2003

CyberCombat

Fulp, J.D.

Monterey, California. Naval Postgraduate School

CyberCombat

Concept

Interested schools/agencies build and maintain exercise networks that will be connected to one another for scheduled, coordinated, and mutually edifying cyber-attack/defend scenarios.

Approach

Participating schools/agencies schedule mutual network security assessment/defense scenarios with one another. Scenarios will be both "canned" (e.g., footprint/scan, server exploit, perimeter-penetration, denial of service, etc.) and less scripted "free-play". Memorandums of Agreement (MOA) will cover all aspects of inter-participant coordination, ranging from legal/administrative to VPN setup and the educational objectives of each scenario. Competitive scoring/grading, though an option, is not intended; thus obviating the need for 3rd party adjudication or equipment/software standardization.

Benefits to Participants

- A controlled venue to learn and implement best practice network attack (vulnerability assessment) and defense strategies, tactics and techniques
- Provides a test-bed for novel network and/or platform security research prototype "trial-by-fire" testing
- School's/Agency's CyberCombat network can be as small as one computer
- Additional service and/or security components can be added to each school's/agency's network as befits their individual educational or mission goals (see suggested functional areas below)
- Good infrastructure with which to illustrate/employ; Defense-in-Depth, Pirnciple-of-Least-Privilege, and Survivability concepts

Background and Miscellaneous

- NPS already has experience participating in three Inter-Service Academy Cyber Defense Exercises (CDX 2001, 2002, and 2003)
- NPS' CyberCombat Lab is already in place. Students will finalize configuration and hardening circa May 2004
- Interested schools/agencies need only designate a local network that connects to the Internet via a VPN gateway (IPSec, ESP, tunnel-mode), and agree to adhere to the MOA established with counterpart shools or agencies to participate
- More formal/coordinated management may follow as interest and activity in the program increases
- Point of Contact: J.D. Fulp, CISR Lecturer and Principal Investigator jdfulp@nps.navy.mil

Suggested CyberCombat Functional Areas

- Domain Controller, DHCP, DNS (i.e., Admin Services)
- Web, Mail, Database, VoIP, VTC, FTP (i.e., Public Services)
- Secure Wireless Access
- Strong Authentication
- PKI (Public Key Infrastructure)
- Vulnerability Assessment (intra- and extra-)
- Filtering/Firewalls ("Perimeter Defense")
- Data Backup
- Intrusion-Detection/Prevention
- Audit/Log Collection and Analysis
- VPN/Tunneling
- Computer Forensics
- DCS protection (Distributed Control Systems)