2003

CyberCombat

Fulp, J.D.

Monterey, California. Naval Postgraduate School

CyberCombat

J.D. Fulp – Principal Investigator jdfulp@nps.navy.mil

In 2001, 2002, and 2003, NPS participated in the first three Inter-Service Academy Cyber-Defense Exercises (CDX). These exercises involved having students at several participating DoD schools (Blue Teams) build secure service networks that would be subsequently attacked by various DoD Information Warfare agencies (Red Teams). Since the exercises were competitively graded; a White Team (referee) was also employed, courtesy of Carnegie Mellon University's SEI (Software Engineering Institute). The White Team's role was to ensure a level playing field (i.e., like equipment and software) and compliance with exercise ROE (Rules of Engagement). NPS enjoyed great success in these three exercises, twice finishing as the highest scoring team.

In 2004, NPS embarks on a more accessible and flexible cyber-exercise program dubbed CyberCombat. This program will be more accessible than the CDX-style exercise, as any school, university, or DoD agency wishing to participate, may do so with little concern to any conformance issues relating to their exercise network. This is unlike the CDX which necessitates a high level of uniformity to facilitate competitive comparison. Conduct of the CyberCombat program will not entail any comparative win/lose grading; unless the participating agencies specifically desire to incorporate that dimension into their exercise. The typical CyberCombat exercise will entail a non-competitive network "dialogue" between two or more participating schools' exercise networks. The nature of any specific exercise dialogue will be previously agreed upon by means of co-signed MOUs (Memorandums of Understanding) between the participating schools. The MOUs will specify such administrative and procedural items as; the expected learning objectives, VPN connection parameters, points of contact, and start-stop times/dates. Several typical attack/defend scenarios will be standardized into MOU form, thus providing a ready menu of exercise scenarios to draw from. Any new/novel scenario may be drafted into MOU form by the participating schools. The omission of competitive scorekeeping alleviates the high exercise overhead of having to draft, and verify compliance with, exercise rules-of-engagement. It also promotes the freer exchange of lessons-learned among participants, and opens the door of participation to smaller schools or agencies that lack the necessary curriculum or lab infrastructure to compete at the same level. Removing the competitive element, allowing virtually any VPN-capable network to participate, and the ad hoc nature of the MOUs, yields a very flexible environment for inter-school/agency cyber-play exercises.

Students participating in CyberCombat exercises benefit from the realistic, hands-on experience they provide. Such practical application is the perfect complement to the computer and network security theory that is delivered in the classroom or via textbooks. A well-prepared network participating in attack/defend dialogue with other networks will incorporate several hardened services, along with most or all of the protective security functional areas and concepts. Students may work on any number of these services or areas/concepts as time permits. These services and security areas/concepts include: DHCP, PDC, Web, Mail, FTP, MySQL, DNS, WiFi, Authentication, Hardening, VTC, Routing, Switching, Integrity-Checkers, Vulnerability Assessment, Filtering/Firewalls, Backup/Imaging, PKI, Intrusion-Detection/Prevention, Audit/Log Collection and Analysis, VPN, Honeynet, Forensics, Isolation, Defense-in-Depth, Perimeter Defense, File Encryption, Principle-of-Least Privilege, Policy Writing, and various other aspects of administrative and operational security. Any schools/agencies interested in participating can do so at whatever level their available network infrastructure and collective staff/student knowledge permit.