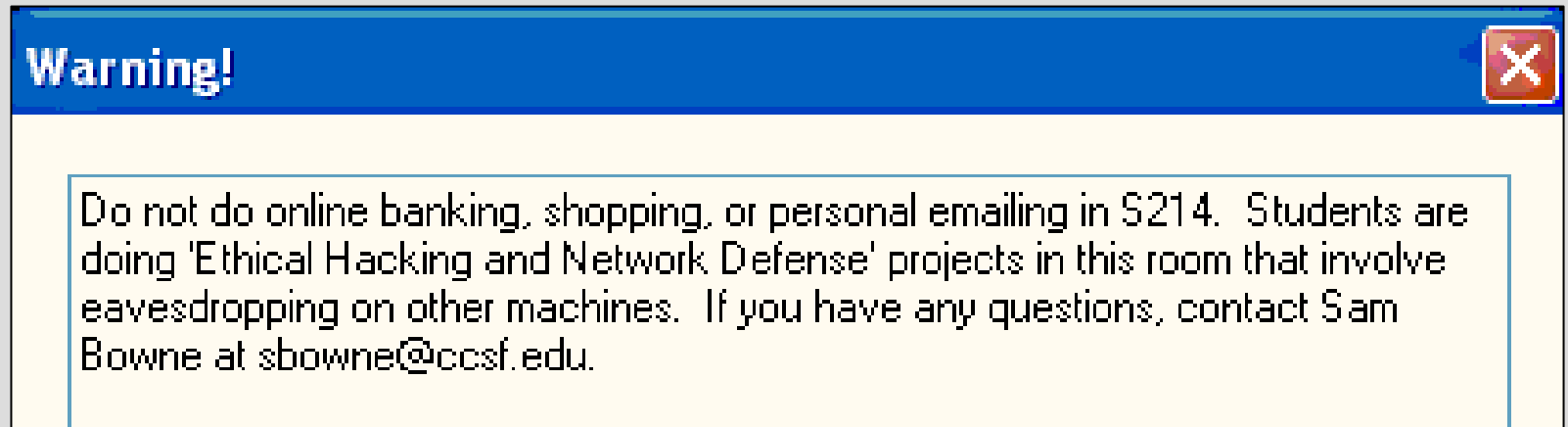
- Host systems:
 - Windows XP, 1 GB RAM, 2.2 GHz Pentium 4
 - 20 GB System drive, 80 GB drive for VMs
- Each student has a folder with three VMware virtual machines
 - Windows XP
 - Windows 2000 Pro
 - Ubuntu Linux

Internet Connection

- A single ZyXel router connects the lab to the Internet
- Upstream bandwidth throttled to 128 kbps
 - To protect the Net from the lab

Warnings

- Each student signed a "Code of Ethics" agreement
- Warnings posted in lab and on screens at boot-up



Student Assistants

- Student volunteers monitored the lab, and had keys
- The lab became a hangout for hackers
- None of the equipment was broken or stolen
- Morale was high

Projects: Attacks

- **Metasploit**
 - Taking Over a Windows 2000 box from Windows XP
 - Taking over a locked Windows 2000 box from Linux
- Performing a Denial of Service attack on a Web Server with Nmap
- Rootkitting Ubuntu Linux (and fixing it)
- Basic Website hacking with HackThisSite.org



Projects: Finding Vulnerabilities

- Port Scanning with Nmap
- Analyzing Port Scans with Wireshark
- Testing Firewalls
- NetBIOS Null Sessions
- Nessus Vulnerability Scanner
- Microsoft Baseline Security Analyzer (MBSA)
- Winfingerprint

Projects: Stealing Passwords

- Ettercap
- Software and Hardware Keyloggers
- Ophcrack
- Cain and Abel
- John the Ripper

Projects: Bypassing Passwords

- Ubuntu Linux
 - Live CD and mount
 - Using **recovery mode**
- Windows
 - Ultimate Boot CD

Results of the Class

- 80 students took the class
- 40 of them passed (a typical success rate)
- No security incidents
- Very high enthusiasm and praise from the students
- A lot of interest in more advanced hacking classes

Conclusion

- Teach Hacking!
- High rewards, no problems
- BUT:
 - CCSF is different from four-year colleges
 - Our students are typically working professionals
 - Students in dormitories may get into more mischief

Credits

- Supported by the **Institute for Convergence of Optical and Network Systems (ICONS)**
 - Funded by **NSF**
- Encouraged and hosted by the **Computer Networking and Information Technology Department**
 - Especially Carmen Lamha and Pierre Thiry

Contact Information

- Sam Bowne
- Website: **samsclass.info**
- Email: **sbowne@ccsf.edu**