

Asymmetric Defense

How to Fight Off the NSA Red Team with Five People or Less

Efstratios L. Gavas

Department of Marine Transportation
United States Merchant Marine Academy

DEFCON 17



Outline

Introduction

- What is the Point?
- About the USMMA
- About the CDX

Network Design

- Overview of Network Design

Quick Guides

- Operating Systems
- Tools
- Network
- Application Servers
- FreeBSD



What I hope you take away

- ▶ Simplicity is the only way to save yourself
- ▶ **If you don't understand it – it is *not* secure!**
- ▶ Don't be afraid of your system



What is the CDX?

- ▶ A week-long, annual information security event for students from various military institutions
 - ▶ 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)



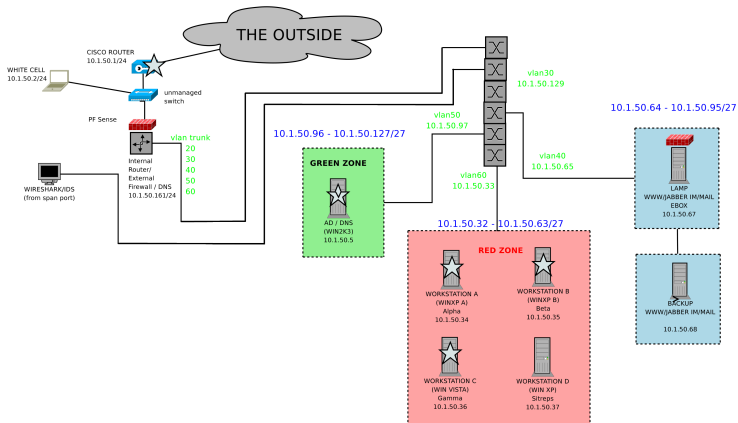
What is the CDX?

- ▶ 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
- ▶ Administrate network while under live-attacks from NSA Red Team
- ▶ Deal with exercise “*injects*”
 - ▶ Forensics, help-desk requests, DNS and network reconfigurations
- ▶ Reporting requirements



Review of USMMA Network Design

Keep It Simple Sailor



Learn multiple OS'es

Variety is good

- ▶ Lots of OS'es for lots of different jobs
 - ▶ Ubuntu, FreeBSD, OpenBSD, Solaris, MacOS, DSL...
- ▶ Look at the NSA guides for some secure configuration
 - ▶ www.nsa.gov/ia/guidance/security_configuration_guides/



Learn about multiple OS'es

But you can't forget about Windows

- ▶ Use Group Policies
- ▶ Don't get carried away with Group Policies
- ▶ Vista is OK... for security



A Simple Tool is a Useful Tool

- ▶ SysInternals
- ▶ Firewall/IDS
 - ▶ Internal Firewall, Core Force
- ▶ Anti-virus Scanner
 - ▶ Ad-Aware, AVG (don't go scan crazy)
- ▶ Pass-phrases vs passwords



Layout of the Network

Logical and Physical

- ▶ VLANs or,
- ▶ Real LANs

This option exist for small networks



Firewall/Gateway Applications

Survey of Firewall/Gateway Applications

- ▶ m0n0wall
- ▶ IPCop
- ▶ Untangle
- ▶ pfSense



Application Server Tools

Survey of Application Server Tools

- ▶ eBox
- ▶ Webmin
- ▶ Untangle



Don't be Afraid of FreeBSD

Boris Kochergin teaching us how to fish...



Using FreeBSD for routing

FreeBSD vs m0n0wall

- ▶ NAT
- ▶ VLANs
- ▶ pf *AND* ipfw



Using FreeBSD for Application Servers

FreeBSD vs eBox

- ▶ Email
- ▶ Webserver
- ▶ Database
- ▶ Jabber



Summary

With a small team, and a limited budget, simplicity is critical.

- ▶ Use the simplest possible security, but no simpler.
- ▶ Remember, **if you don't understand it – it is *not* secure!**
- ▶ Security is about exploration. Jump in, and don't panic.

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

