TeamDefend

A White Paper on
Strengthening the Weakest Link:
Organizational Cyber Defense Training

a CyberPatriot Initiative

Submitted to the 17th Annual FIRST Conference (2005)

TeamDefend

A White Paper on
Strengthening the Weakest Link:
Organizational Cyber Defense Training

The purpose of this White Paper is to describe an innovative and cost-effective way to train an organization's Cyber Security Team or Incident Response Team to effectively recognize and counteract today's cyber threats. The White Paper discusses the current cyber threat and describes a highly effective method for preparing the teams within companies/organizations of all size and importance in the protection of their Critical Infrastructure; be it organizational, national, or international in nature. TeamDefend addresses the weakest computer network link in that Infrastructure: The Network Defense Team. Using an on-site, real-time training system, TeamDefend prepares and evaluates an organization's ability to recognize and effectively deal with the cyber threat. Affordable, flexible and responsive to customer needs, TeamDefend will raise your IT staff's level of proficiency in a measurable way.

Background: More and more companies are finding that the use of the Internet greatly reduces their cost of long-haul communications with little degradation in performance. Whether used to share corporate information between satellite offices, conduct e-commerce transactions or provide remote control to supervisory control and data acquisition (SCADA) units connected to critical business operations, the broadening use of the Internet introduces increased exposure to corporate spies, cyber terrorists, and an growing number of "wannabee" hackers. To protect these networks and resources, strong Information Assurance (IA) measures must be put in place to ensure the uninterrupted, reliable operation of these critical business systems.

There are many forms of Cyber Incidents which we increasingly hear about such as Code Red, Nimda, Blaster, Sasser, etc. and much more cyber terrorism that goes unpublicized, all because the company's team of system administrators and security personnel are ill-prepared to recognize, mitigate and document cyber incidents. Compounding the situation is that knowledgeable hackers can use the aggregated power of unsuspecting, low value compromised systems to execute a coordinated attack against more critical system. As such, any IT infrastructure, regardless of its apparent unimportance to national or civil defense, becomes a weak link in the national critical infrastructure if left unprotected. This weak link is further magnified by the inter-organizational and international nature of the network links comprising the Internet which force Cyber Security and Incident Response Teams to search for more efficient, effective, cost sensitive means to collaborate against this distributed threat.

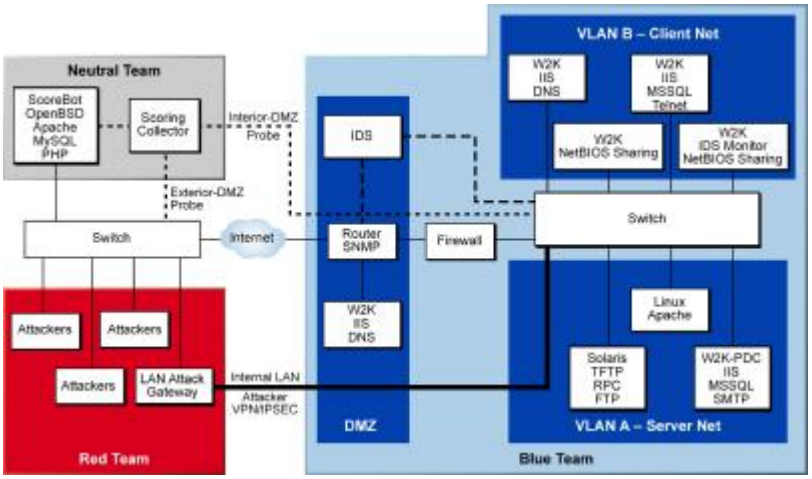
Discussion: There are many different means for defending against cyber threats, whether launched by the company insider or from a hacker in cyberspace. One of the most effective is to ensure that a company's IT staff is armed with the technical skills and practical experience to recognize the indicators of, and defend against today's cyber threat. To most effectively prepare an IT organization, staff members need to train as they would operate in their everyday environment. They need to not only train with training systems that present realistic attack scenarios against IT systems that mirror their own IT infrastructure, but they also need to learn to work as a team and to work inter-team, administering and coordinating the many functions of computer network defense.

There are two stumbling blocks to this type of live data, team training. First, many companies cannot afford to send their IT staff to remote school house training either for budgetary reasons, or they cannot afford the absence of their staff members that provide continual system support. Secondly, running this type of live training on production systems is not only very risky due to potential service outages caused by training scenarios, but they may also experience reductions in performance or system responsiveness to customers.

Solution: TeamDefend is a comprehensive mobile training system (pictured below) that is delivered to the customer site and can be set up in minutes in a location convenient to the customer. It provides an architecture representative of the customer's IT infrastructure, employs real-world, live data, and provides a real-time assessment of IT staff personnel during the training process. TeamDefend is self-contained, with pre-scripted cyber exercises that present the most common cyber threat scenarios, and automatically collects a wide variety of performance data. With TeamDefend, students are trained to recognize and take timely, corrective action to counter cyber attacks.

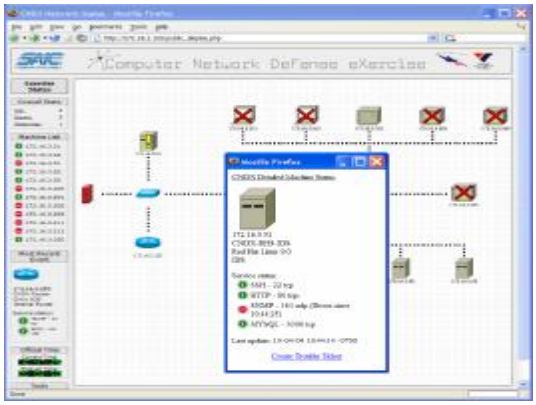
TeamDefend trains and evaluates the level of IT staff proficiency to perform intrusion detection, forensics and mitigation of cyber incidents. The training will also include the basics for handling the collection and maintenance of evidentiary data in the event the company wishes to prosecute the cyber assailant. The training is structured to provide a variety of scenarios to permit the organization to choose what is most appropriate to their operational environment. The training system is a self-contained, portable suite of systems basic to all organizations, such as servers, such as Windows, Linux, and UNIX servers, Windows workstations, network devices such as routers, switches and firewalls, and network-based intrusion detection systems. The system will also permit the addition of host-based intrusion detection systems and other components if desired. The systems, therefore, can be tailored to the needs of the customer (Cyber Security & Incident Response Teams).

Training Process: The TeamDefend training is typically conducted over a period of several days. The basic training package includes three days of training, exercising and debriefing. Depending on the customer requirements, and the level of proficiency, the training can be tailored to go as fast or as slow as desired. The result of the training will engender a repeatable cyber security practice that distributes the division of defensive tasks across an entire team.



The TeamDefend architecture (pictured right) is based on the Network Defenders Trainee Group (Blue Team), the Instructor Group (Red Team) and the Evaluation Group (Neutral Team). The Blue Team begins training by accepting responsibility for the Blue systems and assuming that there are vulnerabilities in those systems.

Phase I: The initial training will be conducted as an instructor-lead classroom experience. The training begins by reviewing with the Blue Team students the best practices for identifying and mitigating system vulnerabilities. This includes verification and installation of security patches, as well as the identification and eradication of back doors and trojans and use of computer forensics to verify systems security status. The next step provides the student with instruction in the configuration of network devices (firewalls and routers/switches) according to their security policy, and finally in the configuration of intrusion detection systems for use as threat detection system.



Phase II: After the previous day's review of the "best practices", the instructor will provide the parameters and rules for the following day's exercise, explain the functions of the automated scoring system and trouble ticket interface (pictured right) and then will commence launching a series of live data, cyber exploits that are typical of the real-world environment. Representative exploits are launched in a logical sequence that provides the System Administrators (sysadmin) with experience in seeing the individual and cumulative affect of these incidents.

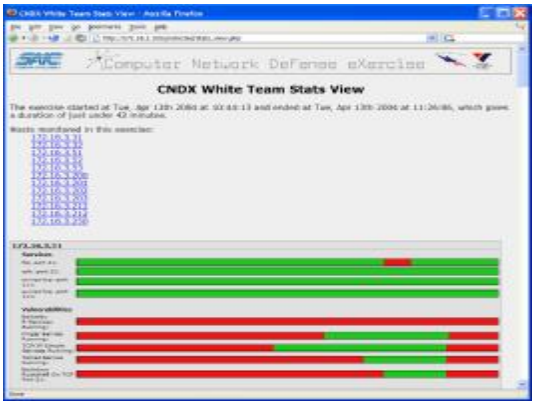
Each of the exploits is explained in the following terms:

- What the exploit is;
- What impact it is expected to have;
- How does the IT staff detect/recognize it;
- What corrective steps should the IT staff take to stabilize and the mitigate it;
- How to determine the extent of damage that may have occurred; and,
- How data should be handled to meet evidentiary requirements.

The instructor will walk the students through each exploit, demonstrating the affects to the systems, where and how to recognize the exploit's existence, and how to contain and remediate it's affects. The trainer will also provide instructions on how to capture the data that is required for most prosecutorial portfolios.

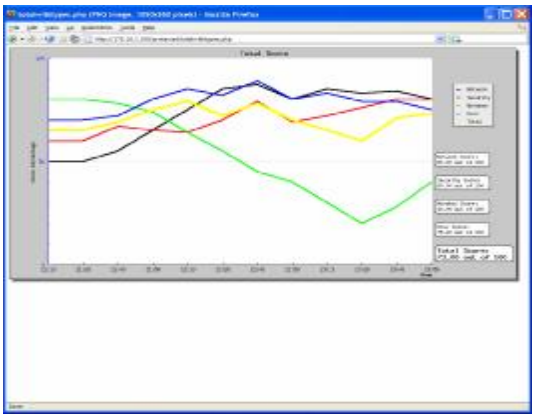
Once this demonstration is completed, the students are then permitted access to the training system computers and asked to check the blue systems for common exploitable vulnerabilities and to configure their network and security devices in accordance with their security policy. The Neutral Team will evaluate the Blue Team, providing feedback as to the degree of success in performing this function.

Phase III: During the evaluation phase, the Blue Team will begin to apply what they learned in Phases I and II to lock down their networks and systems. After a short period of time, the Red Team will begin executing scenarios and launching a sequence of exploits to validate that the student has truly learned how to evaluate the data and recognize a cyber attack.



The Blue Team will be evaluated by the Neutral Team using the automated scoring system (pictured left) that measures: system configuration data, system vulnerability data, student response to incidents, and vulnerability exploit results. It also collects data on how well the Blue Team kept systems and services online. The scoring system provides a real-time visual aid, as well as a database, that aids both the Neutral and Blue Teams in understanding the effectiveness of Blue's actions, allowing timely corrective action by the Instructors.

Lastly the instructors provide a final briefing for the students to run through the exercise with complete transparency, thus showing the blue team each attack and action in the system, as well as displaying the corresponding reaction in the score values. (Pictured right) With this overview of the exercise, the instructors can provide to the blue team students, the appendix to the user manual, which contains the "answer key" to each exploit in the system, where it should have been detected, how it needed to be mitigated and how the red team could leverage that exploit to gain control. Thus the students are left with the answers to those problems that they missed, so they can learn from their experience.



Once the on-site training is completed, the company has the option of additional on-line follow-up training via an Internet-based subscription service. By remotely connecting to the SAIC TeamDefend web-site, training can be conducted to reinforce previous training, or to receive up-date training on newly released cyber exploits. The company will have the same control over the training infrastructure, and will benefit from the web-based scoring system for real-time feedback. SAIC trainers will also be available via chat or phone for additional questions.

Benefits: Therefore, the benefits provided by TeamDefend are:

- Real-world, live training on systems that replicate the customer's own;
- Initial Training conducted on-site, thereby minimizing expense and loss of IT staff from the premises;
- Follow-on Training conducted remotely for reinforcement or updates to current exploits;
- Sharpening of individual cyber skills, while fostering a TEAM-work approach to problem solving;
- Updated scenarios to keep current with the changing threat;
- Sharpening of individual cyber skills, while fostering a TEAM-work approach to problem solving;
- Training curriculum that addresses all of the basic day-to-day practices required to administer network and system security; and,
- Real-time performance feed back to reinforce successful behavior.

Conclusion: TeamDefend addresses the weakest computer network link in the critical infrastructure: The Network Defense Team. Using the on-site, real-time training system, we are proposing using TeamDefend during the 17th Annual FIRST Conference (2005) as a compelling addition to the tutorial track. During two half-day tutorial sessions supporting approximately 40 people per session hands-on (room capacity determines the total number of observers) , we will provide a venue which will prepare and evaluate a FIRST member team's ability to recognize and effectively deal with the cyber threat. Further, we will be adapting the tutorials to highlight inter-team coordination. The focus will be to allow FIRST member teams to literally "train as they fight" going beyond traditional information collaboration & dissemination during an incident to exhibiting through the hands-on environment of TeamDefend how teams can work together at a technical level to resolve threats in real-time and receive feedback based on the Neutral Team and the automated scoring mechanisms.

For further information: Please contact:

Scott C. Kennedy, Program Manager-TeamDefend,
Science Applications International Corporation,
4224 Campus Point Court, MS B-1-E, San Diego, California 92121
Phone: 858.826.3035.
Email: kennedysc@SAIC.com

Hart Rossman, Chief Technology Officer
Science Applications International Corporation
12100 Sunset Hills Rd., Reston, Virginia 20190
Phone: 703-375-2261
Email: rossmanh@saic.com