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

Engaging Students through an Information Assurance Exercise

William Conkling, Lieutenant Colonel George Trawick,
and J.A. "Drew" Hamilton, Jr., *Senior Member, IEEE, Auburn University*

Abstract- In this paper, the Information Assurance Exercise that has recently been developed at Auburn University will be discussed. This educational exercise provides Auburn University with a means to foster student interest as a potential area of study in information assurance as well as Computer Science. This sort of high speed, low drag exercise is designed to be a student's first exposure to real information assurance practices and demonstrates the stark differences between setting up a virus scanner on a home computer and the level of effort required in securing an enterprise level system. Optional courses in information assurance and computer forensics continue to grow at most universities. This exercise is designed to offer students a chance to explore their interest in the discipline in a hands-on, goal driven manner. The components of the exercise are specifically selected and designed so that they can be taught at a variety of technical levels based upon student knowledge and experience.

Categories and Subject Descriptors
Experimentation, security, forensics

General Terms
Information Assurance Exercise, Exercise, Laboratory, Security, forensics

Keywords
Information Assurance Education, Information Assurance, forensics

I. INTRODUCTION

Many students have an interest in Information Assurance as can easily be seen in the recent National Security Agency (NSA) and Department of Homeland Security (DHS) press releases designating many schools as new National Centers of Academic Excellence in Information Assurance Education [1] as well as National Centers for Academic Excellence in Information Assurance Research. [2] Auburn University falls into both of these categories and is expanding the number of courses offered to include Computer Forensics and a course in Information Assurance Risk Analysis. Auburn is also expanding the number of government level certifications available to students throughout their coursework. However, many of these courses are targeted toward the upper-level undergraduate students or graduate level students. It is recognized that information security education needs to be expanded [3] [4]. This effort to create a day long educational and entertaining exercise presents information security to students who might otherwise never have an opportunity.

The Homeland Security Presidential Directive 23 discusses the need for partnering with academia for improved education of cyber professionals. This nationally recognized need for information assurance professionals [5] creates a great opportunity for improving student enrollment and student interest is clearly growing; however there has been a decline in enrollment in Computer Science in general despite this need. This is leading to the development and introduction of many new and arguably more interesting courses in Computer Science all in an attempt to attract more students into the computing sciences. [6] In that effort, the Auburn University Information Assurance Center recently developed and executed their first Information Assurance Exercise (IAE). The exercise had several goals. Foremost, the exercise was to identify students with an early interest in information assurance (IA), give them some hands-on experience and a basic education in information assurance, as well as to foster their interest in research and IA education. Secondly, develop an instruction set that could be easily tailored to different levels of student experience and knowledge. That would provide an interesting and entertaining presentation of current information assurance topics. Finally, build the

exercise in such a way as to make it portable to locations outside the Auburn campus, providing the experience to those who cannot come to us.

II. RELATED WORKS

There are multiple cyber warfare exercises that are put on every year [7] [8] [9]. These exercises attempt to give students a glimpse into what real life cyber security is all about. The students often come in as the hackers (red team) or defenders (blue team) and are then allowed to hack away at each other; in some exercises all students are either blue or red. Either way students generally prepare for months before hand to gather the required knowledge and practice on the systems they will be using. Students are given a variety of software based tools, workstations, and sometimes physical access to networks in order to complete the task at hand. There is no doubt that these exercises have the "wow factor" that many people are looking for when it comes to recruitment and publicity. However, the personnel actually doing the exercise are almost always already committed to the field of Computer Science and likely information assurance.

While the participants in these exercise certainly all enhance their knowledge and skills in computer security, the winners may even have a trophy and bragging rights, but often the exercise is simply a practical application of months or years of education leading up to the big day. While not distracting from the importance of these exercises or deny their fun factor, these exercises really don't do much for the potential computer science students. The Auburn University Information Assurance Center's Information Assurance Exercise (IAE) addresses a different and very important need: the need to attract students that have little or no prior background in Computer Science without requiring them to go through months or years of training. This is where the Information Assurance Exercise contributes to the overall goal. While in the eyes of computer science and information assurance professionals, it may initially lack some of the "wow factor" of other cyber warfare exercises, for students that have never investigated information assurance, even sending a spoof e-mail, hacking an e-mail account or finding major vulnerabilities on their own university's web server can have a very large impact.

III. SETUP

A. GOALS

Initially, Auburns Information Assurance exercise was to model other cyber warfare exercises, where the students run a scripted red team and blue team type of hacking and defending exercise. However, it was quickly realized that this would present a steep learning curve for inexperienced students and that the increased complexity of a red/blue team style exercise would dampen the portability of the instruction. Information Assurance covers a broad range of topics, each of which could be a course by itself. Great care was taken to develop a set of instructions such that it would touch on each area just enough to give the students exposure to the many facets of Information Assurance.

The exercise is designed such that the participants could learn from and participate in the IAE without being required to prepare beforehand. The goals here were twofold. First, the program would be more accessible to a broader range of students if they were not required to have deep technical knowledge and prepare for months and secondly to give the students some instant takeaways. Also, most information security exercises focus heavily on active hacking of an infrastructure, but a much larger number of exploits occur due to other reasons. This is another area where this exercise differs. The IAE covers the less technical and often overlooked aspects of social engineering, physical access and networking vulnerabilities and present it in a way that non-computer science students can easily relate.

It was decided that there should be a few specific areas of security that were explored, and the exercise should follow a story line not only to help tie the different facets together for the students but to express how this is important to their everyday lives. The final objects for the exercise are:

1 Access Control
2 Network Exploits
3 Local Exploits
4 Disaster Recovery

Another goal was to keep the activities hands-on to engage the students without requiring much previous knowledge. This required that the learning occur predominantly through hands on activities. With the social implications of the programs being created, Computer Scientists are not the only people that need to understand security. "Increasingly, there are many

other fields where computing is a critical component of a field that includes another subject area." [10] While the initial IAE was designed for potential Computer Scientists the exercise has built in flexibility that allows students and professionals from disciplines outside of computer science to be introduced to information assurance and the importance of information security.

B. PHYSICAL SETUP

One of the most important factors of this exercise was to get the students engaged in hands on activities right from the start. This was facilitated by giving each student unrestricted access to their own terminal. Often times many students share a machine for programming assignments and are limited to what they are allowed to do on the machines Fortunately, not only is the exercise designed to be performed in parallel, students could also have unfettered access to the entire system without any concern. The systems that were purposely built for this exercise were dual-boot machines with Ubuntu Linux and Windows XP Professional Service Pack 2. Originally two separate machines each with a different operating system was considered the most appropriate course of action. However it was decided that it was important to demonstrate the idea that owning one operating system on a machine means that you own all of the files on the disk. With all of the virtual machines and multi-boot systems that exist, many people do not understand that access to one system most often means access to all of the systems. Further, dual booting allows the exercise to offer double the number of physical systems available for students to use.

It was important for the exercise that the students had complete access to the entire system, including the ability to shut them down and open up the case. This will be explained more in depth later, but it is important to the overall theme of the instruction. Because of the level of access given to students with little or no experience the machines used in this exercise were university surplus machines, long past their usefulness in other labs. This allowed the students to really experiment without worrying about repercussions of possibly breaking the systems. This was a new frontier for many of the students in the pilot session. Each machine had a single DVD drive and only one network card. None of the machines had wireless access. All of the systems were on desks so that the students could see each other working and could openly communicate. The idea was to share information and encourage the students to work together.

In addition to the main systems there were several research systems with access to internet search engines available to the students. The importance to this comes into play later, but these machines were unprotected and were intended to be shared by the students. The idea was for the students to be able to collaborate when they needed to figure something out, but to be able to actually implement the ideas individually. Also, each student was given a USB stick for later use.

A. *SYSTEMS CONFIGURATION*

All of the machines were configured with two Windows user accounts and one Linux user account. On the Windows machines, several unique usernames and hard passwords were established. For the Linux login, all the machines used the same username and easy passwords. This setup is intentional and helps facilitate some of the key learning points described later. Furthermore, all of the systems were configured with BIOS passwords and the DVD drives were disabled for booting. All used software was pre-installed.

For Windows this was:

1 NESSUS

2 Nmap and ZenMap GUI

3 WireShark

4 CyberProtect Game

For Linux the following were installed:

1 Nmap

2 NetCat

3 Fping

The students were each given 2GB USB sticks that were preloaded with the supporting files and open source programs to assist with backing up files, wiping drives and recovering files from drives.

IV. INFORMATION ASSURANCE EXERCISE

A. *STORYLINE*

To help present the learning points to students who are not computer scientists, a story line was created. This story line is used to tie the technical aspects of computer security and information assurance to a logical flow of procedures. The storyline will bring together the concepts of information assurance with the everyday experiences of the students. Helping to

ease any apprehension the students may have about computer science.

The storyline starts with showing how physical security is the first line of defense for a computer system, the story and the learning point's progress from there, through cracking user accounts, to gaining network intelligence and finally, how the persistence of data can tell the story of a hacker's action. The flow of the learning points and a coinciding storyline is a high priority of the planning of this exercise. Eight major topic areas were selected for use in this exercise:

1 Physical Access
2 Footprinting
3 Network Mapping
4 Traffic Monitoring
5 E-Mail Account Hacking
6 E-Mail Spoofing
7 System Backup and Restore
8 User Education

These activities were completed in order. The idea is to show that once a potential attacker has chosen a target, they often try to exploit the people before any sort of technical attack. Why try to exploit a difficult buffer overflow when you can simply ask someone for their username and password through a spoofed e-mail from technical support?

B. *PHYSICAL ACCESS*

The story begins by arming the students with a couple of tools and a tiny bit of knowledge. First the students were oriented to the lab and given the scenario that they were to be the bad guys and their mission was to simply log into the Windows machine, by any means available. The students were given a bootable password cracking CD and access to the internet.

As stated previously, the exercise started with all of the machines having passwords set for the BIOS and the Windows and Ubuntu operating systems. Further, the CD ROM was removed from the boot sequence. When the students came into the room they were oriented to the lab and given a short set of instructions. After showing the students where the research machines were and giving them an Orphcrack bootable CD. The students were quickly given their first hands on task. The Orphcrack was the Windows XP version. The lead instructor explained the CD would boot up and crack the passwords and it was a "no holds barred" task for them to get logged in to Windows. It was made clear that these were shop machines and the students should not have to worry that they would not be responsible for any damage to the machines; they should feel free to do whatever they felt like.

At 8 o'clock in the morning this was clearly a daunting task but the students went to work trying to boot from the CD. They soon realized that they could not boot from the CD or get past the BIOS passwords. Additional instruction was often necessary to explain some more vague or difficult points, such as to tell the students what a BIOS does and how it could be used to allow the machine to be booted from the CD. The students were excited and eager to learn these techniques that are well known to computer science majors. The students soon started using Google to search for hints. In order to keep the scenario moving and minimize student frustration, every ten minutes the group was given guidance so they could keep progressing. Eventually the students realized they needed to open the machine up. They first tried removing the CMOS battery but fortunately the DELL machines had a hardware backup of the BIOS password. After about thirty minutes one of the students found a page explaining how to bypass the password but the students could not figure out what to do.

To keep on schedule, the students were guided through the bios and boot portion, the point had been made that physical access is greater than any software protections. The students were shown the electronic copy of the user manual on DELL's website and that showed them how to reset the BIOS password with a jumper. The students reset the BIOS, enabled the disc drives and booted into Orphcrack. While they were waiting for their passwords they had gone from groggy to excitedly chatting with us about physical access. Now was an opportunity to guide a quick discussion on the importance of physical security.

The key learning points for the students during this part of exercise were the importance of physical security and the necessity of complex passwords. The students were exposed to a password cracking technique helping to tie their learning to topics common in the news.

C. *FOOTPRINTING*

Once the students had successfully bypassed the bios password, cracked the Windows administrator password and had logged into the Window machine, they were given the Ubuntu passwords and were told to boot into Linux. The foot printing section started by orienting the students to the command prompt and explaining basic commands. From there the students started with basic foot printing.

The storyline continued by discussing what a hacker might do once they had access not only to your computer, but now they have access to your network. It was explained how a hacker, like other criminals, will want to gather some intelligence on their target so they can choose their tactics and tools to maximize the effects of their attack. First, the students were introduced to command line and web-based whois lookups. Using Microsoft as an example to show students how hackers use whois to list chat channels and forums sharing the goal of hacking into Microsoft.

After that the students played with nslookup. They were shown the different types and what all of the returned information meant. A little extra time was spent explaining mail exchange servers to setup the later exercises. The importance of this information and how it could be exploited was explained in addition to what countermeasures existed. The students were further instructed on how the information that is easily and publicly available could be effectively used by criminals. The recent proliferation of VOIP services and possible vulnerabilities were presented as an example.

The key learning points for the student in this session was to show the importance in carefully configuring network systems, and how inexperience and inattention to how systems are configured and the information is presented to the public can easily be exploited by criminals.

D. *NETWORK MAPPING*

The exercise continues with the students using their new found access to local machines to explore the local area network looking for vulnerabilities.

The students were introduced to trace route in Linux. The discussion included the basic differences between ICMP and UDP traffic and what type of intelligence that is available simply by tracing a route. The information that is available in the last few hops was explained and the intelligence that information gives to a person who knows what they are doing. It is important to understand that locking down the machine you know will be a target is not good enough; you also have to harden the other machines on the network. Next the students were shown fping and the additional capabilities it has over the simple ping command. They were allowed to use it on the network to demonstrate how it can be used to look for active hosts on a subnet. With this new information the students were instructed to begin drawing the network on the whiteboard in the front of the room and that is when the students clearly started to understand what they were doing.

To finish up the manual command line portion, The students were told to check for open ports with NetCat. Both UDP and TCP scanning was demonstrated and the students ran various scans using both methods. The students then added the open ports to the network map on the board. This opened a great discussion on how to counter this sort of information and how the criminals would use the intelligence to hack the network.

After showing the students the manual way, they were introduced to Nmap and let them see just how easily the information can be obtained. The speed provided by Nmap allowed them to map their home institutions as well as the places onsite and to verify the network map they had created earlier on the board.

The students learned some very valuable lessons from this session. The students experienced firsthand the ease of intelligence gathering and how the intelligence could be used to gain access to a remote system.

E. *TRAFFIC MONITORING*

Next is how to gather intelligence on the network. Building on the information acquired and the network map built in the previous section. The students were now going to use a GUI based automated tools such as Wire Shark. The students ran WireShark and observe what it did when they were running automated tools. The students used ZenMap (Nmap's Windows GUI) as well as Nessus. These tools allowed the students to see the ease at which the automated tools accomplished the network mapping and the usefulness of the intelligence available was carefully explained. Nessus even allowed the

students to identify exploits that they had been introduced earlier in the session. This opened the door for a great discussion about version control and default passwords. To drive home this learning point the students were shown multiple online repositories of default passwords and discussed how the default password should always be changed before hooking a system up to a network.

This block of instruction really showed the students the speed and ease at which even the most novice hacker could obtain a great deal of information about the network and how they could use it to exploit unpatched vulnerabilities in the network.

E. *E-MAIL ACCOUNT HACKING*

With some of the basics of network intrusion complete, it was time to tie in the learning with current events and add relevance to the exercise. This block of instruction was nicknamed the "Palin Exploit". At the time of this exercise, the recent hacking of Governor Sarah Palin's Email account was front page news. Although the vulnerability has existed for ages only after Governor Sarah Palin's e-mail was hacked this way did it get much attention. The point here was to impress upon the students the truly unsophisticated and non technical nature of this attack. In preparation for this portion, a fake AOL account for a well known public figure was created and their password secured with password hints from their personal lives found from the Internet. The instructor demonstrated for the students how to try to reset a lost password and then found the publicly available information that answered the questions needed to reset the passwords. The students then logged into the e-mail account with the new password. Of course after this exercise everyone wanted to check and see if their own personal accounts were safe.

The students learned a couple of lessons from this session. First, is that you do not always have to have sophisticated or technical tools to gain illegal access. Second, that the user friendly features of some operating systems or applications introduce vulnerabilities that are easily exploited. Finally, it is sometimes the users themselves that present the greatest security risks; risks that cannot be mitigated by a high priced firewall, fancy anti-virus or even the most vigilant systems administrator.

F. *E-MAIL SPOOFING*

The concept of the users being the weakest link in the security chain fed nicely into the next session. The students were introduced to the concepts of social engineering. After a short discussion and some real life social engineering stories, it was time to let the students get some hands on experience with creating a fake email to possibly gain some inside information for an unsuspecting recipient.

The students went back to Ubuntu and used nslookup to find some open mail exchange servers. The students then used telnet to gain access into the servers. They were given the commands to send very simple spoof emails. All the students then sent a spoof e-mail to the dummy account that was created for the Palin Exploit. These emails were later examined closely. A discussion followed about how most people read and respond to emails out of habit and how a criminal could use this behavior against them to gain some intelligence. Next the emails headers from the spoofed emails were explored. This showed the students how easy it is to trace the email back to its true source. Due to the topology of the lab there is only one IP address but it was still traceable back to the lab.

The lessons here gave the students a practical demonstration of just how easy a criminal could take on the disguise of someone else through email and then request information that could allow them illegal access. This also reinforced the fact that not all of the security tools are technical; sometimes its user training that will give you the greatest security.

G. *SYSTEM BACKUP AND RESTORE*

In the final block of instruction, the students shifted roles a bit and began to look at things from a system administrator's perspective. As the day was winding down, discussion on how criminals who either use computers to commit crimes or attack the information within a computer as the target of their crime, will always leave a trace of their activities. This portion of the exercise shows the student that if you know where or how to look you can find these traces. To demonstrate the persistence of data and the forensic traces left behind the USB memory sticks the students had been using throughout the day were used.

It was explained to the students that deleting files is not the same as destroying a file. To prove the point

the students conducted a backup the files from their USB sticks to their hard drive and then deleted them off of the USB stick.

With the files deleted from the USB sticks, but still safely stored on the hard drive the students were shown how to use a forensic tool to see that the files were still there, only the pointer had been removed. The students then used the tool to recover the deleted files from their USB sticks. This allowed the students to not only restore the file, but also explore file header information and even the file contents before it was recovered. This block of instruction concluded with a demonstration of a Department of Defense (DOD) level wipe of the USB stick. The technical details of how and why this was an effective method for most deletion activities was explained as the students waited for the wipe to complete. It was also explained how it would likely require an electron microscope to recover anything and how it was too time consuming and costly for most law enforcement agencies or private citizens. The idea that shredding and melting a disk is the only way to ensure information has been deleted was also discussed by the students.

The lessons learned from the session were well received by all the students. Most seemed truly amazed that data could be so easily recovered and at how long deleted files actually remain intact, especially on super capacity drives available today.

H. USER EDUCATION

The overall exercise was concluded with a network security simulation called Cyber Protect. It is an unclassified network simulation that is like a computer game, created for training of DOD personnel. The simulation elegantly brings together all the points of the days exercise. It incorporates many information assurance facets, from protecting against social engineering and user training to proper placement of intrusion detection devices and the use of backups. In the simulation the student is acting as the network administrator of an enterprise level network and is given resources to protect the enterprise. The students must evaluate the network, analyze the threats and use their limited resource to mitigate the risks. The game goes through four financial quarters where it randomly generates different style attacks. Each quarter the administrator is given more money and they need to buy new protections as well as upgrade and patch old ones. In the onset it was thought that the game would be too intricate and detailed for the students but they caught on very quickly and did a great job of trying to protect against insider threats and lack of user training. In the future this game will be used at the beginning as well as the end and see how effective the IAE is as far as user training goes. From this singular experience however, it seems the learning points and goals were being accomplished..

The introduction of the Cyber Protect simulation brought home all the key points of the days exercise. It also gave the students an understanding the many facets of the information assurance field.

V. DIFFICULTIES

There were a few difficulties encountered that had not been anticipated. Two of them were tied to the systems chosen for use in the exercise. In order to allow the students to have physical access to the machines and use questionable software, old surplus systems were used. As a result, only USB 1.0 was available and since the smallest USB flash memory drives purchased for this exercise were 2GB sticks, the backup and recovery module took much longer than expected. This was the only portion where the exercise seemed to drag, but it was a good demonstration in that backing up enterprise level systems is a very slow, boring process and that is why many people do not do it. Secondly, due to the age of the systems there was a single system failure during the exercise. Fortunately proper planning helped out and there was an extra systems standing by. The lesson learned here is to use new, cheap systems for the exercise. With the overwhelmingly positive response the cost is justified.

The second problem was with the number of potential people participating it was difficult to give everyone the attention needed. To remedy this problem there will be a student hand out and additional assistant instructors and future exercises.

VI. BENEFITS

Based on the evaluation and the discussions with the students following the exercise it was very successful. All of the students asked for applications to the graduate program, information about the lab, as well as information about information security as a discipline. This demonstrates that hands-on exercises even for a day can spark enough interest in security to draw students in. It is a way for students to explore the opportunities without having to commit to a program. Also, this demonstrates that students can be interested by more realistic scenarios and not just by

red team and blue team competitions.

Another major success was that the students had significantly varied backgrounds but they all were able to successfully complete all of the scenarios. This means the goal of making the exercise open to many people of various backgrounds had been achieved. The students expressed a high level of satisfaction with the flow and pace of the program. Also, the students did very well on the CyberProtect game, exceeding the goals for the level of knowledge they walked away with.

VII. IMPROVEMENTS

As mentioned previously there will be numerous improvements to the Information Assurance Exercise

1. Use more up to date systems to improve the speed of the backup and restore portion of the program.
2. Increase the number of instructors or helpers available to the students.
3. Publish an Information Assurance Exercise workbook that covers in more detail each of the topics presented in the exercise and provides a useful take away for the students.
4. Use the Cyber Protect game before and after the activities to measure students' learning.
5. Create multiple versions of the program to target different technical levels

VIII. CONCLUSION

For a pilot run, this exercise was very successful and improved executions of this exercise are already being planned. It demonstrates that students can be drawn in to Computer Science and Information Assurance without lengthy preparation times before hand or any relevant prior experience.

The Information Assurance Exercise demonstrated how easily students could be engaged in the field of computer science and information assurance. The reaction and feedback from the pilot group shows great promise for using this exercise as a way to introduce computer science to students in a way that is not overly technical or intimidating.

The implications from this exercise really affect all Computer Science areas. Other day-long exercises can be modeled based on this to help and grow the discipline

REFERENCES

1 National Security Agency list of Centers for Academic Excellence in Information Assurance Education, http://www.nsa.gov/releases/cae.cfm

2 National Security Agency list of Centers for Academic Excellence in Information Assurance Research, http://www.nsa.gov/releases/cae_r.cfm

3 Matt Bishop. Deborah A. Frinckle. Information Assurance Education: A Work In Progress. Security & Privacy, IEEE, pages 54-57, Sept.-Oct. 2008

4 Department of Homeland Security, "Protecting Our Federal Networks Against Cyber Attacks", April 8, 2008. http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm

5 Federal Networks against Cyber Attacks", April 8, 2008.http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm

6 Elliot Koffman , Heidi Ellis , Charles Kelemen , Curt White, Steven Wolfman, New paradigms for introductory computing courses, Proceedings of the 38th SIGCSE technical symposium on Computer science education, March 07-11, 2007, Covington, Kentucky, USA

7 Paul J. Wagner , Jason M. Wudi, Designing and implementing a cyberwar laboratory exercise for a computer security course, Proceedings of the 35th SIGCSE technical symposium on Computer science education, March 03-07, 2004, Norfolk, Virginia, USA

8 National Security Agency 8th Annual Cyber Defense Exercise, http://www.nsa.gov/releases/cdx.cfm

9 Midwest Regional Collegiate Information assurance comp, http://ccdc.morainevalley.edu/

10 Lillian N. Cassel, Gordon Davies, William Fone, Anneke Hacquebard, John Impagliazzo, Richard LeBlanc, Joyce Currie Little, Andrew McGettrick, Michela Pedrona. The computing ontology: application in education. Annual Joint Conference Integrating Technology into Computer Science Education, pages 171-183, 2007, Dundee, Scotland