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
Collective Views of the CDX

Outline

Introduction

Overview
- What is the CDX?

Academies’ Experiences
- United States Merchant Marine Academy
- United States Military Academy
- Air Force Institute of Technology
- Royal Military College of Canada

Attacks
- What happened?

Conclusions
Collective Views of the CDX

Introduction

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 “injests”
  - 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

THE OUTSIDE

GREEN ZONE

AD / DNS
WIN2K3
10.1.50.5

WORKSTATION A
WINXP A
Alpha
10.1.50.34

WORKSTATION B
WINXP B
Beta
10.1.50.35

WORKSTATION C
WIN VISTA
Gamma
10.1.50.36

WORKSTATION D
WIN XP
Sitreps
10.1.50.37

RED ZONE

10.1.50.96 - 10.1.50.127/27

10.1.50.97

10.1.50.32 - 10.1.50.63/27

10.1.50.64 - 10.1.50.95/27

LAN
WWW/JABBER IM/MAIL
EBOX
10.1.50.67

LAMP
WWW/JABBER IM/MAIL
10.1.50.68

BACKUP
WWW/JABBER IM/MAIL
10.1.50.68

WIRESHARK/IDS
(from span port)

PF Sense

Internal Router/External Firewall / DNS
10.1.50.161/24

unmanaged switch

WHITE CELL
10.1.50.2/24

CISCO ROUTER
10.1.50.1/24

vlan trunk
20
30
40
50
60

vlan 30
10.1.50.129

vlan 50
10.1.50.127

vlan 60
10.1.50.33

10.1.50.65

10.1.50.129
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)
Collective Views of the CDX

Academies’ Experiences

United States Military Academy

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