An Approach to Developing An Information Assurance Environment

By

Marion Bogdanov

Index

Acknowledgements

First, I'd like to thank Dr. Alec Yasinsac for giving me the opportunity to work on his security research team and in particular on this project and for spending invaluable time in critical moments of my master's career. The meetings really helped. I would like to thank my committee members Dr. Ernest McDuffie and Dr. Mike Burmester for being interested in my research topic. Next, I would like to thank Mr. David Gaitros for convincing me to enter the graduate program in the computer science track and for always being ready to give me advise. Also, I would like to thank the following faculty members that have influenced me one way or another: Dr. Whalley and Dr. Lui, for their invaluable care about my education and advise about my future, Dr. Baker, for giving me a second chance and great lessons on operating systems, Mr. Ken Baldauf, for taking the time to listen to my trials and tribulations, Dr. van Engelen, Dr. Yuan, Dr. Schwartz, Dr. Mascogni and Mr. Bauer. I would like to thank the system group, for allowing me to create a test bed environment for my project. I'd like to thank Damon Snyder for giving me the opportunity to work in the systems group. I'd like to also thank Mr. Sprague from whom I learned quite a bit about management. Thanks to the CS staff, in particular, Eleanor McNealy and Jennifer Reed, and all my friends with whom I've fought many battle at Momo's on Thursday!!! Finally, I'd like to thank my parents for supporting my decision to furthering my education.

Abstract

With the constant threats of denial of service attacks, intrusions and compromises of computer networks on the Internet, the need for information security education is in the highest demand these days. A laboratory environment in an accredited educational institution with world-renowned professors would be an ideal place to offer such education for future network and system administrators and information security enthusiasts. It doesn't stop there. The educational institution can have an impact in three different areas: education, research and outreach.

This project will provide a necessary baseline environment where students will be able to perform the research, gain the education and to lend their knowledge to the community through an outreach program.

1. Introduction

Is security on the mind of everyday Internet users? Do they know the risk they take when they connect on the Internet? I don't know the absolute answers to these questions but a source states that stolen credit card and bank account information, distributed denial of service attacks, and transmitting of viruses and worms on large business, government and personal computers and computer networks are every minute events on the Internet [13]. Statistics related to attacks are available on the following web site: http://aris.securityfocus.com.

Information technology is the driving force of today's economy, but is the information secure and how can it be made secure? In a recent interview, the famous Winn Schwartau on his latest book *Cybershock*, which can be summed up as a guide on how to protect oneself on the Internet, the author answered the following when asked why he wrote the book:

> "Tens of millions of Americans are diving onto the Internet and the vast majority have no clue of what they are getting themselves into. The Internet is a technical medium, which has evolved for day-to-day use by the average non-technical person. Trillions of dollars are moving across the Net. Privacy is being violated more then ever before. This book was written to give people the tools they need when they visit a very dangerous neighborhood."[1]

Part of the reasons for such conclusions is the education, or lack there of, about information technology, let alone security, our citizen have gained through the cyber era. Are they ready for the new era?

The focus of this project is two fold: 1) to create a functional laboratory network environment with the appropriate resources, which will serve as a focal point for members of different academic disciplines, government, and industry to carry out world-class research and to advance the practice and public awareness of information technology in security and assurance through research, education, and public service (outreach), 2) to provide a mechanism which will maintain the integrity of the original computer configuration.

2. Research, Education & Outreach

The Research, education and outreach programs in information security have to be supported by an environment where the necessary task of the programs can be performed. The next three sections describe how this goal can be accomplished in the three areas.

2.1 Research

An essential element of any major university or department is a strong research program. One of the hottest topics in computer science research today is information security. This university has taken great strides to provide a facility where students and faculty can conduct research in information security. SAIT laboratory has become a facility where practical security techniques can be exercised and experiments conducted in order to test theoretical ideas. Professors interested in information security have a laboratory where they will be able to test their researched information. There are already a wide variety of research projects ongoing in SAIT Laboratory

One example is a current US Army research project that is part of eleven-investigator team that studies problems of critical infrastructure protection. One of the teams, is a collaborative effort by two FSU professors who are going is to develop a case-based reasoning (CBR) system for network intrusion detection. Currently, a CBR system that replicates the functionality of the well-known Snort intrusion detection package is being devised. In addition, add-on modules such as SnortSnarf that interpret and summarize the Snort output data are going to be constructed. Once this is accomplished, the object will be to seek ways to build-in higher levels of intelligence, enabling more sophisticated and accurate alerting capabilities.

As another example, another ongoing project has a goal to extend the network monitoring and intrusion detection system described in [6]. Extensive research, programming and implementing the system has been conducted. Specifically, a knowledge-based intrusion detection system that identifies intrusions into security protocols has being implemented. That system is presently being extended to include a behavior-based capability that can detect even previously unknown attacks on executing protocols. It detects malicious and questionable activity by tracking and analyzing user and network behavior with respect to security protocols.

These research projects use the SAIT laboratory as a testing environment. A goal of this project is to allow research projects to be installed, analyzed and documented without having to put the Computer Science Department network in danger. Also, this process, which is discussed in section 3.2 of this paper, will not violate network and system administration policies that condemn modification of baseline computers.

With more existing projects in Information Hiding, Tracing and Watermarking, Intrusion Detection, Key Distribution, Key Escrow, Security Protocols, Survivable Computation, and Threshold Cryptography, the laboratory is on sound research footing. As the examples above demonstrate, the SAIT laboratory is an ideal place for the final product to be tested. The researchers will not have to worry about contaminating the configuration of the computers in such a laboratory because it is an environment that maintains the configuration of the original installation; one of the goals is to provide a facility in which security research projects can be safely conducted and advancement in the field of information security is enhanced.

2.2 Education

The computer science field, especially information security, has drawn a huge public interest in recent years. Individuals, governments and business corporations have a direct interest in information security because they are affected by it whenever they connect to the Internet. In order to have a constructive and beneficial impact on the personal, economic and national level, it is the job of educational institutions to provide services that will educate individuals, government and corporations about information security. The next few paragraphs describe how the SAIT laboratory can provide these services.

The educational functions of the SAIT Laboratory are focused on, undergraduate and graduate education. Within Florida State University, SAIT Laboratory coordinates graduate and undergraduate security and information assurance curriculum development, including theory and practice. The curriculum provides a strong foundation in security principles. Courses in information security in Computer Science at Florida State University satisfy the National Security Telecommunications and Information Systems Security (NSTISSC) training standard for Information Security Specialists. Courses such as Practical Security and Network and System Administration are excellent candidates to use SAIT laboratory's capabilities. The missing component is a rich library of tools.

In the Practical Security course, projects can be devised from the tools in the library. For example, a project's goal for a pair of students, working as a team, could be to successfully install an intrusion detection system (IDS) such as the network-based tool called Attacker. This will be followed by running vulnerabilities test on the machine with a Scanner tool, such as Typhon. The team will practice the techniques that they learn in the classroom and document details of their work.

Another application for the library of tools is the Network and System Administration course, a course designed with hands-on experience in mind. This course offers a hands-on component where teams of 2-3 people are formed. Each team has to install and maintain 3 computers with 3 different operating systems. Part of the course's curriculum is to focus on security of the computer and the network.

As a student of this class, during "security week", I was asked to find tools on the Internet that would allow us to secure our computers and also find tools which would allows us to break into or "hack" into other teams' computers. I conducted a personal survey, and found that 50% of the students where not aware of the type of the different types of tools that they could find to protect their machines, and 90% didn't know where to find "hacking" tools, let alone use them. A focus of this project is to provide students a baseline set of tools for use in classroom projects such as this.

With information security on the mind of everyone connected to the Internet, an educational institution that provides services that will educate individuals, government and corporations about information security is essential. The skills learned will provide better information security practices. Also, the education will create leaders who are capable of serving our governments and businesses for betterment of the nation and the economy. From the above examples a conclusion can be drawn that the SAIT laboratory type environment is an ideal facility for serving education to the public interested in applied research in information security technology.

2.3 Outreach

The SAIT Laboratory outreach program foster communication and promotes mutually beneficial relationships among members of the government, industry, and academic communities. Academic communities can specially benefit from collaboration with industry or government sponsors because the sponsors would be able to leverage existing resources, experiences, and relationships. By participating, the sponsors will gain access to the research and education laboratory. Participation will provide partner access to security experts, such as the professors or their research assistants, interaction with other center sponsors and early access to research findings. Sponsor Partnerships will enhance researcher access to modern equipment and professional resources in tune with marketplace needs.

An example where the current state of the SAIT laboratory can provide service is a corporate sponsor who is willing to have their network scanned for vulnerabilities. An ideal solution to meet the goal would be to use our library of tools to perform our tasks. A team of experts from our department can be sent to perform the vulnerability assessment. Once the assessment is performed, thorough report will be presented and proposal for consideration of future necessary services will be provided.   If the corporate sponsor is willing to cooperate with the proposal, a partnership program can be established, where they will provide the SAIT laboratory with new technologies, while the laboratory provides them with most current research, and security issues regarding their network services.

Along with the capabilities as a research and educational facility, a SAIT laboratory type environment also has the capability to be involved in an outreach program, which will generate benefits not only for the SAIT laboratory, but also for the corporate sponsors. Creating and maintaining a mutually beneficial relationship with corporate sponsors will enhance researcher access to modern equipment and professional resources in tune with marketplace needs. However, this laboratory isn't complete without a mechanism for creating a baseline of laboratory computer configurations.

3. SAIT Environment

In order to support Research, Education and Outreach, this project will equip SAIT Laboratory with an environment that facilitates use of the individual computers, protects the network, and provides a resource library of information security tools.

3.1 Background on SAIT

In 1999, the Computer Science Department of Florida State University decided to expand in the area of trusted systems. Upon the hiring of world-renown professors in the information security arena, the university modified its curriculum and started offering courses in computer and network security. These courses were certified by the National Security Telecommunications and Information Systems Security (NISTISSC) curriculum for Information Security Professionals and FSU became an institution in which certification for information security can be earned. As a result of this accomplishment, the National Security Agency (NSA) designated FSU as a center of excellence in Information Security Education. Accordingly, the College of Arts and Sciences from FSU dedicated $125,000 of equipment to start a laboratory.

The following equipment was purchased for the laboratory:

- 1 – Sun Microsystems Enterprise^{TM} 220R Server
- 1 – Cisco Catalyst 3500 Series XL Switch
- 1 – Sun Microsystems StorEdge^{TM} A1000
- 9 – Sun Microsystems Ultra 5 Workstations with Solaris 7 as an operating system and a PCI card with the Windows 2000 Professional operating system
- 5 – Tri-C Systems Custom Build PCs with Windows 2000 Professional as an operating system
- 4 – KVM Switches
- 1 – HP LaserJet 4100N Printer

For the purposes of this project, the switch and the workstation personal computers (PCs) were the most important hardware components. The significance of the switch is that it allows management of all Cisco switched ports from a single IP address. Accordingly, the lab can be segmented into several networks, which can accommodate PCs serving as routers to other PCs. This environment provides multiple simulations for the mentioned goals of the laboratory. The availability of PCs with Windows 2000 allowed focus on security tools for the Windows operating system. The tools, which provide hands-on experience for users, will be discussed in the next section. The illustration in Figure 1 represents the laboratory setup:

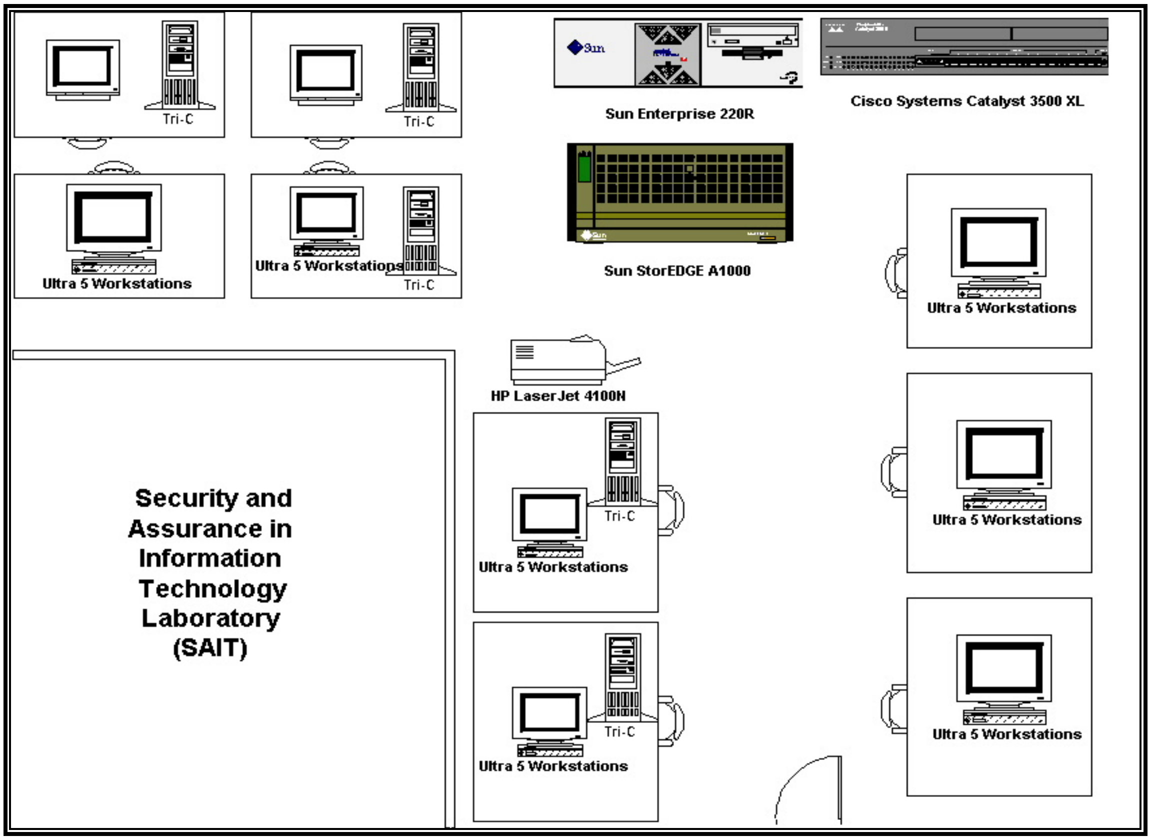


Figure 1

Maintaining security on the local area network (LAN) is an essential issue in the computer science department. On the computer science network, user accounts are served on a network file system (NFS). Since students and faculty need to perform research with administrative privileges on the PCs in the SAIT laboratory, the safest solution was to connect the lab on its own LAN. Therefore, the lab was created on a separate subnet on the Florida State University network. This will prevent any tampering with the NFS from the lab.

Another security issue involving the SAIT laboratory was allowing students permission to install software on the laboratory computers. From a security point of view, no user should have permissions that would compromise the computer that the user is using, since all computers have a baseline installation. Understandably, it was taken as a challenge to create an environment where users are able to make changes that will not compromise the used computer, yet provide administrative privileges as a desired functionality.

In summary, the goal of this project is to create a functional laboratory network environment, with baseline computers that retain original integrity, and appropriate resources dedicated to serve as a focal point for members of different academic disciplines, government, and industry. Laboratory users will be able to carry out world-class research and advance the practice and public awareness of information technology security and assurance through research, education, and public service or outreach. The SAIT Laboratory is dedicated to the synthesis of research, education and public service through the combined focus on theory and application of information security techniques. It provides facilities that are used for research and graduate level teaching in security and information assurance and allows security projects that are not safe to conduct using the regular campus computing facilities [5].

4.0 The User Environment

The first goal of this project was to provide a baseline mechanism that will maintain the integrity of the original computer configurations for a general-purpose laboratory. This task is a key component in creating the SAIT laboratory. The idea is unique by extending the user privilege by granting users permission to install and remove software. Many security software tools require administrative permission to carry out the installation process and to use the software. The installation process modifies the configuration of the host computer, which may create real security vulnerability. The desired outcome is to refrain users from making configuration changes.

Controlling computer configuration is essential to maintaining the integrity of a computer. Once the baseline configuration is compromised the computer might be vulnerable to security attacks. Compromised computers are invalid research tools because the alterations can cause invalid or inaccurate data.

Additionally, introducing new software can have a negative effect on the computer's performance and configuration. Once a machine has been setup properly, the ideal procedure is to restrict non-administrative users from changing the configuration of that machine. Establishing and controlling a baseline configuration is a difficult task. We considered three methods to solving this problem; two software solutions and a third based on creation of a complete image of a computer's hard drive.

4.1 Cloning

Cloning is a process where one computer's hard disk is used as an image and it's copied over to as many computers as desirable. The problems with this concept were the following:

1. Network malfunction
2. Process too time consuming
3. Update of computers
4. How often to update?
5. Hard-drive wear and tear.

Network cloning can be unpredictable because many variables are involved in correct function of the network. Network downtime is a risk that this lab should not have to take because research productivity levels will suffer. Also, if network cloning is considered, a decision about cloning the machine needs to be determined. This process will inconvenience users since they have to compromise lab usage with cloning time. Non-network cloning allows only one machine to copy an image from another machine. This process takes too much time, which is not feasible. And finally, hard-drive wear and tear shortens the lifetime of the hard-drive, causing the lab equipment to diminish rapidly.

4.2 Deep Freeze

Deep Freeze is proprietary software with a concept to prevent configuration file changes to a computer. Its functionality is amplified by "freezing" the configuration file [7]. Appropriate users are allowed to make changes, such as installation, to the machine while the software is in "freeze" mode. This is a great software product, which contains the necessary functionality for the purposes of creating a laboratory environment with the goals that were mention above. Unfortunately, Deep Freeze is only available for Windows 95, 98 and Me, which have file allocation table (FAT32) type structure. The laboratory computers are installed with Windows 2000 professional operating system, which supports the new technology file system (NTFS); therefore, Deep Freeze software is incompatible.

The shortcomings to this concept and Deep Freeze led to choosing the VMWare as an option that best suits the goals for this lab.

4.1 VMWare

VMWare is proprietary software that will aid in maintaining the computer configuration. It provides virtualization layer that turns the physical computer into a logical pool of resources. These resources can be allocated to any application or an operating system.

VMWare is installed as another operating system, called a guest, on top of the host operating system. The host operating system is the system that supports the VMWare's guest operating system. More about the details of the installation of VMWare can be found in Appendix A. The final outcome is an environment that grants administrative privileges on the guest operating system. The user will have permissions to install any software on the machine. See Appendix B for more detailed explanation about using VMWare. Installing software requires changes to the configuration files of the machine; therefore, with administrative privilege, the user is able to do just that. However, this configuration file is not the file of the host computer; therefore, VMWare accomplishes the maintenance of host's configuration file, which is the desired goal.

5.0 Establishing a Library of Security Tools

Since the operating system on the SAIT's lab PCs is Win2000, windows security tools are essential elements of SAIT's goal to carry out the research, education, and outreach programs.

5.1 Selection of Tools and Download Procedure

Over eighty security tools for the Windows 2000 operating system have been researched. Since hacker sites have been known for providing worms and viruses with their software and acquiring IP addresses for later DoS/DDoS attacks, regarding them as legitimate download sites was not reasonable. Instead, a leading provider of security intelligence services for business, www.securityfocus.com, was chosen as the primary website for the tools. The website lists many software, which are linked to their home websites. The tools were downloaded, scanned for viruses, installed, analyzed, documented and categorized by functionality. The tools were installed on the Windows 2000 Professional operating system, which is the operating system for all of the Tri-C computers in SAIT Laboratory. The documentation on each tool is in either a text format, Microsoft Word 2000 Document format or a Microsoft PowerPoint 2000 format, and it specifies the following metrics:

- Date of download
- Location of download
- Size of download file
- Description and functionality of the tool
- Whether the tool is shareware or freeware
- Various screenshots of the tool (if applicable)

The described format will allow user to identify and use the tools and will facilitate maintainability of the database of tools. Each metric specifies its function that provides the user with knowledge about the software. Once the each tool was researched, it was placed in the proper category of tools, a tree-structured directory, which is described in the next section.

5.2 Procedures for creating the Library of Tools

The most challenging task while analyzing these tools was categorizing the tools. It’s important to have categories of tools because it allows the user to make clear choices when it’s necessary to perform the three programs supported by the SAIT lab. One categorization method supports a broad organization by having three major categories that contain many different tools, such as the list in Table 1 [2]. This method exemplifies high-level of abstraction.

General Organization of Security Tools
• Intrusion Detections Systems (IDS)
• Vulnerability Assessment Tools
• Miscellaneous

Table 1

Another categorization method, which is introduced by the leading provider for security intelligence services www.securityfocus.com, supports an organization that has a lower level of abstraction by separating tools in specific categories by specific functionality, such as the list in Table 2 [3].

Specific Organization of Security Tools

- Network Utilities
- Policy Enforcement
- Programming
- Recovery
- Replacement
- Secure Deletion
- Sniffers
- System Security Management
- Utilities
- Access Control
- Auditing
- Authentication
- Cryptography
- Hardening
- Hostile Code
- Intrusion Detection
- Network Monitoring

Table 2

The process of creating categories of tools was based on software application, functionality, description and previous research, such as Tables 1 and 2. After evaluating the software, each criterion was considered and categories were created. The abstraction level intended is in the middle of [2] and [3]. For example, www.securityfocus.com provides tools for each of its category. Some software tools, such as intrusion detection, network monitors, and sniffers, have similar functionalities. After evaluating tools from these categories, it was clear that these tools could be included in a super-category called intrusion detection systems. The Table 3 lists the scheme used in SAIT lab, which is a combination of the Tables 1 and 2:

Windows Security Tools

- Anti-virus
- Firewalls
- Intrusion Detections Systems (IDS)
    - Host-based
    - Net-based
    - Hybrid
    - Forensic Tools
    - Sniffers
- Vulnerability Assessment Tools
    - Front End
    - Hardening
    - Scanners
- Miscellaneous

Table 3

The next several sections describe each category of tools available in the library of the SAIT Laboratory. Also, from each category and sub-category an example of one tool is presented. Since many tools possess great functionalities, but are difficult to configure and install, user-friendliest was chosen as the major criterion.

5.3 The Library of Tools

5.3.1 Anti-Virus Tools

The function of anti-virus tools is to scan files for specific code that matches a database of known virus code. The library contains fourteen different anti-virus software tools listed in the Table 4:

Anti-Virus Tools

- PCDoorGuard
- RetinaCodeRed
- RetinaNimda
- ServerMailReader
- TrojanDetectionSuite
- VirusStriker
- WormGuard
- Anti-Trojan
- IRClean
- MailDefense
- McAfeeVirusScan
- McAfeeVirusScanProfessional
- PandaPlatinum
- PandaTitanium

Table 4

McAfee Virus Scan Professional is the most complete tool. It provides an effective GUI and a broad functionality. Its management console provides the user with a list of tasks to choose. Some of the tasks are: ability to scan the computer for viruses, ability to change the settings, allow managing the quarantined files and view virus scan log activities and the ability to update new virus signature files. This tool can be used in the research and education program where it can be applied to perform disk scanning and cleaning of the system in question.

This software comes in a package that contains a firewall and can be used to setup a firewall on a machine as well. The negative aspect of this tool is that it is proprietary software. Its evaluation version has 30-day trail period.

In an outreach practice, it's desired to have freeware that makes the least amount of configurations to the system in question. Anti-virus software with this ability is IRClean. It's an executable file that checks the desired directory for viruses. It allows management of quarantined files as the proprietary McAfee. The shortcomings of this tool are the slow of software support and the lack of capability to update a virus signature files.

5.3.2 Firewalls

Firewalls are devices that are placed between a network to be protected and another network. Firewalls only allow certain network connections of a desirable nature through, while keeping dangerous ones out, protecting the systems behind it from intruders. The process of traffic regulation that is performed via application gateways or proxies is referred to as filtering [9]. There are many software products that are available to accomplish filtering. In the SAIT laboratory's library of tools there are eleven different firewalls, which are listed in Table 5:

Firewall Tools

- BlackICE
- CHX-I
- ESafe
- GNATBoxLight
- McAfee Firewall
- SecureIIS
- Sygate Personal Firewall
- Symantec Desktop Firewall
- Tiny Personal Firewall
- Virus MD
- Zone Alarm

Table 5

GNATBoxLight is a demonstration version that allows usage of 2 IP sources from a protected network to outbound traffic. It provides a configuration control environment where the user can chose to configure services for a DNS Server, Mail Proxy Server, and Virtual Private Networks (VPNs). This tool provides excellent hands-on experience for setting up firewalls with various services, which are invaluable to someone who desired to receive education about firewalls.

Zone alarm stands out as the best tool. Some of its features are GUI, customizable security levels, password protection, Enhanced MailSafe-Email Attachment Protection, Local and Internet Zones. To understand some of the features, the next few sentences describe their functionalities. Its customizable security levels allow creation of security settings to uniquely desired requirements connecting to the corporate LAN from home, using streaming media or sharing files over the Internet. The password protection ensures the security settings are tamper-proof. The Enhanced MailSafe-Email Attachment Protection stops email-borne viruses. Zone Alarm Pro compliments anti-virus software programs by providing immediate defense against unknown threats, including those that haven't been profiled yet by intrusion detection and virus protection vendors. Local and Internet Zones allow easy expansion of the local network to include VPN servers or advanced Internet services, such as Internet phone calling and remote storage. This tool will aid in the areas of research, education and outreach. It allows users to experiment with different levels of network filtering and teaches different filtering techniques that can be applied to systems in an outreach program.

5.3.3 Intrusion Detection Systems

Intrusion detection systems (IDS) form a small but critical piece of the computer security jigsaw, alerting to intrusions and attacks aimed at computers or networks [8]. They're not a computer security panacea; they do not even prevent attacks. Nonetheless, they are essential in knowing whether the system is under attack. This category deserved extra attention because within IDS there are sub-categories such as network-based systems, host-based systems, forensic systems and hybrid systems.

5.3.3.1 Network-Based System

Network-based systems monitor all network traffic passing on the segment where the software is installed, reacting to any anomaly or signature based suspicious activity. Basically, this is a packet sniffer with attitude [4]. They analyze every packet for attack signatures and some will block suspicious packets. But using this facility is fraught with danger because a hacker could cause two networks to shun each other by spoofing the other networks IP address within an attack. Table 6 lists the Network-based IDS tools:

Net-Based IDS Tools
• Aports
• Attacker
• eTrustIntrusionDetection
• NetMonitors
• NetProwler
• TraceDET

Table 6

The most complete tool from the group above is eTrust Intrusion Detection. It has many useful features. One feature allows administrators to check users web usage log file, which can monitor if users are visiting work related sites. Another similar feature allows viewing of web, telnet, file transfer protocol (FTP), and POP mail traffic activity for productive work. Another feature generates easy-to-read management and detail reports. Extremely useful feature is the ability of the software to send messages via e-mail or fax to the administrator. These messages range from about predefined intrusions and suspicious network activity, to malicious Java and ActiveX applets, to viruses entering the network.

The drawback from this tool is that it has too many features. It can be a tedious task for someone to learn all the available features that can be used on this software. Given the right amount of time, an individual should be able to learn all the functionalities of this tool. Another drawback is that it is a shareware product with a 30-day trail period. Even with its drawbacks, this tool will aid in the areas of research and education where information is learned about IDS from a hands-on approach by installing the software, which is a rigorous process that provides tutelage.

5.3.3.2 Host-Based Systems

The host-based IDS monitor event logs from multiple sources for suspicious activity. Host IDS are best placed to detect computer misuse from trusted insiders and those who have infiltrated the network. There is an added benefit to host-based IDS, because they operate at near real time and as a result system faults are often detected quickly. The concept makes them popular with security personnel such as system administrators [4]. Table 7, lists the available host-based IDS tools in the library:

Host-Based IDS Tools
• Archaeo
• AWPTA
• FileWatch
• FPort
• LANGuardInegrityCheck
• LANGuardSELM
• McAfee Internet Security
• System Analyzer

Table 7

McAfee Internet Security, a shareware with a 30-day trial period, has the most effective detection features. The enhanced intrusion detections allow web bug detections and filtering. The stealth detection provides an extra level of defense in privacy protection. It uses a security check that can alert users to possible security threats posed by key loggers or other stealth programs. This tool also provides a firewall and a virus scan as added features. As an added layer of protection for data, a feature called File Guardian secures files, folders, and drives from prying eyes at the subject machine or even across the Net. An educational benefit from using this tool is the experience configuring its features. Additionally, the configuration of many of the features is rather easy because it provides excellent documentation.

5.3.3.3 Hybrid Tools

Hybrid IDS tools are taking delegation of IDS to host one stage further, combining Network based IDS and Host IDS in a single package. This solution gives maximum coverage and consideration should be given to the amount of data and cost in question. Many networks reserve hybrid IDS for critical servers. All encountered hybrid tools in this research were proprietary. For this reason, the SAIT Library of Tools does not contain these tools for the Windows operating systems servers. This is an area that could be researched more in the future.

5.3.3.4 Forensics Tools

Another subcategory of IDS is forensics tools. Computer Forensics tools are used in investigations of computer-related crimes [10]. This subcategory consists of miscellaneous software that doesn’t belong to either of the three categories mentioned so far, but the implication of the software in these categories deals with reporting to ARIS, which is described in the next paragraph, and checking last-time modification of files, which are types of intrusion detection tools. The Table 8 lists the tools that are found in SAIT laboratory's library under this subcategory:

Forensic Tools
• ARIS
• BinText
• Foresics Tool Kit
• FPort
• NTLast

Table 8

The most significant tool from the list above is ARIS. ARIS (Attack Registry and Intelligence Service (ARIS) extractor is a new database designed to aid IDS users in effective Incident Detection and Incident Handling. This tool is helpful in the area of research because ARIS and its Extractor and Analyzer components will provide a powerful means of accurately identifying and effectively responding to network attacks on an ongoing, real-time basis. It functions by extracting, storing, analyzing and comparing data supplied by the security community and home users alike. The drawback to ARIS is that it needs BlackICE, which is proprietary software, in order to be useful. Fortunately, SAIT's library contains BlackICE, but only for a 30-day trail period.

5.3.3.5 Sniffers

The last subcategory of tools under IDS is the sniffers. The function of sniffers is to capture packets that are sent on the network wire. Also known as network analyzers, sniffers are used for monitoring network traffic [11]. As such, if used by authorized personnel, can prove to be of a great value. But, on the other hand, sniffers represent significant threat to your network, and are very hard to detect. The SAIT laboratory's library contain the following sniffers that are listed in Table 9:

Sniffer Tools
• Analyzer
• Ethereal
• IDSCenter
• Snort
• Windump

Table 9

Ethereal, which is a network protocol analyzer for Unix and Windows that allows examination of data from a live network or from a capture file from disk, is a tool that stood out from the rest of the list. The ease-of-use and the GUI provided excellent review for this software. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. Users are able to interactively browse the captured data, viewing summary and detail information for each packet. Besides the functionality, what makes this tool so appealing is that it's free.

In the area of education, Ethereal can be used to educate students on how to become solid system administrators in the Network and System Administration course. By utilizing this network analyzer system administrators can solve the problems of load imbalance of their respective networks. Ethereal can be used for an outreach program where a sponsor may need to solve similar issues. To summarize, in respect to research, education and outreach, this tool is an asset to the SAIT library of tools.

5.3.5 Vulnerability Assessment Tools

The category Vulnerability Assessment Tools contains three subcategories: hardening, scanners and front-end tools.

5.3.5.1 Hardening

Hardening is a term used for securing a network, a server or a workstation. The hardening subcategory contains one software tool strictly for Windows NT. Primary utilization of this tool is in the area of outreach were sponsors have failed to meet the requirements of securing their Windows NT server. Windows 2000 operating system is much more secure than its predecessor Windows NT; therefore, hardening tools for Windows 2000 were not found in this research.

5.3.5.2 Scanners

Scanners are among the most widely used tools by network and systems administrators. The functionality of these tools is to look at the hosts' operating system and applications for vulnerabilities that could be exploited and checks them against the system security policy for non-compliance [12]. They also advise the user about what vulnerabilities may exist on a system, and some tools may even allow the user to fix the vulnerabilities. There are fourteen scanners available in the SAIT laboratory's library. Table 10 lists the scanners:

Scanner Tools
• AWSPS
• BackOrificeServer
• BOPing
• DDoSPing
• Fscan
• InternetScanner
• LANGuardScanner
• NetBrute
• NmapNT
• SuperScan
• Trout
• Typhon
• URLScan
• Vision

Table 10

The user-friendliest and most feature-filled tool is SuperScan. SuperScan is a powerful connection-based TCP port scanner, pinger and hostname resolver. Its multithreaded and asynchronous techniques make this program extremely fast and versatile. Perform ping scans and port scans using any IP range are made possible. This specific feature is unique to this tool in respect to the library of SAIT security tools. It uses a text file to extract addresses and scans any port range from a built-in list or any given range. It allows the user to view responses from connected hosts and the user can modify the port list and port descriptions using the built in editor. In addition it merge port lists to build new ones and allows connection to any discovered open port using user-specified "helper" applications. A user can assign a custom helper application to any port and save the scan list to a text file. A user-friendly interface compliments the comprehensive help file. Besides the great functionality, what makes this tool so appealing is that it’s free.

Primary Super Scan usage is in an outreach program to help assess the partner’s network for vulnerabilities. The usage of scanners can be applied to the classroom as well as research. Courses such as Network & System Administration prepare students to become well prepared system administrators. Learning to use scanners as an essential part of system administration while preparing and hardening a system. Also in research, students will be able to test different scanning strategies that provide useful solutions to securing systems more efficiently.

5.3.5.3 Front-End Tools

The last subcategory of vulnerability assessment tools, the front-end tools, is a package of tools available in one software bundle. These tools have multipurpose functionality. The SAIT laboratory’s library has three of these tools, which are listed in the Table 11:

Front-End Tools
• ANT
• NetScanTools
• PCSNetworkTools

Table 11

NetScanTools is multi-functional and easy to use software, which has a great GUI to go along with its feature. It provides some of the following features: ping, traceroute, whois, netscan, finger, quote, time, port probe, name server lookup, etc. A user has full control of the features much like SuperScan, the tool mentioned earlier, with the exception of having more tools available in one package.

5.3.6 Miscellaneous Tools

The last category of tools is the miscellaneous tools. This category was a result from evaluating software that was not meeting the criteria mentioned in section 5.2. Since these tools have dependable and effective functionality, they were not overlooked. Accordingly, the tools were placed in a separate category. There are seven tools in the SAIT laboratory's library listed in Table 12:

Miscellaneous Tools
• Diamond • Fpipe • KeyBoardIntercept • LibNetNT • MindTerm • PandaSecurity • RegistryProt

Table 12

Each of these tools has a great feature. For example, MindTerm is a Java written alternative to Secure Shell (SSH). Utilization of this tool is in the outreach program by providing sponsors with a tool for secure network communication. Since the source code is available, this tool can be used as a reference for developing more efficient communication software that provides security, which pertains to the education and research program. PandaSecurity restricts the use of computers to specific users in specific time frames. It also prevents the installation of inappropriate software. Finally, Key Board Interceptor monitors program that allow interception of all keystrokes, mouse clicks, captions of active windows, static text and other. The unique set of features that make it suitable for perfect monitoring of user's computer activity. A system administrator of sponsor organization is a likely candidate to have affinity for such a tool.

Performing the above task was one of the two major components of my project. The library of tools is an essential aspect of the SAIT laboratory. These tools can be used in the three programs, research, education and outreach, that SAIT laboratory's plans to support. In the research program, it will allow students and faculty to experience the use of different types of software. They can install, analyze, benchmark and document the different tools to their specific criteria. In the education program, the tools will allow students and faculty to learn about the different categories of tools and how they are applied in practice. And finally in the outreach program, the tools will be essential in conducting network or system assessments for the outreach partners, as it was described in section 2.3 of this paper.

6.0 Conclusion

A functional laboratory network environment was developed with baseline computer configuration that retains original integrity. The library of Windows security tools as appropriate resources dedicated to serve as a focal point for members of different academic disciplines, government, and industry was developed as well. These two goals result in the ability to carry out world-class research and to advance the practice and public awareness of information technology security assurance. In addition, the resulting product will be able to serve the following desired programs: research, education, and public service or outreach. This research can serve as a template for other educational institutions that have a desire to engage in the three programs that SAIT laboratory has interest in offering.

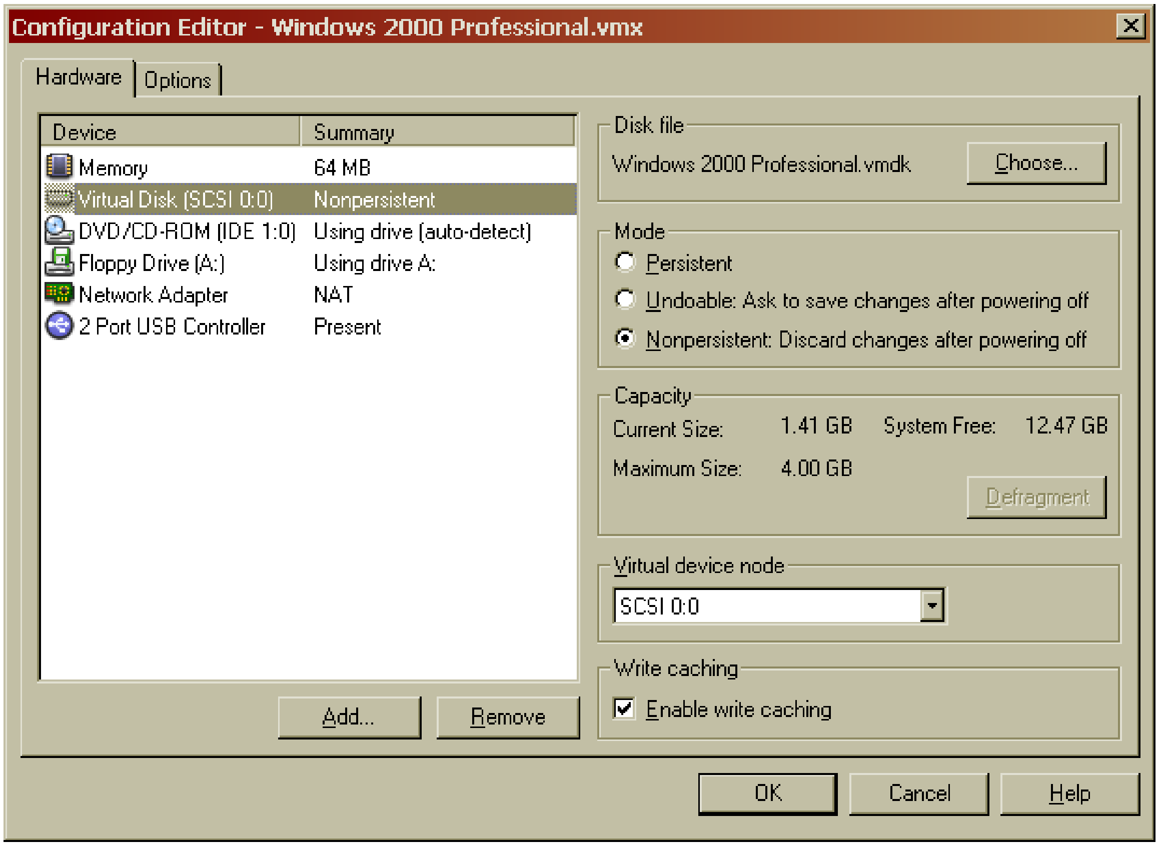
Appendix A.

Procedures for Configuring VMWare in the SAIT Laboratory

With administrative privileges on the host, installation of the VMWare 3.0 on each of the Tri-C computers was performed. Each computer has a virtual machine in which the students or faculty can log in and perform their desired research and education. By following a basic network administration procedure, creation of a baseline configuration for the virtual machine was accomplished, which can be modified only by administrator of the network:

- The hardware configurations are as follows:
  - 176 MB RAM (maximum for computers with 256 MB of RAM)
  - 4.0 GB Virtual Disk, which is much more then necessary, is a disk file set at non-persistent state, which discards ALL changes made to the virtual disk during a user session, which lasts from the time the user starts until the user stops the virtual machine.
  - DVD-CD ROM
  - Floppy Disk
  - Network Adapter NAT used to share the host's IP address. This appears as though the host and the guest are not use the same IP address, but in reality if ipconfig is performed in MS_DOS on the host and the guest, different IP addresses are assigned respectively. If the guest is looked up by name by nslookup, it will show the IP address of the host.
  - 2 Port USB Controller

The following is a screenshot of the configuration:



Device	Summary
Memory	64 MB
Virtual Disk (SCSI 0:0)	Nonpersistent
DVD/CD-ROM (IDE 1:0)	Using drive (auto-detect)
Floppy Drive (A:)	Using drive A:
Network Adapter	NAT
2 Port USB Controller	Present

Disk file
Windows 2000 Professional.vmdk

Mode
○ Persistent
○ Undoable: Ask to save changes after powering off
● Nonpersistent: Discard changes after powering off

Capacity
Current Size: 1.41 GB System Free: 12.47 GB
Maximum Size: 4.00 GB

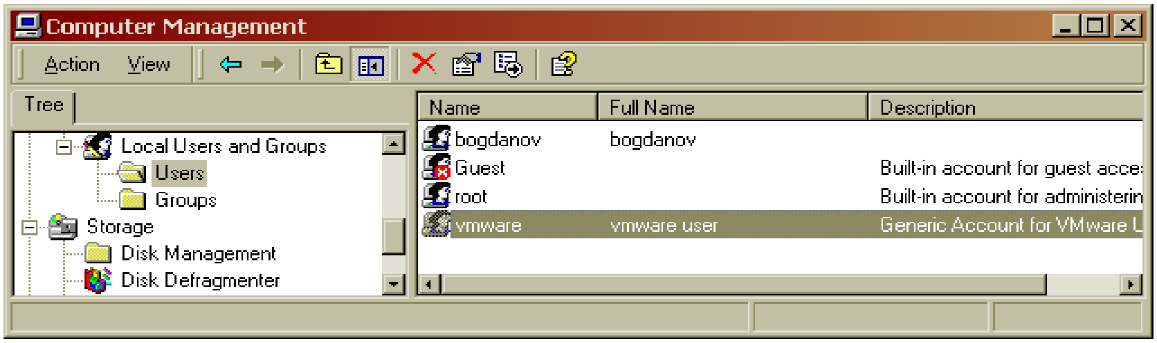
Virtual device node
SCSI 0:0

Write caching
☑ Enable write caching

- The software provided:
    - Windows 2000 Professional Edition with the latest service packs as an Operating System
    - Microsoft Office 2000 Professional
    - Adobe Reader 5.0
    - Secure Shell 2.2.0
    - Internet Explorer 6.0
    - WinZip 8.0

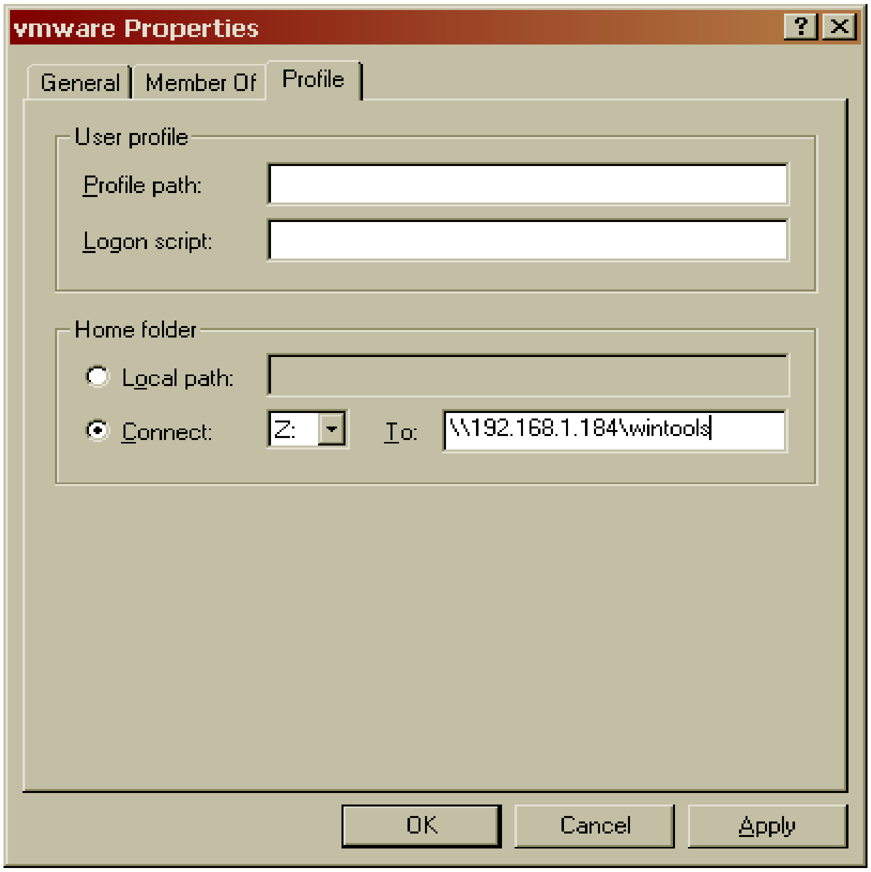
Next, the library of tools was placed on each host computer. The reason the library was not loaded on the server is for unpredicted network failures that will prevent the students and faculty from using the tools. Next, the library of tools was shared under the appropriate directory name WinTools. The properties of WinTools are read-only for everyone. This prevents users from modifying any content in the WinTools directory.

In addition, a generic account on the guest operating system (the virtual machine) that will allow users to login into the virtual machine with a generic username and password was created. The reason for the choice to have a generic username and password was to avoid redundancy, which will create more work for the system administrators. A user has to login to the host operating system with their unique username and password. Why create an account for each user on each virtual machine? It's not necessary. A generic account for the guest operating system will also allow portability. A user can login to any machine in the SAIT laboratory network, and then start up and login to the guest operating system. Therefore, the generic account name is vmware and the password is 123. Here is a quick screenshot:



Name	Full Name	Description
bogdanov	bogdanov	
Guest		Built-in account for guest acce
root		Built-in account for administerin
vmware	vmware user	Generic Account for VMware U

The account possesses the following properties:



User profile

Profile path:

Logon script:

Home folder

○ Local path:

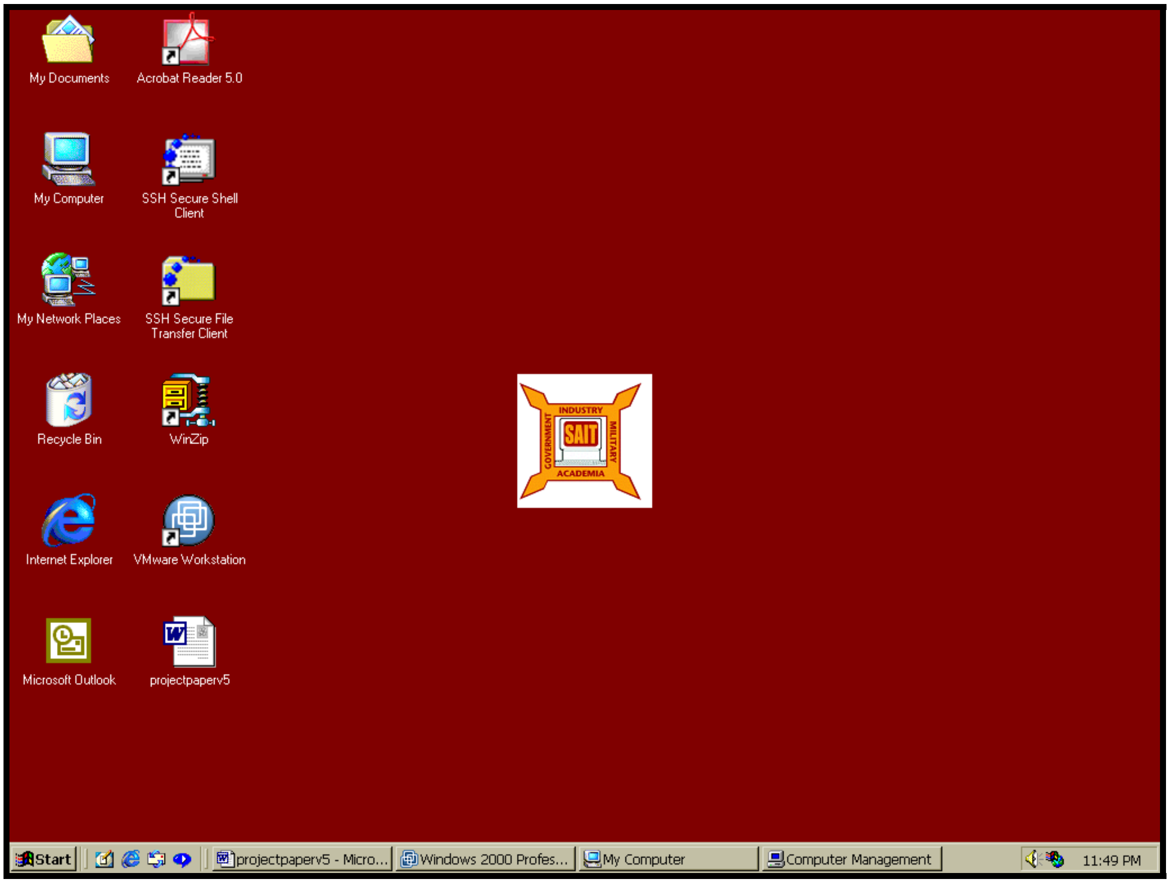
● Connect: Z: To: \\192.168.1.184\wintools

The significance, in the screenshot above, is the mapping of the shared directory from the guest operating system to the host operating system (IP address 192.168.1.184), which contains the WinTools directory. This concludes the procedures for configuring VMWare in the SAIT Laboratory.

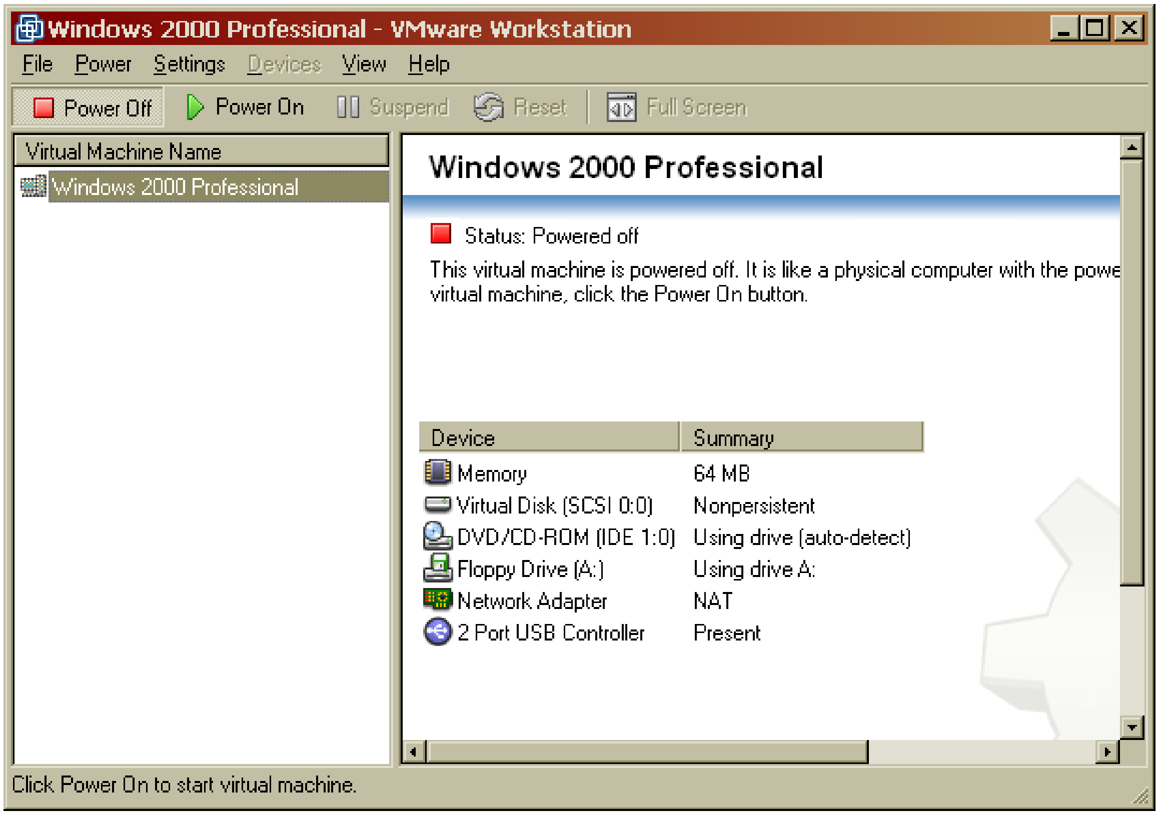
Appendix B.

VMWare functionality

In this section describes the proper procedure that lead to desired functionality of the guest operating system. First, the user will login to the SAIT laboratory domain through any Tri-C computer with their unique username provided by the system administrator and their unique self-created password. The user desktop environment will look like the screenshot below:



From this point onwards, the user will double click on the VMWare Workstation icon, which will prompt the user to choose a virtual machine. There is only one virtual machine installed on each Tri-C computer in the SAIT laboratory, therefore the choice is obvious. Below there is a screenshot of this description:



Windows 2000 Professional

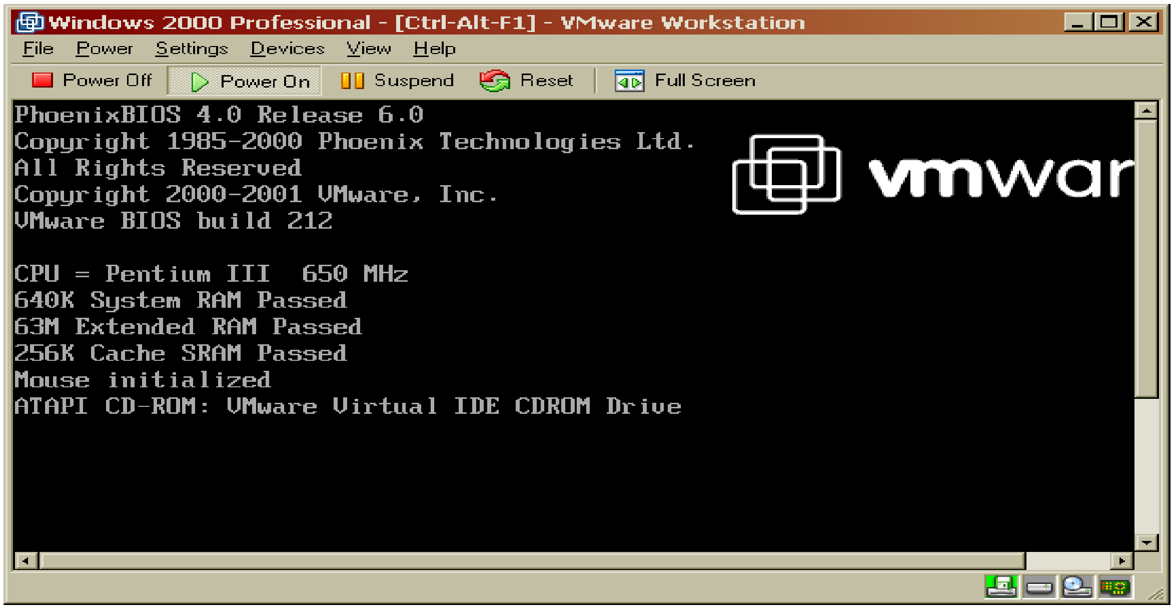
🟥 Status: Powered off

This virtual machine is powered off. It is like a physical computer with the powe
virtual machine, click the Power On button.

Device	Summary
Memory	64 MB
Virtual Disk (SCSI 0:0)	Nonpersistent
DVD/CD-ROM (IDE 1:0)	Using drive (auto-detect)
Floppy Drive (A:)	Using drive A:
Network Adapter	NAT
2 Port USB Controller	Present

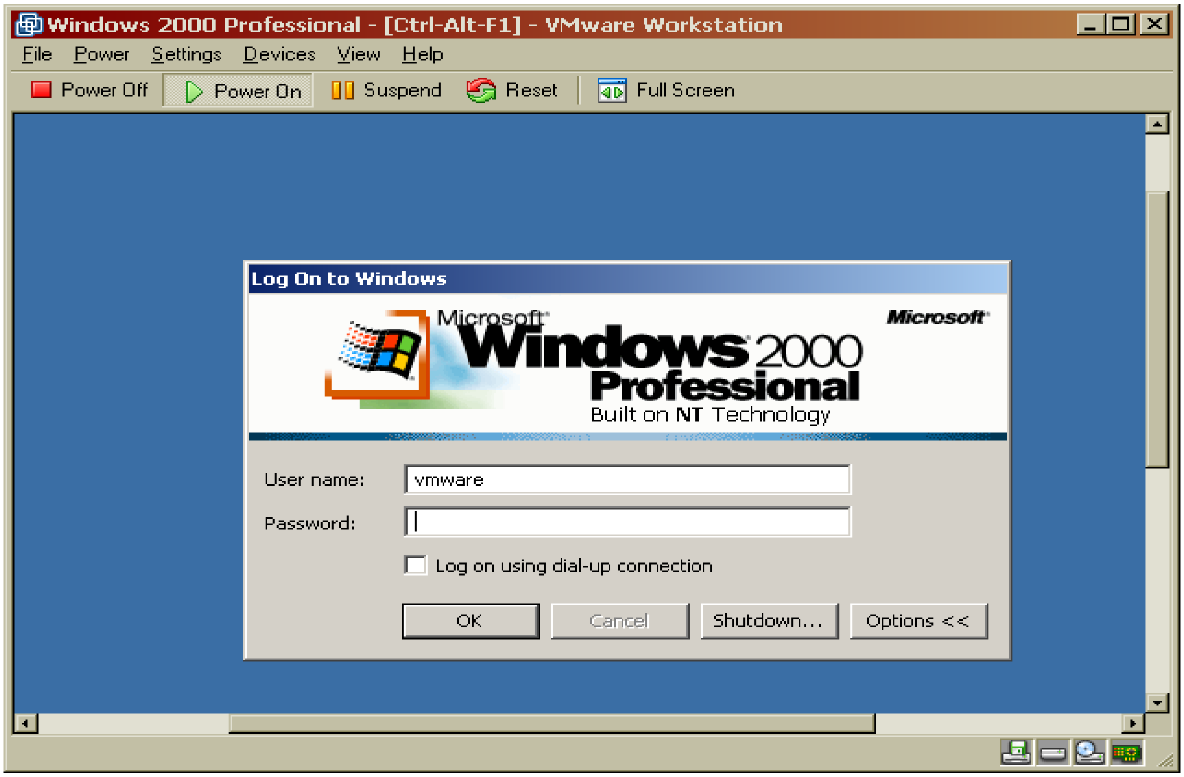
Click Power On to start virtual machine.

Once the user chooses the Windows 2000 Professional as a virtual machine name, the guest operating system will start as show on the next 3 screenshots:


Windows 2000 Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
vmwar

```
PhoenixBIOS 4.0 Release 6.0
Copyright 1985-2000 Phoenix Technologies Ltd.
All Rights Reserved
Copyright 2000-2001 VMware, Inc.
VMware BIOS build 212

CPU = Pentium III  650 MHz
640K System RAM Passed
63M Extended RAM Passed
256K Cache SRAM Passed
Mouse initialized
ATAPI CD-ROM: VMware Virtual IDE CDROM Drive
```


Windows 2000 Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
Log On to Windows
Microsoft Windows 2000 Professional
Built on NT Technology
Microsoft
OK
Cancel
Shutdown...
Options <<

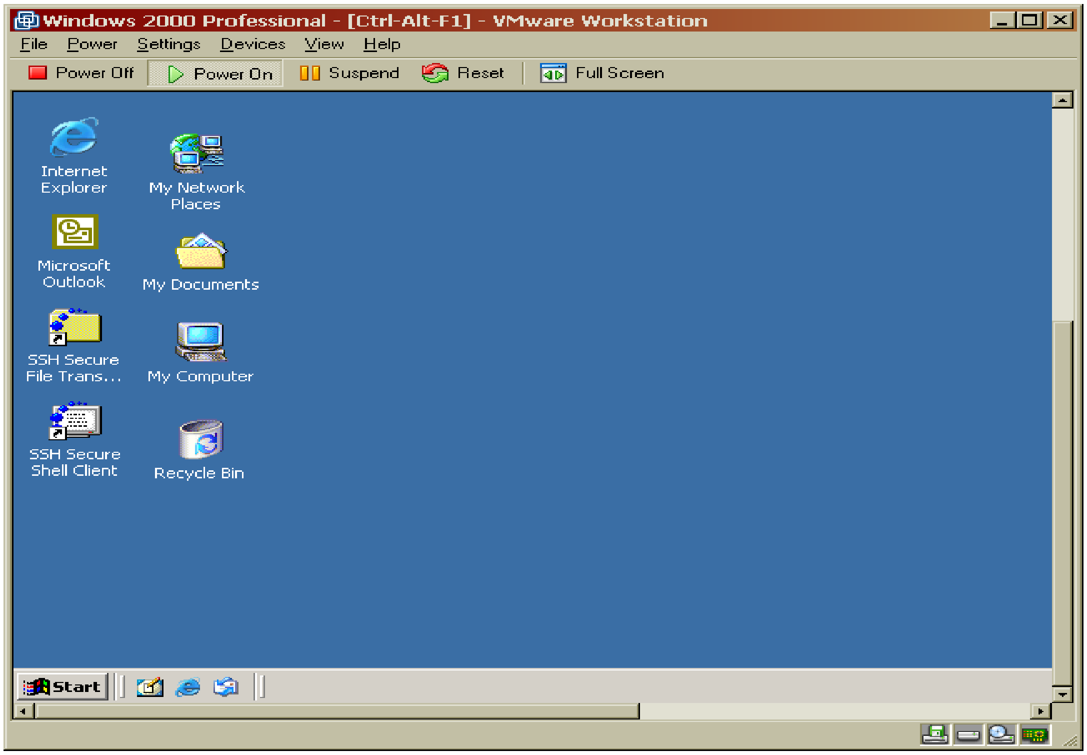
User name: vmware

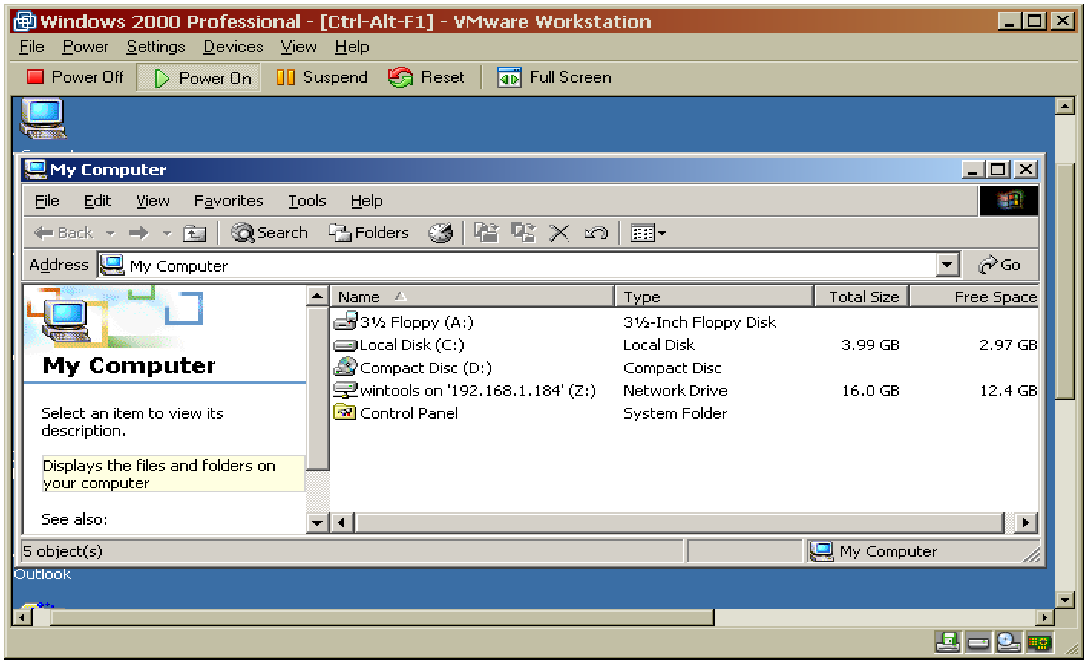
Password:

□ Log on using dial-up connection

The user is ready to login with the generic account vmware and the generic password 123. The desktop for the vmware user will look something like the two screenshots below. The first screenshot is a plain desktop, followed by the desktop with the directory

“My Computer” opened. This confirms the vmware user of having the access to the WinTools.




Windows 2000 Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
My Computer
File Edit View Favorites Tools Help
Back
Search
Folders
Address
My Computer
Go
My Computer
Outlook

My Computer

Select an item to view its description.

Displays the files and folders on your computer

See also:

Name	Type	Total Size	Free Space
3½ Floppy (A:)	3½-Inch Floppy Disk		
Local Disk (C:)	Local Disk	3.99 GB	2.97 GB
Compact Disc (D:)	Compact Disc		
wintools on '192.168.1.184' (Z:)	Network Drive	16.0 GB	12.4 GB
Control Panel	System Folder		

5 object(s)

Next, the user will be able to perform any educational research because they will have the ability to download, install, configure, and analyze any software in the library and beyond. The key is that once the user shuts down the guest operating system (the virtual machine), or logs off the host operating system, the information contained on the guest operating system will be completely wiped off. Therefore, this mechanism provides the user with an environment, which doesn’t change the original configuration on the host computer.

Bibliography

[1] “Cybershock: An Interview with Winn Schwartau”, Kelley Walker, http://www.interpactinc.com/interview.html, Dec 2001.

[2] “Talisker’s Network Security Tools”, Talisker http://www.networkintrusion.co.uk/index.htm, Dec 2001.

[3] Tools - a leading provider of security intelligence services for business, http://www.securityfocus.com/tools, Dec 2001.

[4] “Intrusion Detection Systems”, Talisker, http://www.networkintrusion.co.uk/ids.htm, Dec 2001.

[5] “SAIT”, SAIT Laboratory Home Page, Computer Science Department, Florida State University, Ted Baker and Ivo Desmedt Directors, http://www.sait.fsu.edu, Dec 2001

[6] "Active Protection of Trusted Security Services", Alec Yasinsac, Department of Computer Science, Florida State University, Jan 2000.

[7] Benefits of Using Deep Freeze Copyright 2001 Faronics Technologies, Inc. and/or Hyper Technolog Dec 2001. http://www.deepfreezeusa.com/benefits.htm#2

[8] "Towards a Taxonomy of Intrusion Detection Systems", Herve Debar, Marc Dacier, Andreas Wespi, Computer Networks, 31, pp 805-822, Elsevier, 1999.

[9] “Network Security, Filter, and Firewalls”, Darren Bolding, http://www.acm.org/crossroads/xrds2-1/security.html, Dec 2001.

[10] ”Computer Forensics Tools Verification”, Gary Fisher, http://www.itl.nist.gov/div897/docs/computer_forensics_tools_verification.html, Dec 2001.

[11] “Network Sniffers”, Aleksandar Stancin, Help Net Security, http://www.net-security.org/text/articles/sniffers.shtml, Dec 2001.

[12] “Vulnerability Assessment Scanners”, Jeff Forristal and Greg Shipley, http://www.networkcomputing.com/1201/1201f1b1.html, Jan 2001.

[13] “Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption”, Winn Schwartau and John Draper, May 2000.