Black Hat/White Hat: An Aggressive Approach to the Graduate Computer Security Course

Jim Aman
Saint Xavier University
CONTENT

- Some Background
- The Rationale
- The Course
- The Audit Exercise
- Conversation
BACKGROUND

• Saint Xavier University

• Computer Science Department:
  Computer Science & Computer Studies
  Master of Applied Computer Science

• Facility: The “Sandbox”
RATIONALE

• John Aycock and Patricia Logan – SIGCSE '05
• Aggressive vs. Passive

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.”
THE COURSE: Books
THE COURSE: Facilities

- Older PCs
- Windows 2000 & Linux
- Hub
- Normally isolated ("sandbox")
THE AUDIT EXERCISE

• Charge:

1) Crack the firewalls guarding the target department
2) Gain access to as many of the computers in the target as possible
3) Continuous activity logging
4) Presentation of final report
THE AUDIT EXERCISE

• Limitations:

1) No dumpster diving or personal social engineering
2) No tampering with files or computers
3) Must sign non-disclosure agreement first
THE AUDIT EXERCISE

• Report:

1) Routers were secure
2) School's default administrative password scheme must be changed
3) Target department extremely vulnerable
4) Recommended corrective actions for each vulnerability
THE AUDIT EXERCISE

• Aftermath:

1) School's default administrative password scheme changed
2) Target department adopted every recommendation (and more)
3) The “rumor mill”
UPDATE

• Is there a middle ground?

• Next spring:
  
  Laptops
  
  VMware
  
  Win2K, WinXP, Linux
CONTACT INFO

Jim Aman
Saint Xavier University
3700 West 103rd St.
Chicago, IL 60655
(773) 298-3454

csmaster.sxu.edu/aman

blackboard.sxu.edu
(csvisitor/csguest – Web Server Security)
CONVERSATION