# Security Assessments

## The Baylor University Experience

# Baylor in Overview

- 13,800 students, 2000 employees
- 85 buildings networked
- Server farm in DMZ

# Why an Assessment?

- Helps you stay out of the news!
- Legal and PR issues
- Defines a baseline for Risk Level

# Choosing a Vendor

- Unbiased look at your system
- Expertise, experience
- Documentation -- Formal report
  - Good -- documents your vulnerabilities, engages your people.
  - Bad -- documents your vulnerabilities, now you're on the hook!

# Three types of vendors

- Tier Three
  - Relatively inexpensive
  - Relatively limited in scope, results.
- Tier Two
  - External and internal scans
  - medium to high cost.

# The High Priced Spread

- Scope, scans are customizable
- Verification of vulnerabilities
- Detailed (380pp!) report with recommendations

# Take-Away Lessons

- It's about trust and confidence
- Remember non-disclosure agreements
- Redefine scope after first meeting
- Watch those sensitive times -- things may break!
- Name a point person to handle ALL issues

# Take-away Lessons

- Social engineering will go on. Put 'em in a hidden location, don't warn rest of CIT.
- Social engineering is scary stuff!
- It takes a while, 2 weeks off-campus, 2 weeks on.
- Prioritize vulnerabilities and remediation

# Was it worth it?

- Got the attention of the right people
- Be inclusive of findings
  - IT personnel
  - Departmental IT personnel
  - General Counsel
  - Executive staff
- Multi-year agreement can reduce cost

# The BotHerd is Coming

University of Albany

Martin Manjak, ISO,
Justin Azoff, Network Analyst

# About UAlbany

- 17,400 students, 700 faculty, 8000 residents
- September 2004
  - over 800 systems booted from network
  - 1000+ open tickets first week of class
  - 3 week wait for remediation appointment

# Never Again!

- Technical Track (later)
- Social Engineering Track
  - More about people than technology
  - Never stop working on awareness

# Need a Narrative

- "Didn't you read the letter we sent?"
- Technology is a turn-off to many.
- Craft a narrative where students can self-identify, "Did you hear the story about..."
- Focus on behaviour and change

# Design is Key

- Attractive format, good graphics
- People, not screen shots.
- Series of brochures were created
  - Trade 'em, collect the whole set!
- Advertised the Network Survival Kit

# The Security Quiz

- Online Quiz in Ethics and Security
- Required to gain Network access
- Must get 10 out of 10 right to pass
- Using the network means you passed, therefore you know the requirements, so
- No excuses when you're kicked off.

# 2004 vs. 2005 Results

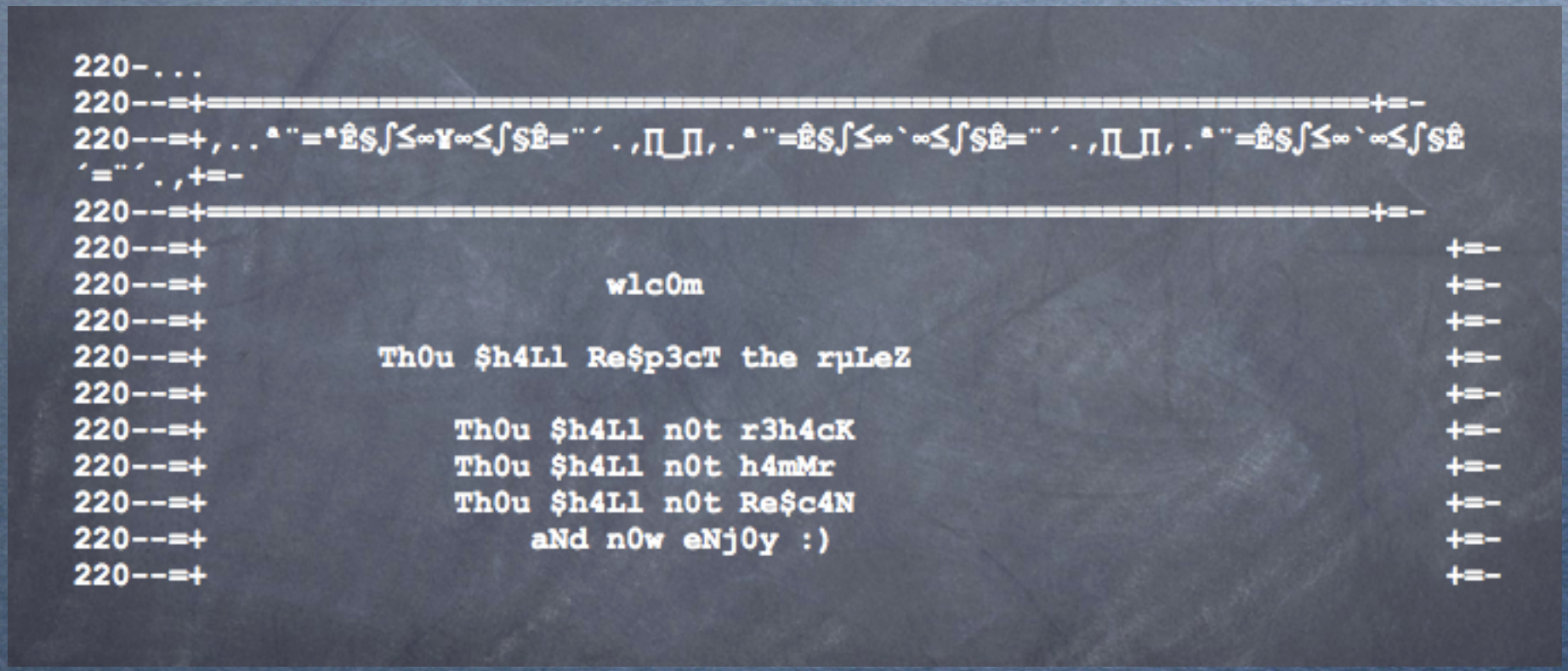
- Cut September's trouble tickets in half
- While network registrations increased 23%

# Technology lags education

- XP SP2 Firewall, patches responsible for some reduction in vulnerabilities, but
- New threat vectors (AIM, Web links) are emerging.
- Patches won't stop students (and staff!) from clicking
- Firewall on -- unable to scan it.

# Technical Measures

- 80k HTTP flows and 1 IRC? (not 6667)
- Never-admit IRC on Packetshaper, with a whitelist of servers
- Scan IPs using blocked IRC, collecting banners, if open.
- Interesting things can be observed...




# Not your father's FTP server

# IRC Bots come in 2^32 types

- Bots have one or more C&C IP addresses embedded in them
- IP based
  - Whack-a-mole, easy to detect
- DNS based
  - HA, load-balanced, redundant botnet!

# You.GotPwndBy.us

- When DNS bots wake up, they must resolve that C&C address.
- Log your DNS queries
  - Frequent flyers, bad hostname list
  - hosts in .info, .us, .cx, not .com, .edu
- IDS, IPS also a help (they didn't have)

# Resources

- Conference site: http://www.educause.edu/Program/8355
- Botnet slides: http://www.albany.edu/~ja6447/educause/
- UNiversity Security Operations Group, unisog@lists.sans.org (http://www.dshield.org/mailman/listinfo/unisog)
- SECURITY@listserv.educause.edu
- REN-ISAC, http://ren-isac.net/

# Shameless Plug

Suggestions? Comments?

Smaller Colleges -- Interested?

Presentation Topics, Tracks, Training?