A Virtual Environment for IA Education

Daniel J. Ragsdale, Scott D. Lathrop, Ronald C Dodge JR,

Abstract-- *With the increased potential of a bona fide cyber terrorist attack and the possibility of a future "war in the wires", we must continue to improve the education, training, and resourcing of individuals responsible for defending our national borders—whether those borders be physical or electronic. The Information Analysis and Research (IWAR) laboratory at the United States Military Academy (USMA) has proven to be an exceptional resource for such an education for our students and faculty studying information warfare and information assurance. The lab has also been successful in motivating the need for continued education and training in this area on a much larger scope. A recent initiative, the Virtual Information Assurance Network (VIAN) allows us to provide a robust and fully configurable network for each student to administer in the pursuit of Information Assurance mastery-contained on a single computer! This paper justifies why information warfare labs are necessary, describes the phenomenon that is occurring as a result of the IWAR lab, explains the current configuration, and presents lessons learned that others might use in designing an Information Warfare laboratory.*

Keywords -Information Assurance, Information Warfare, Information Assurance Education, Vulnerability Assessment

I. Introduction

Two years ago, the Information Technology and Operations Center developed the initial Information Warfare Analysis and Research (IWAR) laboratory to support undergraduate education and faculty research in Information Assurance (IA) at the United States Military Academy. Since that time, it has matured into a much larger and robust laboratory. What began as a single, isolated network has matured into three separate networks and a library. Each component has a distinct purpose but all are aimed at furthering education in Information Assurance at West Point and throughout the IA community.

While this presented the student with the opportunity to observe reactions on a target network and machine to various scans and/or exploits, the students were unable to alter or set up the configuration on any of the servers or network routing. Additionally, after executing exploits the target machine would be unavailable for other students. What was lacking in their experience was the ability to exercise complete control over their environment by administering each server and configuring the network while not interfering with another student's exercises.

The intention of this paper is to provide an overview of the recent configuration changes that allow each student to be the administrator over a portion of the network, facilitate the instruction of a wide variety of Computer Science and Information Assurance courses, and be used to support research and vulnerability experimentation.

II. Original IWAR

The original purpose of the IWAR lab focused on providing an isolated lab where students enrolled in our Information Assurance course could familiarize themselves with various known computer security exploits and employ technical measures to defend a network against such exploits. Additionally, the lab provided a facility for faculty members to conduct research in Information Assurance. [1] Currently, the lab serves not only the Information Assurance course which is limited to computer science and electrical engineering majors, but also provides support for our ACM SIGSAC student chapter; supports the annual CyberDefense Exercise (CDX) conducted with the other military academies (Navy, Air Force, Coast Guard, Merchant Marine, and Naval Post Graduate School), and in conjunction with the NSA's red teams, the 1st Information Operations Command, and the 92d Air Force Aggressor Squadron [2]; is used as a focal point for congressional, academic, military, and other visitors interested in observing or replicating our work; and is used for information warfare demonstrations for the freshman cadets. The purpose of this demonstration is to motivate the plebes to take advantage of the lab and IA course while they are at West Point.

The IWAR lab is a completely isolated network that we often compare to a firing range. The Army uses firing ranges to train soldiers on individual weapons and firing systems. Likewise, the IWAR lab is a range where students and faculty may use and experiment with port scanners, vulnerability scanners, Trojan horses, worms, and viruses without running the risk of releasing malicious code onto our production network or into the "wild". Just as a solider would only fire a weapon on the range or in combat, the IWAR network policy only permits users to use the IA tools in the controlled confines of the lab.

Lieutenant Colonel Daniel Ragsdale, Ph.D. is with the United States Military Academy at West Point, NY and is the director of the Information Technology and Operations Center Email: Daniel.ragsdale@usma.edu

ISBN 555555555/$10.00 © 2003 IEEE

Malicious software that exploits system vulnerabilities is installed on select systems within the lab, allowing cadets and faculty to learn about, and experiment with, the capabilities of potential adversaries. Through experimentation with malicious software, users gain an appreciation of the numerous vulnerabilities existing in currently deployed information systems. With this knowledge IWAR lab users are better equipped to protect and defend the information and information systems for which they are, or will be, responsible.

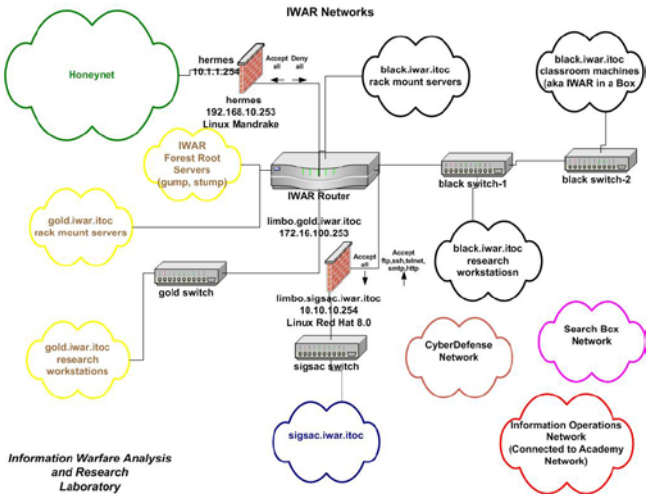

Figure 1 IWAR Lab configuration

The current network, shown in Figure 1, approximately 200 nodes, consists of two primary LAN segments based on the United States Military Academy (USMA) school colors. The *black* segment contains the classroom student machines, "soft" server targets, and a few administrative machines. The *gold* segment, separated from the *black* network by a router and a firewall, consists of a few administrative machines and several "hard" targets. "Soft" targets are computers that have a default operating system installation and configuration with no patches applied. The only "hardening" that has been done to these machines is to insure that all local and domain administrative passwords are strong. Otherwise, the systems are wide open. The "hard" targets are harden using the SANS and NSA guides and applying the current patches to the operating systems. The *black* network serves as the lab's "LAN" while the *gold* network attempts to portray the remaining *Internet* from the perspective of the users on the *black* network. This paper will focus on the benefits provided by using a virtual network on our classroom machines (top right hand "cloud" in Figure 1) to enhance IA education and research.

There are several other courses at USMA, which use the lab in addition to the computer science based, Information Assurance course. Almost every CS course uses the lab for computer security related lessons. A political science course entitled, "The Policy and Strategy of Cyberwar" uses the IWAR lab exclusively as their classroom in order to demonstrate the technologies that common hackers and cyber-terrorists use to gain access to computing resources and then to relate those experience to strategic level policy issues. The Cyber Policy course includes hands-on exercises where the cadets build viruses, worms, and malicious applets. The "Cyber Law" course uses the lab for lessons given to pre-law students to form an appreciation of the tactics and techniques used by cyber-criminals. Finally, the IWAR lab provides USMA with a facility to learn about emerging information warfare. Computing infrastructure upgrades and initiatives often begin in the IWAR lab before moving them to the user base. For example, the lab has been used to install a Windows Active Directory infrastructure before deploying it on a larger scale. It has been also used to familiarize, test, and validate wireless security solutions prior to decisions being made on whether or not to install a wireless network.

III. Related Solutions

Primarily due to the increasing importance of IA education, many colleges and universities are beginning to invest resources towards the construction of information security laboratories. [9, 11, 12] Others have been looking at using simulation-based tools to educate their students. [13, 14] To the best of our knowledge, no one has attempted to design and implement a lab on the scale or complexity currently exhibited by the IWAR lab. Others have created labs, primarily to serve different purposes, but none have the similar heterogeneous nature or scale that the IWAR demonstrates.

Kaucher and Saunders describe an Information Assurance laboratory that they use at the National Defense University for educating information assurance and information security professionals. Their network serves a different purpose and thus does not need to be the same scale or complexity as we have built into the IWAR lab. Similar characteristics include a heterogeneous network. One of the unique features of their network is that they expose the entire network to their students. This works well for their particular situation, as their students often need to see the entire network to "demystify the technology." [9] However, for this particular application major portions of the network are not revealed to the computer science and electrical engineering majors taking the IA course. This forces students to conduct reconnaissance using port scanners and similar tools. Exposing the network might be a better idea for Cyber Policy and Cyber Law courses.

Others have taken heterogeneous networking to another level by implementing different layer 2 architectures such as Ethernet, Asynchronous Transfer Mode (ATM), and Fiber Distributed Data Interface (FDDI) on a token ring. [12] Their network design is different from ours in that they are using it more for system modeling and simulation, networking, and special projects rather than information warfare. The scope of their network is also much smaller and where our heterogeneous nature consists of multiple operating systems and services, their heterogeneous flavor is a result of different link layer protocols. Some

similarities also exist, however. We have begun establishing a wireless network using the 802.11b protocol in order to further investigate the security issues surrounding this wireless protocol.

Yasinsac describes a computer security laboratory project for outreach, research, and education. Their laboratory serves a similar purpose as the IWAR laboratory but on a smaller scale. Similar to the IWAR lab, they have been challenged to provide an environment where students are free to explore without creating administratively challenging headaches when systems break because of the use of certain tools. One of their solutions is to use a virtual machine software wrapper created by VMware. [11] Yasinsac uses VMware to provide a mechanism of configuration control over a single machine; the user boots the computer and launches a single "guest" operating system (OS). The user then operates within the guest OS and when done all changes made to the guest OS can be un-done. We also use VMware but in a significantly different paradigm. We use VMware to provide the student with a fully configurable network that they are administrators over. This solution is the focus of this paper and is discussed at depth in section IV.

Others have begun designing or looking at simulation based-tools to educate others in IA. Simulations also allow the proposed network to be tested by a larger variety of conditions and attacks than would be feasible with a real network. There may also be a number of attacks that are too dangerous to perform on the real system. [13] However, to the best of our knowledge, many tools exist that model networks, but no tool exists that accurately models the specific decisions that must be made to simulate an IA education. A proto type simulation for use in IA curriculum is being developed at the United States Military Academy, but it is not yet being used for instruction. [14]

One of the greatest advantages of a simulation environment is typically the reduced administration load. The implementation and maintenance of an IWAR type lab requires significant investments in terms of hardware, software, and human resources to build and maintain the physical networks of computers and communication components. This is not a unique problem. The use of a VMware solution provides a significant level of relief due to its ability to operate in a non-persistent mode and its ease of re-imaging (which is as straight forward as copying over the content s of one folder).

IV. Virtual Information Assurance Network (VIAN) Solution

The IWAR laboratory consists of a set of student workstations connected to an isolated network that present the student with a wide variety of services and operating systems, as originally cited by Schafer.[1]. While this gives the student an opportunity to observe reactions on the target network and machine to various scans and/or exploits, they are unable to alter or set up the configuration on any of the servers on the network or control the routing and firewall policies. Additionally, after executing exploits that may cause significant damage, the target machine may need to be rebuilt. What is lacking in their experience is the ability to exercise complete control over their environment by administering each server and configuring the routers. The VIAN concept allows us to offer complete administrative control to the student without placing the network or other student s work at risk!

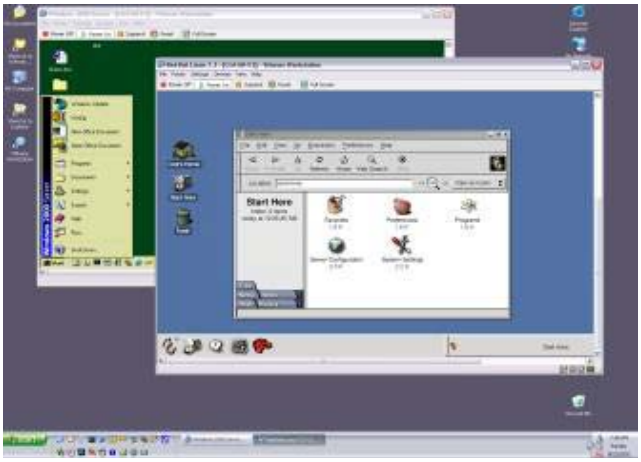

Figure 2 VMware running on Win XP with two guest operating systems

Our implementation uses the commercially available VMware Workstation software package. VMware Workstation allows you to create one or more virtual machines that run within a secure virtual boundary on a base operating system. You can run VMware on a host machine running Windows NT4, 2000, and XP, as well as Linux. (See Figure 2). The virtual machine (guest) OS can be any variant of Windows, DOS, or Linux. You can load as many guest operating systems as you have disk space for, and they can be run side by side if enough RAM memory is available on the host machine. Our implementation runs six virtual machines simultaneously with no significant latency problems.

VMware provides a layer between the host OS and the guest systems that provides an interface to all physical hardware resources, as shown in Figure 3. The amount of memory resources (disk and RAM) that a guest OS is assigned and the processor priority are established when the guest OS is installed. This segmentation provides a completely separate environment for each guest OS. When the guest OS is not running, CPU and RAM resources are returned to the host OS.

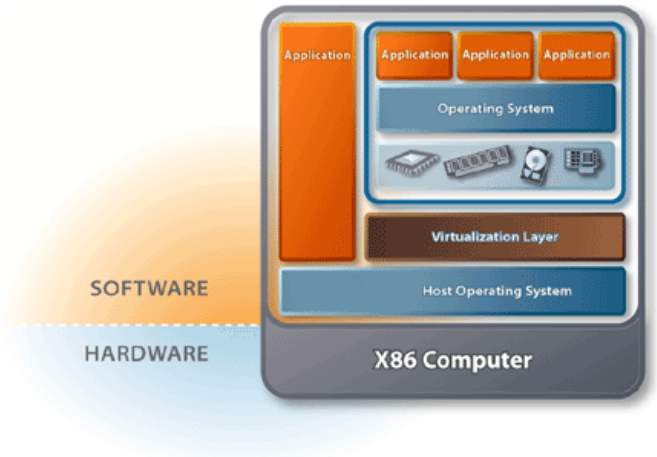

Figure 3 Virtual Machine Architecture

The network configuration for each guest OS can permit it to communicate with only other guest systems, with other guest systems and the host machine or with the external "physical" network using network address translation. This is an important feature because it allows a student to use and see an exploit completely within the virtual network, eliminating possible contamination of a production network.

The VIAN solution offers many advantages over a typical laboratory configuration. They are:

- Adding additional guest systems. The entire configuration file for a guest OS is contained in a folder that, depending on OS type, ranges from 500 MBtyes to 4.5 GBytes. Additional guest systems or copies of an existing gust OS can be added by simply copying the VM folder.

- The guest OS is a full and complete installation of the operating system. All system calls and network protocol operations are executed exactly as if the guest OS was on its own hardware.

- If an exploit or a configuration change causes significant damage to a guest OS, it can simply be deleted and copied back from an archive location.

- The guest OS is capable of operating in non-persistent state. This means that when a guest OS is rebooted, any damage or intentional changes made in the previous session are discarded when the machine ends its session.

- A user is able to exercise complete administrative control over a group of machines and network components. The number of guest operating systems that can exist on a given host is limited only by the amount of hard disk space.

- The ability to operate as an administrator provides an invaluable hands-on learning experience.

- The virtual network can operate in isolation *or* interaction with external networks.

- The VIAN can provide a highly mobile and robust solution by implementing it on a Laptop.

A. Network Configuration

Our first priority for the IWAR lab was to give each student the ability to experience, hands-on, the full authority and responsibility of configuring a functional network as both a network and a server administrator. We started by installing a suit of virtual machines on each student workstation. These are the "firing positions" discussed in the opening section. From each workstation the students can interact with both the other guest systems on the host machine and the rest of the IWAR network. As shown in Figure 4, the possible virtual network configurations are almost limitless.

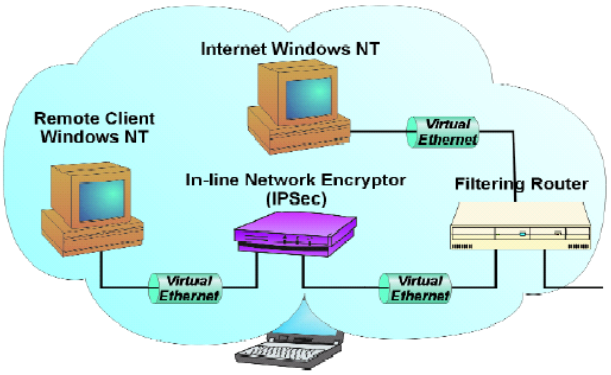

Figure 4 Virtual Machine Network

For our VIAN solution, shown in Figure 5, the host operating systems is Windows XP professional. Using VMware, we installed as guest systems, Windows XP, Windows 98, two Windows NT4.0 Servers, five Red Hat Linux 8.0 systems, and one Red Hat Linux 6.0 machine. The virtual network is designed to present the user with two internal networks, a "red" network, containing machines that are used to launch exploits, and a "blue" network, consisting of target machines. These two networks are separated by a firewall (SNORT) running on one of the Linux guest machines. A second firewall (SNORT), also running on a Linux guest machine, acts as a gateway to the host machine. On the blue network, we have installed two separate installations of WIN 2000 server and Red Hat Linux 8.0 so each dedicated user of a computer has their own set of servers to administer. The red network is shared by each user on a given physical computer. The WIN NT, WIN 98, and Red Hat 6.0 machines are target machines with no administrative requirements. This configuration allows gives each student a "virtual network" on their machine and provides some flexibility and creativity for the instructors and the students

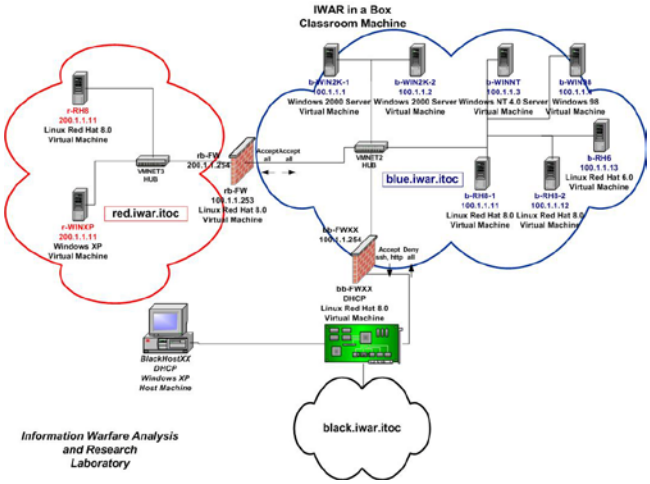

Figure 5 Example Classroom Computer

Our IWAR classroom is currently configured to support two students per physical machine; however adding another set of guest machines to accommodate another user is as simple as copying a folder. Likewise, if a student damages a guest OS, it can be restored in a like manner, from a database of virtual machine folders. A further extension planned for the VIAN is to add a set of guest machines that can be used for students or visitors not part of our Information Assurance course.

B. Education Uses

The primary focus for the development of the IWAR Lab and the VIAN is for use in support of a 400 level Information Assurance (IA) course. In this course, the students concentrate on understanding the fundamentals of Information Assurance; including confidentiality, authentication, integrity, non-repudiation, and availability. The IA course takes the students from understanding the requirements of Information Assurance to a capstone event where the students design, build, and defend a network from attacks. [2] The VIAN solution offers the students direct hands-on experience in:

- Scanning and vulnerability testing.

Port scanning is very bandwidth intensive; 18 students scanning would rapidly bog down a network and possibly place a given machine in a denial of service situation. Each student scanning his own virtual network provides everyone with valuable hands on experience, while eliminating the possibility of network/service failure.

- Hardening multiple operating systems.

The students also are required to examine the various guest operating systems and go through the steps of hardening them against known exploits and common vulnerabilities. In addition to hardening an existing guest OS, the student could install, configure, and then harden an operating system using a security checklist such as from SANS or the NSA. The virtual machines enable the student to perform these functions without having to worry about tampering with the base operating system's configuration. This task would not be economically or space wise supportable in a physical lab where each OS was installed on a separate system.

- Installing, configuring, and testing security tools.

In conjunction with scanning and OS hardening (and throughout the remainder of the course) students must install and evaluate a series of security tools. For many of these applications, configuration and use is far from trivial. During the course, the students will use the VIAN to select, deploy, and configure all the tools necessary to establish and defend their network. They go through a formal decision making process where they evaluate and test each tool. The VIAN provides an excellent resource for this process by enabling each student to have a dedicated network with a variety of operating systems to conduct their investigation.

- Seeing exploits in an isolated (and non-persistent if desired) network.

The traffic in the virtual network is typically very quiet. In fact, if properly configured, there is *no* background packet traffic. This enables a student to monitor network traffic and see only packets that relate to the exact sequence of events leading up to a given exploit. For example, a student may exploit an IIS buffer overflow on one of the guest systems and the packet logs and TCP stream information would show only the traffic associated with the scanning and exploit. On most networks the variety of services running will make network *sniffer* logs very difficult to interpret. For an untrained observer (student), this detracts greatly from the learning environment. Additionally, the severity of the exploit need not be a concern because the target guest OS can be configured to be non-persistent for a given session. Thus when the guest OS is started again, any harm from the exploit was discarded when the OS was shutdown.

- Building Exploits.

A valuable exercise for students is to actually build an exploit. While this can be effectively done in most common laboratory configurations, a "rouge" exploit being set loose on a production network should be a great concern. Developing the exploit on an isolated network eliminates the risk of accidental launching of an exploit and causing unintended harm to a network.

- Planning general defensive measures.

From a defensive perspective, we use the virtual machines to demonstrate the concept of firewalls. The Linux virtual machine running on the "external" network portion serves as the outside world from which the student wants to protect their internal network. The internal network consists of the remaining virtual machines. The students then configure a Linux virtual machine as a firewall

between the two internal virtual networks. Using ipchains, a stateless packet-filtering firewall, we can demonstrate the advantages of a packet-filtering firewall. In order to show a stateful packet-filtering firewall we can then use iptables. Finally, in order to take the exercise to the final level, we can install a proxy server such as Squid on the student's Linux machine and demonstrate the firewall that separates the *black* and *gold* networks.

As illustrated in each of the points enumerated above, it is both economically and space wise unfeasible to provide this level of support using standard laboratory configurations. The VIAN provides the student with a complete environment to learn and practice all the components of securing and monitoring a system and network. For example, a student may want to test an exploit against an IIS sever running on Windows 2000. The individual can create the malicious virus, worm, or applet. After scanning the virtual network (using Nessus for example) for hosts that might be vulnerable to the newly created exploit, launch it from their Linux virtual machine and target the IIS server running on their Windows 2000 virtual machine. The entire attack sequence is isolated to their classroom PC. The student can observe the network packet traffic to determine what the exploit looks like form a network level with very little or no extraneous packet traffic. If the target guest OS was running in non-persistent mode, the student can restart the guest OS, conduct any hardening operations or system patches necessary to thwart the vulnerability. The exploit can then be used again and the student can verify that the hardening actions were in fact successful!

Once the student has perfected their exploit, they can then attempt to target the "soft" and "hard" targets existing in the larger black or gold network. The virtual network configuration "exposes" only a portion of the network, similar to Kaucher and Saunders idea. [9]

The IWAR in-a-box, while very well suited for IA education, is also well suited for other computer science courses. We have explored the possibility of using the virtual network for Operating Systems and Networking courses. Using the VIAN solution for these courses bears similar benefits as explored in our IA curriculum. In all circumstances, providing each student with a robust network where they are the network and systems administrator is almost exclusively not supportable in standard computer science laboratory configurations.

C. Research Uses

The benefits from the VIAN extend beyond that of support for an educational curriculum. Many of the benefits outlined in support of courses transfer directly to active research projects. Specific topics include exploit testing/modeling and signature verification, network protocol development, and IA tools and services development.

One research area currently using the VIAN solution is exploit testing/modeling and signature analysis. As pointed out previously, there is virtually no background network noise on the virtual network. This enables a very accurate signature file to be documented for a given exploit. Additionally, since the virtual network is isolated from a physical network, the possibility of launching an exploit that very little is know about (especially for newly "captured" exploits) is very small. The ability to conduct exploit analysis with a robust set operating systems and a fully configurable network topology from remote locations has many useful applications. We have implemented the virtual network described here on a 1.8 GHz laptop with 1 GByte of RAM and a 30 GByte hard drive. We run 5 and 6 guest operating systems with out any significant latency in any of the guest systems or the host system.

Another area well suited for the VIAN is that of network protocol research. The ability to build networks and test the functionality of protocol research efforts in an isolated environment where extraneous network interference can be minimized is beneficial. As in the previous cases, the resources required to fully test a robust network protocol might be prohibitive in some cases. VMware currently supports [15]:

- Nine virtual Ethernet switches,
- Virtual Ethernet protocol support includes TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell NetWare, and Network File System
- Built-in NAT supports client software using TCP/IP, FTP, DNS, HTTP, Telnet, and NetLogon.

An additional area where the VIAN solution is currently used is research, development, and testing of IA tools. We are using the VIAN technology to examine actions initiated by several open source IA tools. As noted previously, the relative absence of background networks packet noise provides a very clear picture of what a given IA tool transmits from a system. Since several tools function over a network, this scenario provides many benefits. Additionally, the guest OS can be configured in any manner necessary and easily restored to its previous state. Finally, restricting the tool to function within a virtual network establishes a solid security perimeter, not allowing a malicious tool to corrupt the physical network. A subset of IA tools worth mentioning specifically is network and system logging. The benefits described here provide significant advantage toward logging protocol development.

V. FUTURE WORK

The key to implementing future work is to make incremental changes and learn from their lessons. We plan to follow this approach as we continue to refine and improve the VIAN so that we continue to provide a quality IA education to our students and sustained research work for the greater community.

One are of specific improvement is specific curriculum development to fully leverage the unparalleled advantages of the IWAR in-a-box. We are developing a series of courses that, at varied levels of material knowledge, provide specific lessons and hands-on experiments.
Another area under active development is constructing a deployable solution, including the defined curriculum along with the virtual environment.

VI. Conclusion

The IWAR lab began as a small experiment, but with continued visibility resulting from a high level of academic, commercial and government interest, the IWAR lab continues to grow. The justification for the lab is clear—in order to provide a quality Information Assurance education, the hands-on experiences acquired using the lab's networks cannot be replaced by PowerPoint presentations or simulations. Using the VIANsolution affords each student the full advantage of being able to touch every moving part in a robust network and suite of operating systems. This capability is not attainable in standard network laboratories.

Neither Rome nor an IWAR lab is built in a day. The influence that Rome had on Western civilization is well documented in history. The positive influence that the IWAR lab will have on the education of students and faculty at the United States Military Academy will provide a firm foundation for the future leaders of our country for years to come. These are the same individuals who will ultimately have to make critical decisions concerning the assurance of information.

REFERENCES

[1] J. Schafer, D. J. Ragsdale , J. R. Surdu, and C. A. Carver, "The IWAR range: a laboratory for undergraduate information assurance education," presented at Consortium for Computing in Small Colleges, Middlebury, Vermont, 2001.

[2] D. W. Welch, D. J. Ragsdale, and W. Schepens, "Training for Information Assurance," *IEEE Computer*, pp. 2-9, 2002.

[3] J. Garamone, "Capabilities, Strategy Must Converge to Face New Threats," http://www.defenselink.mil/news/Jun2001/n06222001_200106221.html, accessed on May 9, 2002.

[4] Department of Defense Report to Congress, "Network Centric Warfare," http://www.c3i.osd.mil/NCW/, accessed on April 23, 2002.

[5] J. Garamone, "Land Warrior Coming to a Grunt Near You," http://www.defenselink.mil/news/May2001/n05092001_200105094.html, accessed on April 15, 2002.

[6] G. Blackwell, "802.11's in the Army Now," http://www.80211-planet.com/columns/article/0,4000,1781_1000821,00.html, accessed on April 15, 2002.

[7] CERT/CC Advisory CA-2001-23, "Continued Threat of the "Code Red" Worm," http://www.cert.org/advisories/CA-2001-23.html, accessed on April 15, 2002.

[8] R. M. Felder, "Reaching the Second Tie--Learning and Teaching Styles in College Science Education," *Journal of College Science Teaching*, vol. 23, pp. 286-290, 1993.

[9] C. E. Kaucher and J. H. Saunders, "Building an information assurance laboratory for graduate-level education," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.

[10] M. Brakewood,"Question, D. J. Ragsdale", March 05, 2002.

[11] A. Yasinsac, J. Frazier, and M. Bogdanov, "Developing an Academic Security Laboratory," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.

[12] G. A. Francia and R. K. Smith, "The Design and Implementation of a Heterogeneous Computer Networking Laboratory," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.

[13] J. H. Saunders, "Simulation Approachs in Information Security Education," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.

[14] J. R. Surdu, J. M. D. Hill, D. J. Dodge, R. C., Lathrop, S.D. Ragsdale , and C. A. J. Carver, " Military Academy Attack/Defense Network Simulation," Advanced Simulation Technologies Conference (ASTC), Orlando, FL, March 2003.

[15] VMware, *VMware Workstation 3.0 User's Manual*, 2001.

[16] The Honeynet Project, *Know Your Enemy Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*. Boston: Addison-Wesley, 2002.