Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

Strengthening the Weakest Link: Organizational Cyber-Defense Team Training

Duke Ayers, AVP, SAIC TeamDefend Program Manager, Chief Systems Engineer, MBA, CISSP, HISP

Abstract – Information is a critical business asset, which depends on protection by competent system administrators experienced in real-world environments and threats. With the cyber threat increasing, we need a meaningful way to train, and certify, the level of cyber competency. A cyber-defense curriculum and live-fire trainers that quantify a student's performance are essential to the survival of our "Information Age" critical assets.

I. Introduction

All businesses rely on worldwide data network communications to meet their business goals. We use these networks to transfer sensitive information to conduct business between satellite offices and trading partners, to perform e-commerce transactions with customers or to provide remote control to supervisory control and data acquisition (SCADA) units connected to critical business operations, etc. The broadening use of the Internet, however, introduces increased exposure to corporate spies, cyber terrorists, and a wide spectrum of hackers looking to gain access to corporate sensitive information or to deny service. To protect these networks and information resources, strong information assurance measures must be put in place to help ensure the uninterrupted, reliable operation of these critical business systems. Technology speeds and complexity continue to grow to meet the ever-increasing, sophisticated threats; it is the man-in-the-loop who is not keeping pace with the problem. To adequately meet this challenge of cyber threat, we need better trained and tested system administrators (SysAdmins) who effectively use technology and procedures to recognize threats and defend our information systems.

II. Fight as you have trained!

There are many different means to prepare a defense against cyber threats, whether launched by the unsuspected insider or from a determined adversary in cyberspace. One of the most effective methods is to ensure that the information technology 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, people need to train as they would operate in their everyday environment, or "train as you will fight...and you will fight as you have trained." (Russell D. Sanders) They need to rehearse on training systems that present realistic, live attack scenarios against hosts and network devices that mirror their own IT infrastructure. They also need to learn to work as a team, administering and coordinating the many functions of computer network defense, ensuring timely, substantive communications. You may have SysAdmins who observe network activity that they have not seen before and which, therefore, concerns them, but they are not sure how to deal with it. If they think like a team and provide as much information as possible regarding the potential incident and pass that on to a team mate or second tier of response, then they have effectively sounded the alert for a more senior, experienced SysAdmin to mitigate the situation.

III. Cyber defense training requirements

How, then, can you train students to recognize and take timely, corrective action to correct misconfigured systems and counter cyber attacks. You need a training platform that trains and evaluates the level of IT staff proficiency in maintaining critical services, hardening systems, performing intrusion detection, and mitigating cyber incidents. The training should include the basics for handling the collection and maintenance of forensics evidentiary data in the event the company wishes to prosecute the cyber assailant. The training should be structured to provide a variety of scenarios to permit the organization to choose what is most appropriate to their operational environment, policies and regulatory requirements. The training system should be self-contained, so that it does not interconnect with any company operational networks; this is necessary so that the students are free to experiment and not worry about causing any network or system outages. This training environment should encompass a suite of systems basic to all organizations, containing Web, email, database, and file servers running Windows® (Micosoft Corporation), Linux® (Linus Torvalds), and UNIX® (X/Open Company). The system also contains Microsoft's Windows® workstations, network devices such as routers, switches and firewalls, and network-based intrusion detection systems. The system should also permit the addition of host-based intrusion detection systems and

ISBN 1-933510-96-9 ©2009 CISSE

other components, if desired. The overall system should be capable of being tailored to the needs of the customer.

IV. CONDUCT OF TRAINING

Training should be conducted over a period of several days to accommodate training sessions, exercises and post-exercise debriefings. Depending on the customer requirements and the level of proficiency expected, the training should be capable of being tailored to go as quickly or as slowly as desired. The training can reinforce individual skills as well as instill repeatable cyber security practices that are distributed across the entire cyber-defense team.

Phase I. The initial training should be conducted as instructor-lead classroom training to bring all participants to a common level. The training starts by reviewing "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, plus the use of computer forensic tools to verify systems security status. The next step instructs students in the configuration of network devices (firewalls and routers/switches) according to their security policy. Finally, the configuration and use of intrusion detection systems should be discussed.

Phase II. After Phase I review of the "best practices," the instructor should provide the parameters and explain the functions of the team trainer, especially the automated scoring system and trouble ticket interface. Instructors should then demonstrate live exercise play, including cyber exploits that are typical of the real-world environment. Representative exploits should be launched in a logical sequence that provides the SysAdmins with the opportunity of seeing the individual and cumulative effect of these attacks. Each of the exploits is explained in the following terms:

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

Once this demonstration is completed, the students are then permitted access to the training system computers to investigate their hosts for common exploitable vulnerabilities and to configure their network and security devices in accordance with their security policy.

Phase III. During the evaluation phase, the students will begin to apply what they learned in Phases I and II by locking down their networks and systems. After some period of time, the instructors will begin executing scenarios and launching a sequence of exploits against pre-configured vulnerabilities to validate that each student has truly learned how to recognize and mitigate against cyber incidents.

V. QUANTIFYING SYSADMIN PERFORMANCE

Throughout the exercise, the automated scoring system should track the security health of the network by measuring system configuration data, system vulnerability data, loss of critical services and the student response to incidents, and vulnerability exploit results. It should also collect data on how well the students maintained critical systems and kept services operational. The scoring system should maintain a database of system status while providing a standard network management view for students and a special view for instructors to keep the game-play on track and enable them to focus training based on real-time results.

VI. THE "LIGHTS GO ON"

By the time that the exercise is over, the students should feel as though they have experienced the worst day of their cyber lives. It is at this point, that the instructor will provide a debrief, walking the students through the entire exercise with complete transparency, showing the students each attack and each corresponding action taken and communication sent. This is then correlated to the minute-by-minute score they received.

VII. CONTINUING EDUCATION

After walking the students through the exercise results, the instructors might also provide a student manual that is the "answer key" to each exploit in the system, where they should have been detected, how they needed to be mitigated, and how the hacker can leverage the exploits to gain control. This student guide permits the continued training experience in later weeks after the team trainer.

Additionally, the trainer should be capable of providing training to remote users. This flexibility permits refresher training to be conducted to reinforce previous training. In fact, the trainer should be capable of conducting the exact same exercise, including timing and sequencing of exploits. This capability is key to evaluating if the students have learned and grown from the first experience. Remote exercising can also be used to train

students on newly released cyber exploits as well as changes in their IT environment or policies.

VIII. TEAMDEFEND

Several years ago, SAIC recognized that there was no effective means to maintain the skills and tool kits of their penetration testing personnel (white hat hackers) in a repeatable, real-world way. Based on our multiple years of participation in the "Capture the Flag" tournaments at the DefCon Computer Security Conventions in Las Vegas, we decided to build an internal capability to train and exercise our cyber warriors. The cyber-defense trainer (SAIC's TeamDefend) has evolved over the years and has been used in multiple exercises, working with academia, Federal, State and Department of Defense (DoD) organizations.

TeamDefend is a self-contained training system, which provides a "sandbox" training environment for system administrators. Although the chassis is compact in size, it contains a full suite of state-of-the-art hardware that can be tailored to reflect the organization's production environment. The flyaway trainer includes UNIX and Windows servers and workstations, network devices such as routers and switches, and security mechanisms such as firewalls and intrusion detection systems. It not only emulates the operational environment, but also presents realistic, live cyber attacks, and provides a real-time assessment of IT staff personnel during the training process.

TeamDefend is semi-automated, with updated cyber exploits that represent the most common and newly emerging cyber threats, and automatically collects a wide variety of performance data. These exploits are continuously updated as new threats emerge; the new scripts can be transmitted to organizations within minutes of creation and validation if necessary for continual refresher training.

TeamDefend is patent-pending and mapped under the Committee for National Security Systems Instruction National Information Assurance Training Standard For System Administrators (SA) (NSTISSI-4013) sponsored by the National Security Agency (NSA).

IX. OUTREACH

SAIC is a large supporter of various science, technology, engineering and mathematics (STEM) initiatives throughout the United States because of its commitment to mentoring and inspiring new scientists in our communities. One of those projects, called the "Cyber Defense Challenge," was conducted in conjunction with the San Diego Chapter of the National Defense Industrial Association (NDIA). NDIA sponsored this competition in order to evaluate its efficacy for potential national competitions and meeting the STEM goals, which included:

- Innovate in the classroom and beyond the bell;
- Expand math and science educational opportunities;
- Reach all regions with equal training opportunities;
- Address the achievement gap; and
- Make math and science fun!

The University of San Diego (UCSD) and SAIC teamed to bring local area high school students to the SAIC campus to experience this video game-like cyber-defense training, with the goal of encouraging students to pursue university degrees in the technical fields. Over the course of several Saturdays, six to eight student teams from five San Diego area high schools met to receive three hours of security training to baseline their knowledge and then three hours of live exercise time to see how well they could harden systems and fend off computer attacks. Exercises were conducted under the following conditions:

- Ethics of competition were stressed
- One school at a time; 6-8 students
- Targets were configured with Windows operating systems
- Scenarios were exactly the same for each school
- Scripts with times for launching attacks were used
- Target operating systems and services were announced prior to competition
- Competition sequence was established by draw
- NDIA provided the trophy for the winner
- Quantitative Points Criteria:
  - Maintain critical services, and
  - Remove vulnerabilities.
- Qualitative Points Criteria: Submit timely and substantive trouble tickets.

Figure 1. Students during NDIA Competition

The schools competed against each other and with the use of the exact same scenario and sequence of exploits; we were able to assess an "apples-to-apples" competition winner. At the end of each day, we conducted the exercise debrief, as well as presented a career message from our senior security professionals on the rewards and challenges of pursuing a technical degree.

Out of this exercise, we gained quite a few insights on working at the high school level and received important student and teacher feedback.

"The kids were still pumped up on Monday after the competition. In fact, they used their 'new found' knowledge and crashed the server they had set up to practice on!" (Greg Volger, educator)

Greg Volger continues, "One of the most interesting lessons learned is that our university systems are not encouraging formal computer science training in this information age. I feel this competition is a step in the right direction for high school students. I only wish that colleges would support computer science in the high school in a meaningful way. Currently, there are no computer science entrance requirements for a college applicant. Colleges complain that computer science majors are decreasing. High-tech companies are complaining that they cannot recruit enough applications and must go abroad to do so. This trend will continue until students at the high school level are introduced to computer science. Currently, many students wish to take my AP computer courses, but they have no room in their schedules because they are fulfilling college entrance requirements. I had to convince many students to take AP Computer Science and once in it, they loved it and continued their computer science education through college and their careers." (Greg Volger, educator)

X. CYBER PATRIOT I

With a local high school event under our belts, we were invited to participate with the Air Force Association (AFA) and the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio (UTSA) in the first National High School Cyber Defense Competition. This inaugural event was conducted as a proof-of-concept to demonstrate that it was a viable and valuable learning experience for high school students. The lessons learned from this event are being applied to future competitions with the ultimate goal being to expand the competition so that any high school in the nation can participate.

The AFA Mission Statement [1]
"The High School Cyber Defense Competition (HSCDC) provides high school students with an opportunity to learn about and exercise information assurance and computer security methods and procedures. It provides a controlled, competitive environment to assess students' depth of understanding and operational competency in managing the challenges inherent in protecting a network infrastructure."

Figure 2. Students during AFA Competition

Event objectives were similar to the San Diego NDIA STEM competition:

- Encourage students to learn about information assurance and computer security;
- Provide an educational venue in which students are able to apply the theory and practical skills they have learned;
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams;
- Create interest and awareness among participating schools and students; and
- Encourage students to consider information assurance and computer security as a possible career path and/or as a possible course of study to pursue in higher education.

Here was one sequence of trouble ticket conversations between the students and the instructor (control cell) to give an example of the level of exercise play.

Student - 1:02:25: We restarted the SNMP on all parts of the network. How do we keep the hacker from getting back in and changing the service

Control Cell - 1:03:51:You need to figure out how to block the vulnerability that the attacker came in through. You'll need to determine how to correct the vulnerability in the software.

Student - 1:08:54: what sort of vulnerabilities can

the hacker get in through? do we need to add software, or just adjust the configuration

Control Cell - 1:10:16:Could be both. Patches are usually a good start.

XI. EXPANDING THE REACH

Cyber Patriot I proved to be an invaluable competition to excite and challenge students to careers in technical fields. As a result, AFA and UTSA immediately set their sights on Cyber Patriot II, with the goals of

- Expanding the numbers of participants from around the country, and
- Raising the bar on the degree of difficulty to qualify for the finals in Orland, Fla., in February 2010.

During Cyber Patriot II, there will be a series of qualification events and even a consolation round to keep schools involved in the competitions for as long as possible.

XII. CONCLUSION

Information is a critical business asset, which depends on protection by competent SysAdmins experienced in real-world environments and threats. With the cyber threat increasing, we need a meaningful way to train and certify the level of cyber competency. A cyber-defense curriculum and live-fire trainers that quantify the performance of students are essential to the survival of our "Information Age" critical assets.

The goal of our cyber-defense training environment must include:

- Real-world, live training on systems that emulate the production environment;
- Initial training conducted using a structured, on-site methodology; a "train the trainer" model can provide continuity for routine exercising thereafter;
- Continual training capability for routine training and timely exposure to new threat scenarios as they are released;
- Follow-on remote training as an option to continue the training experience;
- Up-to-date scenarios to keep current with the changing threat;
- Sharpening of individual cyber skills, while fostering a teamwork approach to problem solving;
- A training curriculum that addresses all of the basic day-to-day practices required to administer network and system security; and
- Real-time, comprehensive performance feedback to reinforce successful behavior.

XIII. REFERENCES

[1] Air Force Association (AFA) and University of Texas San Antonio (UTSA) National High School Cyber Defense Competition Team Packet.