Collective Views of the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives

William J. Adams[†]
Tim Lacey[¶]
Efstratios L. Gavas[‡]
Sylvain P. Leblanc[§]

[†]United States Military Academy
[‡]United States Merchant Marine Academy
[¶]Air Force Institute of Technology
[§]Royal Military College of Canada

USENIX CSET 2009

Outline



Objective of Paper

- Discuss the *Cyber Defense Exercise* (CDX)
- Review curriculum
- Promote hands-on IA activities
- Show flexibility of cyber security exercises

Overview of CDX

- Four-day exercise, but months of preparation
- Ninth year of competition
- Red vs. Blue, with White moderating

Overview of CDX

- Eight teams participated:
  - Air Force Institute of Technology (AFIT)
  - Naval Postgraduate School (NPS)
  - Royal Military College of Canada (RMC)
  - United States Air Force Academy (USAFA)
  - United States Coast Guard Academy (USCGA)
  - United States Merchant Marine Academy (USMMA)
  - United States Military Academy (USMA)
  - United States Naval Academy (USNA)
- Participation at both graduate and undergraduate levels

Overview of CDX

- Each team is given a mock budget to secure a poorly-configured/compromised network
  - Email, instant messaging, database and web servers, workstations, and a domain controller
- Administer network while under attacks by NSA Red Team
- Deal with exercise "*injects*"
  - Forensics, helpdesk requests, DNS and network reconfiguration
- Reporting requirements

The Differences

- Different curricula
- Different learning objectives
- Different resources

USMMA Overview

- Established to train Merchant Marine officers
  - Part of the Department of Transportation
- Smallest of the five US undergraduate service academies
- In the *Heroic*[1] phase of security team building
  - . . . Possibly the *Incompetence* phase!

[1] http://taosecurity.blogspot.com/2009/05/lessons-from-cdx.html

How They Came to Their Design

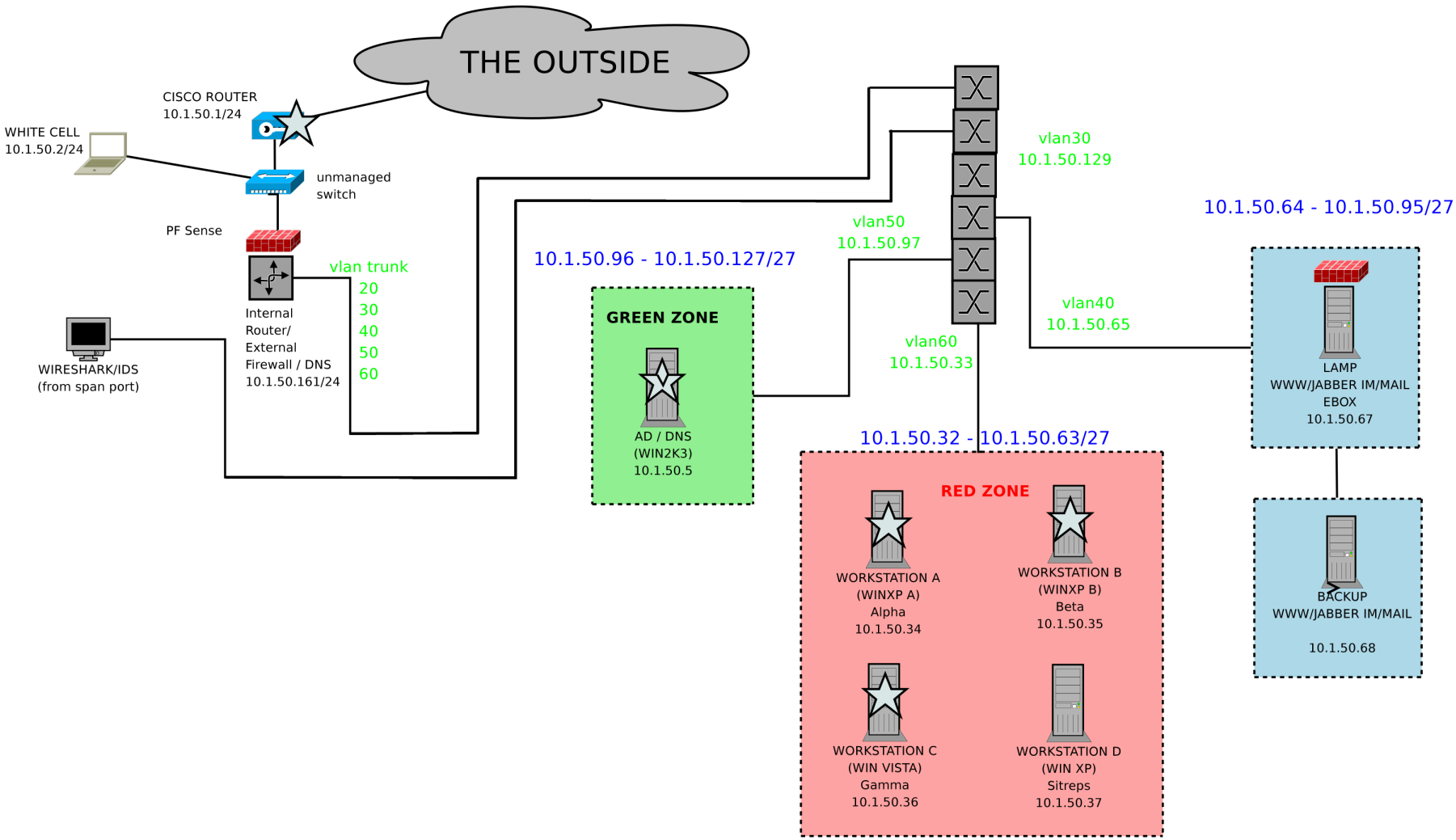
- Cost Trade-Offs
- Administrative Trade-Offs
- Monitoring Trade-Offs

- Mistakes Made
- Last-Minute Course Corrections



Review of USMMA Network Design

Keep It Simple, Sailor



USMMA Summary

- We do *OK*
- Simplicity was our weapon of choice
- If you don't understand it – it is *not* secure!
- Don't be afraid of your system

USMA Overview

- Serves as a senior-level capstone
- Active ACM and CS programs
- Large team size (30-60 people)
- Supported through the *Information Technology and Operations Center* (ITOC)

USMA Observations

- Cleaned workstations with homemade *Tripwire*-like script
- Rebuilt database and web servers
- No significant compromises
- Communication was a special focus


AFIT Overview

- Graduate program
- Focus on lab activities
- Range of skills (novice to network administrator)
- Two teams of fifteen
- Supported through the *Center for Cyberspace Research* (CCR)

AFIT Observations

- Effective use of IPsec
- Utilized proxy server
- Mitigated compromises with user privileges




RMC Overview

- First year competing
- Mixed graduates and undergraduates
- Only graduate participation this year

RMC Observations

- First time working in a *Network Operations Center* (NOC)
- Reinforced communication needs

Attacks

What happened?

- Twenty-one significant, distinct compromises
- Most effective: *Malware callbacks (7)*
- Most interesting: *OpenFire remote access (4)*

A lot to keep track of . . .

Conclusions

- Budget and operational issues are important
  - Fewer successful attacks
  - Wider range of attacks
- Hands-on activities can better direct student
- Live exercises build critical skills
  - Communication
  - Operations
  - Leadership

Summary

More information

- http://www.afit.edu/en/ccr/
- http://www.itoc.usma.edu

Final Words. . .

- If you hack boats or students, contact me (gavase{at}usmma[.]edu)
- Suggestions welcome