# A Hands-on Approach to Computer Security Instruction

***Rayford B. Vaughn, Jr.***[1] ***and David A. Dampier***[2]

**Abstract** – This paper describes a full semester upper level undergraduate and graduate level engineering course in computer security which has a lab component and an innovative end of the semester "Capture the Flag" contest that hones the computer penetration skill sets of the students in the class. The full paper describes the twelve laboratory experiences that the students are exposed to during a semester and the three class periods devoted to penetration testing tools and techniques to include the competitive capture the flag exercise at the end of the class during which students work in teams to penetrate systems and win prizes in doing so. The paper also describes how students are motivated to write publishable papers which have resulted in more than twenty peer reviewed student conference and journal publications – several of which have earned "best student paper" awards at the conference in which they were presented.

*Keywords:* Information Assurance Curriculum, Computer Security Curriculum, Active Learning exercises

## INTRODUCTION

Mississippi State University is one of the early National Security Agency designated Centers of Excellence in Information Assurance Education (CAE/IAE) which has greatly assisted the growth of the security program at MSU. While this paper concentrates on the security classes and hands on experience, the support and assistance from grant programs at NSF, NSA, Army Research Laboratory, and others is credited in providing the laboratories and infrastructure support to make the "hands on" approach viable. This paper specifically describes the evolution of instruction in what we term a "split level" course (i.e., a course for upper level undergraduates and graduate students together) titled Information Assurance and Computer Security. When first offered in 1999, the course was delivered only by lecture. Over time, it has evolved to a highly interactive, laboratory enhanced, hands-on course culminating in a competitive "Capture the Flag" contest. There are a total of twelve independent labs to be accomplished, two special lectures on tools useful in defending systems and in penetration testing. One full class lecture is dedicated to use of a powerful penetration testing framework known as Metasploit [1]. Guest lectures are scheduled though National Science Foundation and National Security Agency grants in order to expose students to security engineering practitioners and scientists in the field. In a split level class, graduate students are expected to write a "publishable" paper on some aspect of security in order to create a research component for those students. Undergraduates are encouraged to write such a paper also in exchange for the option of replacing one of their three exam grades with the paper grade. Additionally, any student that obtains acceptance of their paper in a peer reviewed conference is sent to the conference by the instructor in order to present their work – an additional motivating factor.

[1] Department of Computer Science and Engineering, PO Box 9637, Mississippi State, MS 39762, vaughn@cse.msstate.edu

[2] Department of Computer Science and Engineering, PO Box 9637, Mississippi State, MS 39762, Dampier@cse.msstate.edu

The remainder of this paper describes the class itself (to include major topics, lab exercises, and funding sources), a separate description of the tools and techniques classes to include a final capture the flag exercise, a section briefly describing the growth of our security program and its outreach, and a final summary.

## THE CLASS

The class itself is conducted over a sixteen week semester. Topics addressed during the semester include a historical perspective of information assurance, operating system security, data base and data mining security, network security, control systems security, administering security (policy and procedure), defense in depth strategies, privacy, and a brief introduction to cryptography (we offer a full semester course on network security and cryptography, so it is not addressed in great detail within this introductory course). This class has been offered every Fall and Spring semester for the past several years and averages approximately 35 students per class. For ten years the class has received very high student evaluations and its popularity has grown. Initially, the class was taught solely by lecture. Students evaluated the class with very high marks, but began suggesting that they would like to have some practical experience with the subject and would enjoy working with some of the tools used by security engineers. Seeking to accommodate the student suggestions, the authors pursued external funding to establish the necessary isolated lab infrastructure to support the class and support for the development of an interesting, but not dangerous, set of lab exercises. The remainder of this section describes the funding sources found for the infrastructure and class support upgrades followed by a description of the lab exercises. These exercises can be made available to other U.S. universities by request to the authors. Last we describe the final live fire exercise referred to as “Capture the Flag”.

During the semester, we strive to bring in speakers that are well known by reputation or who are practicing security engineers. Our target is a minimum of three such speakers each semester. By doing so, we tend to motivate the students in their security studies and we are then able to expose our program to these speakers who help us promote in on a national basis. In the past we have hosted Dr. David Bell (from the Bell/LaPadula Model of Computer Security); Dr. Matt Bishop (text book author); Dr. Charles Pfleeger (text book author); Mr. Lance Spitzner (Honeypot author); Dr. Fred Cohen (expert on malicious code); and multiple security engineers from the corporate world (e.g. Harris Corporation and Cisco).

### Sources of Funding

Establishing the necessary infrastructure to support an information assurance laboratory and supporting staff to maintain it is not an inexpensive proposition. Fortunately two government funding sources were discovered that specifically address the building of capacity to teach information assurance and both exist today. The first of these is sponsored by the Department of Defense and the Department of Homeland security and is known as the Information Assurance Scholarship Program or IASP [2]. The second is administered by the National Science Foundation and is referred to as the Scholarship for Service program or SFS [3]. While both IASP and SFS are primarily designed to provide scholarship funding to US Citizens pursuing a BS or graduate degree while concentrating their studies in information assurance, both programs also have what is known as a “capacity building” track designed to provide competitive funding to assist with information assurance curriculum enhancements and having a broad range of supportable activities. An IASP capacity building grant is generally granted in the range of $50,000 to $75,000 while an SFS capacity building grant averages approximately $150,000 for a two year period. Both such grants were used to enhance our program. As a matter of being complete for the reader, it is important to point out that the grant sources mentioned are open only to those institutions which have achieved a designation of Center of Academic Excellence in Information Assurance Education (CAE/IAE) by the National Security Agency. The requirements and qualifications for this designation are beyond the scope of this paper but the reader can find them at [4]. It is also important to point out that if an institution is not a designated CAE/IAE, capacity building funding is still available by submitting a collaborative proposal or entering into a partnership with an institution that is a CAE/IAE. A list of these institutions is also available at [4]. Using these funding sources, the authors established several laboratories at their institution – a basic computer security laboratory; a security laboratory for business information systems students; a forensics laboratory; and a control systems laboratory. The basic computer security laboratory is shown in Figure 1.

### The Laboratory Exercises

The basic computer security laboratory is an isolated facility containing over twenty desktop machines, a compliment of hubs, routers, switches, and firewalls, and a separate machine set up to host Norton's Ghost Server. Students are not restricted on the type of security experimentation they are allowed to participate in subject to the following general guidelines given at the beginning of each semester.

- Do no harm to others
- Do no work on lab machines other than security class labs or research.
- Use the card key entry system for every entry to the lab (for accountability)
- Do not touch the Ghost server in any way (electronically or otherwise)
- Any experimentation outside the assigned lab exercises must be discussed with the instructor

**Figure 1. Computer Security Laboratory**

There are a total of twelve exercises that are given to the students at the beginning of each semester. The labs are due in consecutive order beginning with Lab 1 due at the beginning of the first class of week #2. Each subsequent lab is due each week in the same manner. By following this procedure, the students automatically know that they have 7 days to accomplish each lab on their own time and that the labs are due weeks 2 through 13 of the semester. There is also a Lab "0" that we include which provides specifics concerning the lab architecture, passwords, and useful information on specific operating systems commands. Each exercise is briefly described below.

- **Lab 0 INTRODUCTION:** This lab is used to familiarize the student with some of the OS commands they will need to complete the lab exercises during the semester and to present an overview of the lab itself. Specific login information is given to the students, to include "root" passwords which are needed for certain labs. The facility contains a mix of systems using Linux, Solaris, and Windows OS with various patch levels. Since not all students are familiar with the details of each OS used, this lab provides a useful reference. It should be noted here that students in this class come from a variety of backgrounds to include Management Information Systems, Computer Science, Electrical Engineering, Computer Engineering, and Software Engineering – so the technical skill sets are widely varied.

- **Lab 1 PASSWORDS AND ENUMERATION:** This lab is designed to show the students the importance of selecting and maintaining strong passwords. Students are given a general set of rules on what constitutes a strong password and then are asked to create five user accounts on both a Windows machine and a Linux machine. They are given specific guidelines on how to create two of the five passwords (making them weak) and left to their own decisions on the other three. They are then instructed on how to use a password cracker "John the Ripper" and to attempt to crack the five passwords they created – plus another file of passwords provided to them. Students then learn how fast a cracker breaks a weak password and the value of a strong password. They also compare differences in timing between Linux and Windows OS. As a final part of lab 1, students establish a "null" session between machines using the enum tool and then using the enumeration information provided to exploit accounts.

- **Lab 2 PGP:** This lab teaches the students how to use Pretty Good Privacy (PGP) as an open source encryption tool. Students go through a tutorial on PGP in the lab readings and then install and use PGP on both a Windows and Linux/Solaris system. They not only learn how to use a valuable tool – they also become familiar with public key cryptography in the process.

- **Lab 3 Email Spoofing:** Email spoofing is a fairly common technique used today in Spam and Phishing attacks. It can also be used to trick a user into performing an action or providing sensitive information to an attacker. This exercise demonstrates to the student how easy email spoofing is accomplished, vulnerabilities in the SMTP protocol, and how to effectively read email headers. The student better understands why it is important to deny open relaying from email servers and how to reduce the amount of spoofed emails entering their corporate networks.

- **Lab 4 Steganography:** Many students are not familiar with the notion of steganography and how it can be used in various ways from data hiding to watermarking. Students are taught the concepts and limits of steganography, how to use existing tools to hide data in a JPEG image, how to use statistical tools to detect such images, and how various file formats are subject to being used for steganography. Tools that are used in this exercise include Jphide, Jpseek, Stegdetect and Stegbreak. All tools are provided on a CD to the students.

- **Lab 5 Network Scanning and Footprinting:** For this lab, we encourage the students to work in pairs or teams. The lab exposes students to a common problem faced by network administrators – the use of insecure rogue systems on a network. Students use NMAP for port scanning and NETCAT to determine what services are running on target systems. They are exposed to "banner grabbing" and how easy it is to footprint a system as an attacker. All exercises are ran on a Linux machine.

- **Lab 6 Sniffing and Shared versus Switched Environments:** Students use this lab to gain an understanding of hub and switch technology and the vulnerabilities associated with each when faced with a sniffer threat. Students perform the exercise in both a Windows and Linux environment with Hub and Switch equipment provided in the lab. Students are asked to work in teams so that the lab administrator can assist with the cabling requirements in a more efficient manner. During this exercise students are exposed to Wireshark as an open source sniffer on Windows machines and etttercap as a sniffer on Linux systems. They are also introduced to the Address Resolution Protocol (ARP) and attacks against ARP tables.

- **Lab 7 Tripwire:** Tripwire is used to demonstrate basic intrusion detection. As an open source tool, it is used to determine what changes, if any, have occurred on a system. It monitors attributes of files and is able to report any changes to those files. Students are shown how to install Tripwire and how to use it. The notion of using it to detect changes to Honeytokens is also suggested. While this is the most basic of IDS tools – it is used to open the discussion on IDS.

- **Lab 8 Using SNORT (A network intrusion detection system):** Network intrusion attempts are so frequent that no matter how well a network is designed, it cannot avoid intrusion attempts. Students install SNORT and review audit logs resulting from its installation. They are also taught the difference between host-based and network-based intrusion detection during this exercise. A part of the lab is designed to allow students to install a SNORT rule set and to modify that rule set.

- **Lab 9 Exploit Development:** This lab is one of the more difficult and students are asked to create a buffer overflow exploit in code. Students are provided with a program called "corkboard" that has intentional coding errors in it that render it vulnerable to a buffer overflow attack. If they exercise the lab correctly, they implement a buffer overflow attack that allows them to elevate their privileges from user to root.

- **Lab 10 Comparing SARA, STAT Scanner and Nessus:** Vulnerability scanners are a necessary tool for system administrators today and are used to find vulnerabilities and to patch them. Many are on the market – some commercially available and others that are shareware. Students use three such tools in this exercise to gain experience with scanning networks for vulnerability analysis. They employ SARA (Security Auditor's Research Assistant) which is freely distributed; STAT Scanner, a commercial tool offered for license by Harris Corporation; and, NESSUS, a security scanner available for free download.

- **Lab 11 Introduction to Digital Forensics:** Basic computer security students are introduced to digital forensics in this lab. We offer a full semester course on this topic and the lab is designed to acquaint students with the topic and to garner their interest in learning more. They must document their activities and search for evidence on an evidence drive. The evidence consists of a large number of photographs of "weasels" that hidden in several different ways. Students use a Knoppix disk to boot a system, acquire evidence using a suite of available tools, learn about hashing an evidence disk, and explore for evidence.

- **Lab 12 Firewalls and VPN's:** The purpose of this lab is to help the student understand the principles of firewall security, configure a firewall, understand the concept of a VPN and to configure a VPN. For this lab, a Cisco Pix 515 firewall is used. Students gain experience in configuring the Pix firewall and using it to establish a VPN.

While each of these exercises in their own right are not exceptionally difficult, taken as a whole they significantly augment the class with active learning exercises. By assigning one exercise each week, the students can choose their own time during a seven day period to apply a hands-on exercise to what they are being taught in lectures. They are also told that the exercises will teach those tools and techniques that will be helpful during their final Capture the Flag competitive exercise at the end of the semester in which prizes are awarded to each team. This proves to be adequate motivation for the students to complete the exercises. For grading purposes, each lab is graded with an overall value of 10 points per lab. Lab performance counts 10% of the final course grade.

### The Tools Lectures

Two special lectures are conducted toward the end of the class that are designed to reinforce the tool expertise gained during the lab exercises and to prepare the students for their penetration exercise. During the tools lecture, students are shown a series of tools, given the web site for tool download, and the tool is briefly demonstrated to them. The lecture divides the tools into those that help with reconnaissance, enumeration, exploitation, analysis and system hardening. While it is not the intention to present all off the tools here, we do wish to briefly describe them to the reader. Additional information is available from the authors.

- **Reconnaissance tools:** We present a number of tools here that can help the student discover information about a targeted system. By exposing the student to these tools, the student can better understand how to defend against them. Tools included are p0f for OS fingerprinting; Network Stumbler for discovering wireless network characteristics; Google for search directives and cache information; and Netcraft for webserver information.

- **Enumeration tools:** Enumeration helps the attacker know more specifics about the operating environment to be exploited. For this lecture, two important tools are covered – NMAP and Nikto. NMAP provides a host of services to include OS fingerprinting, port scans, and other services. Nikto is a web scanner and assists an attacker in finding vulnerable web services.

- **Exploitation tools:** To actually exploit a system, tool support is very useful. Students are introduced to the Metasploit framework, one of the most powerful penetration tools available (essentially a point and click penetration tool); TCPreplay to replay packets on the network; hping2 to craft packets and OS fingerprinting; NetDude for packet crafting; and Cain and Able for wireless sniffing, VoIP recording, and password recovery.

- **Analysis tools:** As a security engineer, the ability to analyze network activity and diagnose problems is essential. Students are shown Microsoft Sysinternal tools [5]; ntop for analysis of network IP traffic; and VisualRoute to visualize network path data.

- **Hardening tools:** There are many automated tools available to lock down systems and make them more resistant to attack. Our students are shown a sampling of these to include Bastille as a tool to harden Linux, HP-UX, Mac OS X and other OS; IPtables as a host based static firewall; and Truecrypt as a freeware product to encrypt laptops.

Once the initial tools lecture is complete, a second lecture is more specifically directed toward the final CTF exercise. During this second lecture, the tools that were demonstrated above are actually used in class in a life fire demonstration that shows how they are used in sequence and how the information gained from one is used in another to further the attacker's objective. In other words, the students are shown how to put it all together.

### The Capture the Flag Contest

The last class prior to the final exam is used to host this contest. The students are divided into 5 person teams (approximately) with an attempt made to balance technical expertise between each team. Each team has a team captain appointed and 3 laptops configured for the exercise. Each team is allowed to bring one extra laptop with them with tools pre-installed. That laptop may not be connected to the CTF network. Two system administrators are used to assist the students with technical assistance and periodically, the students are given hints based on the overall progress of the class.

**Figure 2: System Administration Staff setting up the exercise**

In figure 2, the system administration staff is configuring the room and the isolated network for attack. Each team has a separate circular table with the three laptops configured and wired when the team arrives in the room. Prizes are announced ahead of time and displayed in the room when the class arrives (as shown in figure 3).

**Figure 3:  Prizes for winning teams**

The prizes tend to be a real motivator for the students (plus the obvious bragging rights that come from winning). We simply purchase "office supply" items that they students can use.  For our most recent exercise, the prize table contained 2GB USB drives with snap links; wireless optical mouse; neon colored R/W CD's; laser pointers, computer security books, and portfolios.    The team placing first is allowed to choose their prizes first, second place second, and so forth.  We have found it helpful to invite the news media to witness the event and to document it for local media.  By doing so, we are able to further motivate the students and to advertise our program at the same time.  The most interesting side effect of this exercise is the intensity seen in the students during the exercise.  They prepare hard for this exercise and, judging from the comments we receive on end of course evaluations, they find it instructive and fun.  Representative student focus can be seen in figures 4 and 5 below.

**Figure 4: A five person student team working together in CTF competition**

**Figure 5: Multiple teams competing during CTF**

## SHARING AND OUTREACH ENDEAVOR

We have been active in the past with other universities in sharing our class exercises, our lab architecture, and curriculum design. We have also assisted a number of universities with their applications to the NSA for CAE/IAE status. By doing so, we have developed strong collaborations and have increased our reputation nationally. Some of these outreach efforts have subsequently led of research collaborations. Examples of our outreach include teaching a security class (full semester in length) to Jackson State University and Tuskegee University (both designated as Historically Black Colleges or Universities) and to students at the University of Alaska Anchorage during the summer of 2006. We have assisted in successful CAE/IAE applications at New Mexico Tech, Illinois Institute of Technology, DePaul University (Chicago), Dakota State University, the University of Louisville, and others. We currently are engaged with universities seeking that status and assisting them in doing so.

We also developed a very strong outreach program now funded by the Department of Justice which involves the training of state and local law enforcement in digital forensics techniques. While not the subject of this specific paper, we would point out that in less than 24 months, we have trained (free of charge) more than 1200 law enforcement officers and assisted in establishing a Cyber Crime Fusion Center in our State capital of Jackson where Federal, State, and Local law enforcement work together with academia to address computer crime in the State of Mississippi. We believe this is a one of a kind mode. The facility is housed in a 10,000 square foot floor of our State office building (see figure 6).

**Figure 6: Mississippi Cyber Crime Fusion Center (17th floor of State Office Building)**

## SUMMARY

We have outlined a very hands-on, active learning environment for our information assurance students at Mississippi State University. This paper has focused specifically on one course – the introductory course on Computer and Information Security. We also have described our approach to lab exercises and tools instruction and have offered to share the specifics on request with other universities. It is important to emphasize that a key component of our educational philosophy is that of maintaining a tie between classroom discussion and real world activity. We do this through our guest speaker program, our law enforcement collaboration, and by using real commercial and free-ware tools in labs and class exercises.

## ACKNOWLEDGEMENTS

The authors wish to acknowledge the strong and continuing support in our computer security pedagogy and research by the National Science Foundation's Scholarship for Service program (multiple grants); the National Security Agency's Information Assurance Scholarship Program (multiple grants); the Department of Justice Office of Justice Programs; and the Department of Homeland Security.

## REFERENCES

[1] See http://www.metasploit.com (accessed Nov 30, 2007)
[2] See http://www.defenselink.mil/cio-nii/iasp/ (accessed Nov 30, 2007)
[3] See https://www.sfs.opm.gov/ and http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5228&org=DUE&from=home (accessed Nov 30, 2007)
[4] See http://www.nsa.gov/ia/academia/acade00001.cfm (accessed Nov 30, 2007)
[5] See http://www.microsoft.com/technet/sysinternals/default.mspx (accessed Nov 30, 2007)

**Rayford B. Vaughn, Jr.**

Dr. Vaughn received his Ph.D. from Kansas State University in 1988. He is a William L. Giles Distinguished Professor and the Billie J. Ball Professor of Computer Science and Engineering at Mississippi State University and teaches and conducts research in the areas of Software Engineering and Information Security. Prior to joining the University, he completed a twenty-six year career in the US Army retiring as a Colonel and three years as a Vice President of DISA Integration Services, EDS Government Systems. Dr. Vaughn has over 100 publications to his credit and is an active contributor to software engineering and information security conferences and journals. In 2004, Dr. Vaughn was named a Mississippi State University Eminent Scholar. He is the current Director of the MSU Center for Critical Infrastructure Protection and the Center for Computer Security Research.

**David A. Dampier**

Dr. David Dampier is an Associate Professor of Computer Science and Engineering at Mississippi State University. He received his PhD in Computer Science from the Naval Postgraduate School in 1994. He currently serves as Director of the Southeast Region Forensics Training Center, responsible for teaching state and local law enforcement officers across the southeastern United States to solve computer crimes. He is a retired Army officer and 2003 winner of the ASEE-SE New Teacher of the Year Award. He served as President of the Software Engineering Division of the ASEE-SE and Secretary of the Instructional Division. His research interests are in Digital Forensics and Software Engineering.