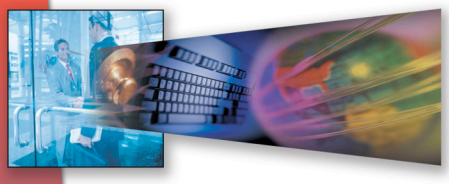


INTEGRITY, STEALTH AND SKILL

TeamDefend

Organizational and Inter-Organizational Cyber Defense Training

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

Agenda

- Background on Cyber Exercises
- Introduction to TeamDefend
- Conduct "Mini-TeamDefend"

Brief History of Cyber Gaming / Network Defense Exercises

- GetInsight has been running private games for clients since 1994
- DefCon has held a CTF contest each year since 1995
- ToorCon has held a CTF for the past 6 years
- DoD ELIGIBLE RECEIVER exercise was held in 1997
- Annual U.S. Air Force Exercise BLACK DEMON exercise began in 2002
- UTSA held Dark Screen in 2003

Shortfalls of Current Training Options

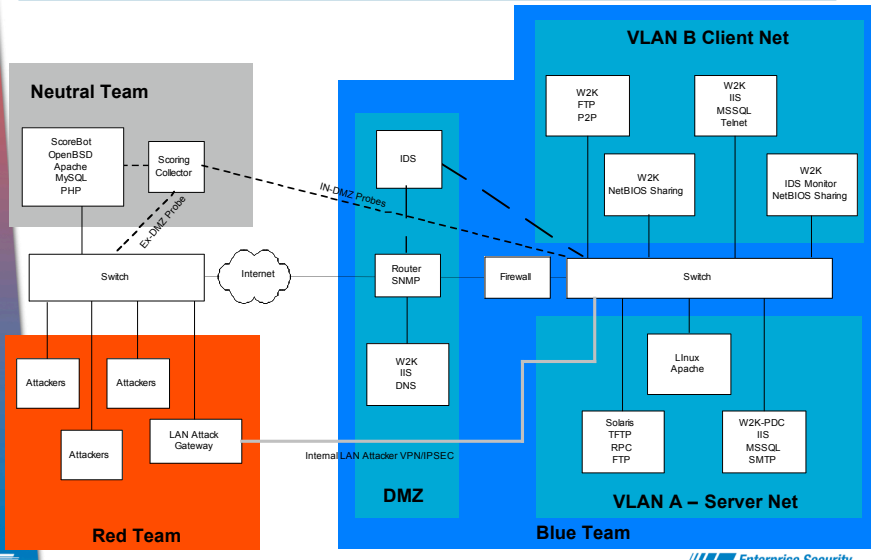
- Not many realistic exercise (non-operational) environments in which to train with reconfigurable targets
- No formalized and repeatable mechanism to conduct routine exercises
- Difficult to send staff offsite for classroom training
- No automated evaluation capability to compare apples to apples performance (trend or vis-à-vis others)
- Overall, no experience with real-world Cyber Threat:
  - *How do you recognize problems that you have never been trained to see?*
  - *How do you fix problems that you have never had to previously solve?*
  - *Once you have been trained, how do you maintain your skills?*

TeamDefend Objectives

Increase operator ability to:

1. **Identify vulnerabilities and lock down systems (network, server and/or workstation) according to the organization's security policy;**
2. **Configure router policies according to the organization's security policy;**
3. **Configure and monitor host-based and network-based intrusion detection systems (IDS);**
4. **Recognize hacker/computer misuse activity;**
5. **Properly respond to hacker/computer misuse activity in accordance with organization's policies; and,**
6. **Conduct forensics and collect data for litigation.**

Example TeamDefend Training Infrastructure



Impact to Op Environment: NONE

- TeamDefend is:
  - Self-contained training system
  - Never touches operational environment
  - Uses mobile container on-site and VPN for follow-on training sessions
  - Emulates customer's operational environment using standard Windows, UNIX and network devices
  - Can accommodate some customer-unique systems with advanced planning

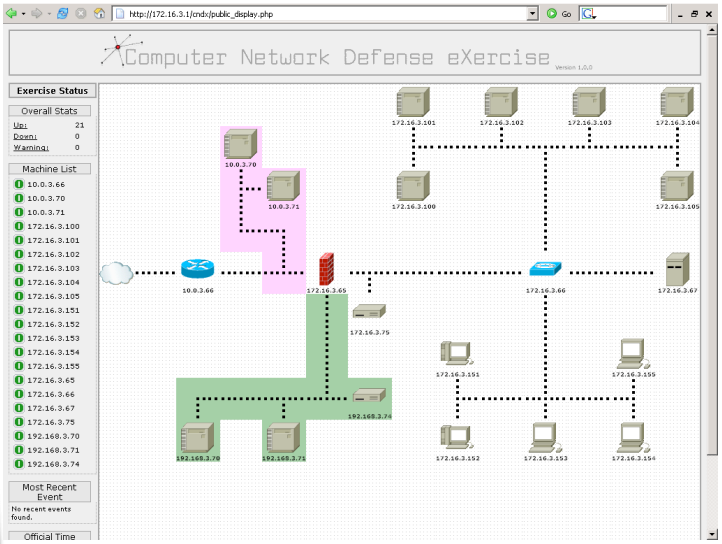
Mobile Training System

- Sun Fire Blade Platform
  - (2) Intel Blades - White
  - (1) Sparc Blade - White
  - (9) Intel Blades - Blue
  - (2) Sparc Blades - Blue
- 3Com 24 port switch
- Cisco PIX 515 firewall
- Cisco Router
- Integrated power filtration
- Roll away 21U Chassis

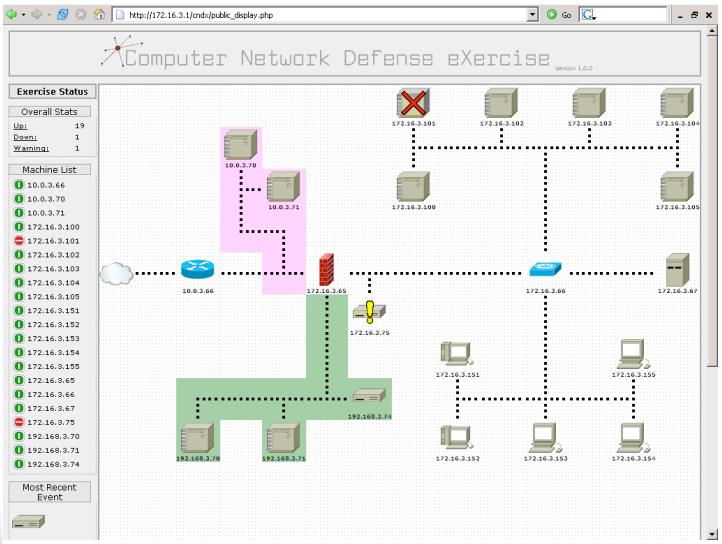
TeamDefend Exercise Controls

- Rules of Engagement
- Exercise Objectives
- Measures of Performance
- Target Configurations
- Communications Plan

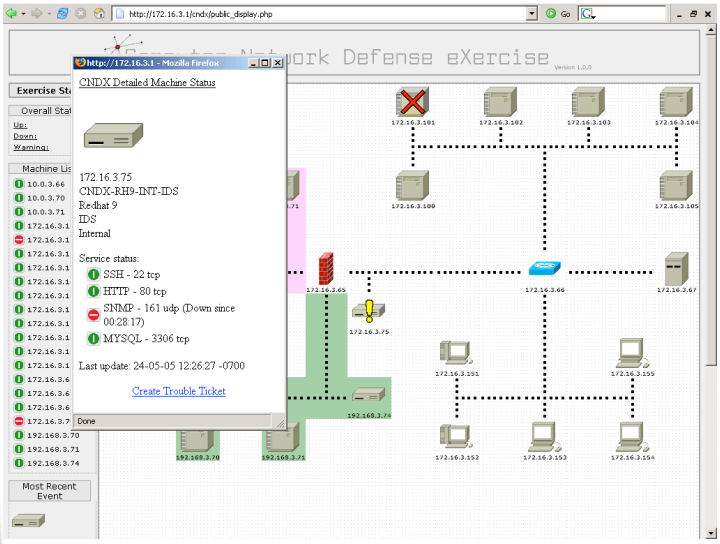
Network Management Interface



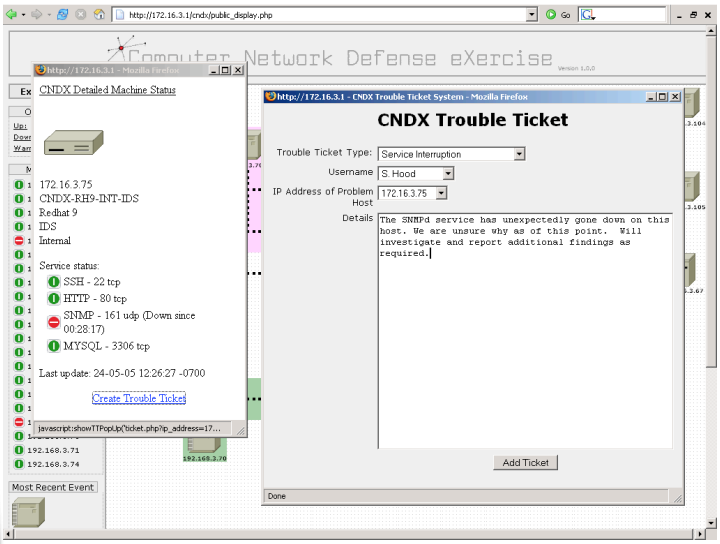
Network Management Interface



Network Management – System Status



Network Management Trouble Ticket Reporting



Measures of Performance

- Quantitative
  - Time to detect system vulnerabilities
  - Time exploit initiation to time detected
  - Time exploit detected to time corrected
  - Time to complete incident handling
  - Percentage of exploits detected and correctly diagnosed
  - Percentage of exploits corrected
  - Percentage of services impacted
- Qualitative
  - Impact of downed services
  - Apparent knowledge of student to detect and fix vulnerabilities
  - Apparent knowledge of student to use detection/monitoring systems

TeamDefend Scoring/Evaluation

- Aids instruction
  - Gives instructors real-time view into exercise
  - Permits identification and focused training on weak areas during the exercise.
- Provides measurement of team performance
  - Tracks multiple values over time
  - Quantitative measure of ability to keep the business operational
  - Permits performance trend analysis to measure progress
  - Shows ebb & flow of team focus during exercise
  - Allows evaluation against best practices
- Provides a reliable, repeatable scoring of teams
  - Evaluates performance across multiple factors
  - Complete history of exercise
  - Full documentation to put performance in context

Scoring System Detail

- Every 45-60 seconds, scoring system checks:
  - System availability
    - Is the system up or down?
  - Critical service availability
    - Are critical services open?
  - Vulnerability checks
    - Is system vulnerable to predefined vulnerabilities?
  - Based on above criteria, host receives a score on a scale of 0 - 100
  - Score is then weighted based on:
    - Predefined system criticality
    - Exercise time

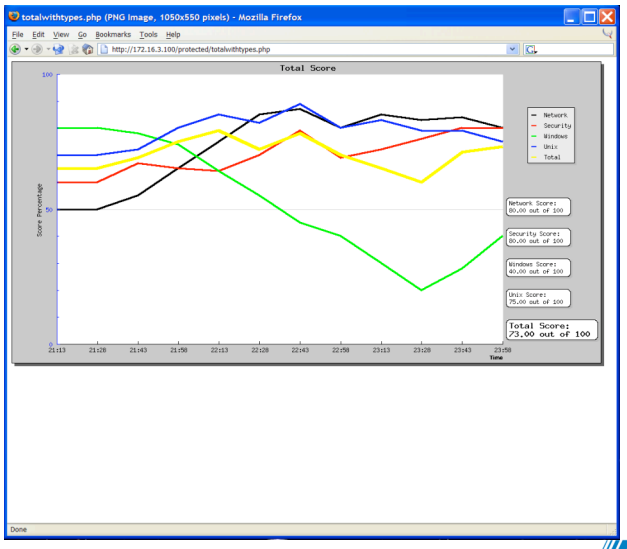
Scoring System Detail

- Score is also affected by:
  - Successful exploitation by Red Team
    - Depends on severity and timing
    - Can lose 1-10% of your score
  - Trouble tickets
    - Incident reporting / mitigation
    - DAA software requests
    - System reconfigurations
    - Can gain OR lose 1-10% of your score – also time dependent

Scoring System Detail

- Categories of scoring are:
  - Overall score
  - System availability
  - Vulnerability rating
- Scores are also broken down by type:
  - Individual host
  - System class
    - Windows, Unix, Network, Security
  - Total

TeamDefend Scoring/Evaluation



Exploits configured in TeamDefend

- 2003/2004 SANS/FBI Top 20 List
  - Top vulnerabilities for 2003 & 2004
  - Released by SANS, US DHS, UK ISCC, Ca OCIPEP
- Common Misconfigurations
  - Default accounts & passwords
- Common Vulnerabilities
  - Buffer Overflows
  - Race Conditions
  - Worms and Virii

SANS 2003 Top 20 Vulnerabilities

Windows

1. Internet Information Server (IIS)
2. Microsoft SQL Server (MSSQL)
3. Windows Authentication (LANMAN)
4. Internet Explorer (IE)
5. Windows Remote Access Service
6. Microsoft Data Access Components (MDAC)
7. Windows Scripting Host (WSH)
8. Microsoft Outlook & Outlook Express
9. Windows Peer to Peer Sharing (P2P)
10. Simple Network Management Protocol (SNMP)

Unix/Linux

1. BIND Domain Name System (DNS)
2. Remote Procedure Call (RPC)
3. Apache Web Server
4. General Unix Authentication
5. Clear Text Services (Telnet/ftp/rsh)
6. Sendmail (SMTP)
7. Simple Network Management Protocol (SNMP)
8. Secure Shell (SSH)
9. Misconfiguration of Enterprise Services (NIS/NFS)
10. Open Secure Sockets Layer (OpenSSL)

SANS 2004 Top 20 Vulnerabilities

Windows

1. Web Servers & Services
2. Workstation Service
3. Windows Remote Access Service
4. Microsoft SQL Server (MSSQL)
5. Windows Authentication
6. Web Browsers
7. File Sharing Applications
8. LSASS Exposures
9. Mail Client
10. Instant Messaging

Unix/Linux

1. BIND Domain Name System (DNS)
2. Web Server
3. Authentication
4. Version Control Systems
5. Mail Transport Service
6. Simple Network Management Protocol (SNMP)
7. Open Secure Sockets Layer (OpenSSL)
8. Misconfiguration of Enterprise Services (NIS/NFS)
9. Databases
10. Kernel

TeamDefend Training Process

- Train in Functional Areas such as:
  - Secure System Configuration
  - Intrusion Detection
  - Incident Management
  - Forensics
- Train in Phases:
  I. Review of Cyber Defense Functions
  II. Walk-though representative exploits/attacks
  III. Conduct full-scale exercise/evaluation
- Provide Exercise Guide

Day 1 Functional Training

- Exercise Overview (50 minutes)
  -- Introduction of selves, students
  -- Goals of the exercise
  -- Scoring system / web interface overview
  -- Network Policy / ROE
- General Security Fundamentals (30 Minutes)
  -- Basic CIA Overview
  -- Overview of Threats, Vulnerabilities, Exploits, and Risk
  -- Security information resources
- Windows Security (90 minutes)
- Unix Security (90 minutes)
- Firewall Configuration Fundamentals (50 minutes)
- IDS Configuration Fundamentals (50 minutes)
- Basics of Computer Forensics (50 minutes)
- Exploits Technologies Overview (50 minutes)
- Toolset Overview (50 minutes)
- Exercise Overview, Policy, Rules of Engagement

Day 2-4 – Hands-On Training

- Completion of Day 1 Review.
- Student Network discovery
- Exercise play
- Hot wash/ Out Brief of exercise

TeamDefend User's Manual

- Executive Summary
- Exercise Concept of Operations
- Exercise Organization Security Policy
- Exercise Rules of Engagement
- Training Systems Configuration
- Appendix – Description of Exploits
  - Overview of What the Exploit does
  - Where it should be Detected
  - How to Mitigate it
  - What Data to Collect

Remote Training Subscription

- Simple and inexpensive, permits training from customer site.
- Reinforces previous training to improve and measure progress
- Permits training against emergent real-world exploits
- Can focus training on improving skills in Intrusion Detection, Forensics, and Incident Handling
- Useful as a follow-up to incidents

"Train as you Fight"

- Train against real-world, live cyber threat
- Train onsite; no travel required
- Train/Exercise Cyber Defend Functional Skills
- Train safely in self-contained training environment
- Train on systems that are similar to operational environment
- Automate the process of scenario delivery and performance analysis
- Train as a TEAM
- Baseline proficiency against common vulnerabilities and exploits
- Remote training for refresher/update

INTEGRITY, STEALTH AND SKILL

Scott C. Kennedy, CISSP/ISSAP, GCIH
Chief Engineer, Cyber Assurance
Integrated Security & Systems Solutions

scott.c.kennedy@saic.com
858.826.3035

Hart Rossman, CISSP
Chief Technology Officer
Integrated Security & Systems Solutions

hart.m.rossman@saic.com
703.375.2261

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION