NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

NETWORK DEFENSE-IN-DEPTH: EVALUATING
HOST-BASED INTRUSION DETECTION SYSTEMS

by

Ronald E. Yun
and
Steven A. Vozzola

June 2001

Thesis Advisor:	Richard Harkins
Second Reader:	Daniel Warren

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2001	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Network Defense-in-Depth: Evaluating Host-based Intrusion Detection Systems		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Yun, Ronald E. and Vozzola, Steven A.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

ABSTRACT *(maximum 200 words)* As networks grow, their vulnerability to attack increases. DoD networks represent a rich target for a variety of attackers. The number and sophistication of attacks continue to increase as more vulnerabilities and the tools to exploit them become available over the Internet. The challenge for system administrators is to secure systems against penetration and exploitation while maintaining connectivity and monitoring and reporting intrusion attempts. Traditional intrusion detection (ID) systems can take either a network or a host-based approach to preventing attacks. Many networks employ network-based ID systems. A more secure network will employ both techniques. This thesis will analyze the benefits of installing host-based ID systems, especially on the critical servers (mail, web, DNS) that lie outside the protection of the network ID system/Firewall. These servers require a layer of protection to ensure the security of the entire network and reduce the risk or attack. Three host-based ID systems will be tested and evaluated to demonstrate their benefits on Windows 2000 Server. The proposed added security of host-based ID systems will establish defense-in-depth and work in conjunction with the network-based ID system to provide a complete security umbrella for the entire network.

14. SUBJECT TERMS Computing and Software, Network Security, System Security, Intrusion Detection, Intrusion Detection System, Defense-in-depth	15. NUMBER OF PAGES 86
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFI- CATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

NETWORK DEFENSE-IN-DEPTH: EVALUATING HOST-BASED INTRUSION DETECTION SYSTEMS

Ronald E. Yun
Lieutenant, United States Navy
B.S., Strayer College, 1995

Steven A. Vozzola
Lieutenant, United States Navy
B.S., Jacksonville University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 2001

Authors: _____
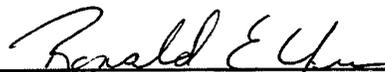
Ronald E. Yun

_____
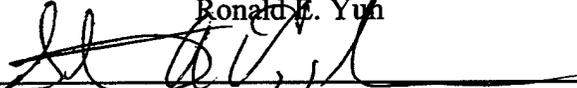
Steven A. Vozzola

Approved by: _____

Richard Harkins, Thesis Advisor

_____
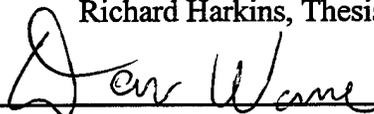
Dan Warren, Second Reader

_____
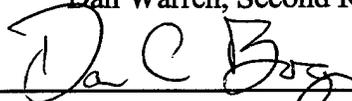
Dan Boger, Chairman C4I Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As networks grow, their vulnerability to attack increases. DoD networks represent a rich target for a variety of attackers. The number and sophistication of attacks continue to increase as more vulnerabilities and the tools to exploit them become available over the Internet. The challenge for system administrators is to secure systems against penetration and exploitation while maintaining connectivity and monitoring and reporting intrusion attempts.

Traditional intrusion detection (ID) systems can take either a network or a host-based approach to preventing attacks. Many networks employ network-based ID systems. A more secure network will employ both techniques. This thesis will analyze the benefits of installing host-based ID systems, especially on the critical servers (mail, web, DNS) that lie outside the protection of the network ID system/Firewall. These servers require a layer of protection to ensure the security of the entire network and reduce the risk or attack.

Three host-based ID systems will be tested and evaluated to demonstrate their benefits on Windows 2000 Server. The proposed added security of host-based ID systems will establish defense-in-depth and work in conjunction with the network-based ID system to provide a complete security umbrella for the entire network

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF SNAPSHOTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENT

I. INTRODUCTION

> Over the last 6 years, Government and defense agencies in the United States have been victim to literally millions of attacks originating from the internet. Due to the low information security budgets and the weak security policies of such agencies, information security has become an uphill battle, as government and military servers are constantly being probed and attacked by crackers.

The Network Security Solutions, Ltd., FIST Staff, February 2001.

A. BACKGROUND

As the digital generation continues to expand, so does the use of personal computers for worldwide connectivity. This expansion has resulted in a myriad of complex computer security issues especially a greater susceptibility to exploitation and attack. The importance of maintaining safe, secure and efficient communications has increased, but the ability to do so has become increasingly more complex. As networks expand, the need to adopt a defense-in-depth posture of providing system security is amplified. The Department of Defense (DoD) relies on computers for nearly every aspect of its operation; DoD computer networks are a rich target for all attackers, foreign and domestic, professional and novice, insider and outsider. Information warfare can be waged extensively on computers, whether it is denial of services, exploitation of information, defacing web sites or deception. The number and sophistication of computer attacks has steadily grown as more vulnerabilities have been found and tools to exploit those vulnerabilities have become more readily available. The challenge currently facing government information system security managers is to secure government systems

1

against exploitation and penetration while maintaining the availability of government systems, ensuring the authenticity and integrity of data transmitted, and establishing an effective means of monitoring and reporting intrusion attempts.

Intrusion detection (ID) systems may offer a solution to the defense-in-depth strategy of protecting government networks. It is critical not only to prevent unauthorized access to government systems but also to have an alert mechanism to notify government personnel of intrusion attempts, successful or unsuccessful. Every organization should know who is attempting to enter their network and why. Intrusion detection systems seem to be the logical complement to network firewalls. An ID system will extend the system administrators' security management capabilities to include security audit, monitoring, attack recognition, and response. There are numerous commercial off-the-shelf (COTS) products designed to accomplish this goal. A thorough evaluation is necessary to determine whether one of these products can successfully satisfy government requirements and enhances the standard of security for individual commands. This thesis will evaluate Windows 2000 Server vulnerabilities and review three host-based Intrusion Detection Systems: BlackICE, ZoneAlarm and Sygate. The objective of this thesis is to provide an analysis of the benefit of utilizing host-based ID systems inside and outside the network firewall.

To establish a baseline for evaluating intrusion detection systems certain terms need to be defined.

B. INTRUSIONS

An **intrusion** is an attempt to break into or misuse a system. An intrusion can be any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. In a military environment intrusions can be used for multiple purposes including compromise of information, denial of services, information warfare and deception.

> In September 2000, a large financial services company had their computer systems hacked, and credit card numbers for over 20,000 people were stolen. [Ref 1]

> In 1999, hackers hijacked nearly 500,000 credit card numbers and stored them on United States government computers. [Ref 2]

The intrusion process begins when an intruder takes steps to fulfill an objective. The objective could be any type of attack including the theft of information, corruption of files, defacing a web site, or causing a denial of service. An essential component of an intrusion is taking advantage of one or more vulnerabilities. The vulnerabilities exploited in this process can range from a software deficiency, such as a buffer overflow, to a flaw in an organizational structure that enables sensitive information such as logins and passwords to be determined through social engineering. The intrusion process ends when some or all of the objectives are achieved or the intruder gets discouraged and gives up. One goal of an Intrusion Detection System is to discourage an attacker to the point that he gives up.

Attack objectives can range from sensitive information being stolen to denial of service (DOS). For example, an attacker can download sensitive information from the FTP or web server from the external host that is acting as a bridge between the Internet and the internal network. A denial of service attack would attempt to overwhelm the network to the point that it can no longer function properly. Common forms of this attack include:

- SYN Flood
- ICMP Flood (ping flood)
- Smurf Attack
- Mail Bombs
- Host System Hogging
- Rogue Applets

The University of California at San Diego stated in a recent study that more than 4000 Denial of Service attacks are unleashed every week. In February 2000 one such DOS attack crippled Ebay, Yahoo!, CNN, Datek, E*Trade, ZDNet and several other Web sites for several hours. Although this kind of attack is not destructive, in that no files are altered or destroyed, the Web site's ability to conduct business is severely impaired or completely interrupted for a period of hours or days. In a military environment where information flow is critical to mission success, this type of attack could be disastrous.

ID systems can provide protection from some of these attacks. When the system receives a SYN packet, the ID system can determine if it is coming from a legitimate, authorized IP address. If the SYN packet is not from a valid IP address or if the request

fits a certain suspicious pattern, a message is sent to the firewall to reject subsequent SYN packets from that IP address. It is imperative that the ID system has the capability of preventing unauthorized outgoing connections.

Intruders who conduct such attacks can fall into two broad categories: Outside Intruders and Inside Intruders. Most people perceive the outside world to be the largest threat to their security. The media scare over "hackers", "crackers" and "attackers" coming in over the Internet has only heightened this perception. However, FBI studies have revealed that ninety percent of U.S. companies experienced Internet fraud over the past two years and eighty percent of intrusions and attacks came from within an organization. A mechanism is needed to detect both types of intrusions -- a break-in attempt from the outside and a malicious attack from a knowledgeable insider.

C.   INTRUSION DETECTION SYSTEMS

In a world of firewalls and security auditing tools, why is a real-time intrusion detection system needed? Similar to the use of security cameras and burglar alarms on a locked and guarded building, an ID system should be used on a secure network for the following reasons:

1. Depth of defense: no matter how many security measures you have in place, if they are defeated, it is necessary to have a system that identifies this immediately -- a "burglar alarm.

2. Efficiency: ID systems, like security cameras and alarms, allow an organization to leverage fewer staff members to monitor and secure a larger area in an automated manner. It is cost and resource-prohibitive to place

firewalls everywhere on the network and run security audits at all hours of the day.

3. Route tracing: ID systems can provide incriminating forensic evidence that may not otherwise be available from firewall or audit logs (again fulfilling the role of the security camera).

4. "Beware of Dog" sign effect: similar to the sign on a fence, a prominently displayed notice of intention to monitor traffic is often the only dissuasion attackers need to move on to another site with less-formidable security obstacles.

Hardware-based network firewalls are ideal for implementing security policies between networks, but they can be expensive, complicated, inflexible, and quickly outdated--susceptible to new attacks. They may also be rendered ineffective by dialup access weaknesses, encryption, VPN's, and remote users connecting directly to the Internet from home.

1. Types Of Intrusion Detection Systems

Most traditional intrusion detection systems take either a network or a host-based approach to recognizing and preventing attacks. A **host-based** ID system is designed to monitor the system on which it is installed. A traditional host-based ID system monitors the Operating System for attack signatures within log files or audit trails. A host-based ID system can also be used to monitor a specific application or database server. Currently, host-based ID system technologies are adapting to the changing industry, and a host-based ID system can employ a variety of techniques. A **network-based** ID system looks for specific patterns or attack signatures that indicate malicious or suspicious intent

within network traffic. Network ID systems can use two different databases to identify intrusions: a built-in static signature database or a dynamic signature database that constantly monitors the system operations and updates its database automatically. Figure 1 below illustrates both types of ID systems.
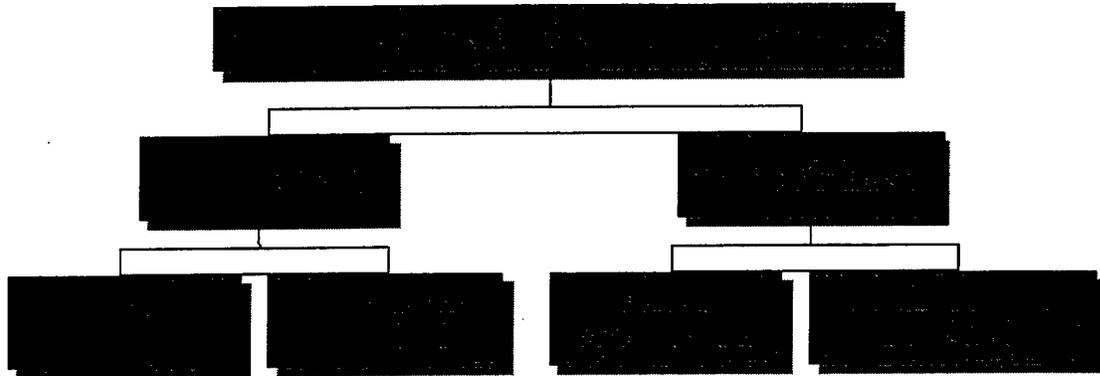
Figure 1 – Types of ID Systems [From Ref 3]

The host-based ID system resides at the Application Layer of the OSI model on the host as seen in Figure 2 and is therefore restricted to monitoring the audit trails of the operating system or applications. The Network-based ID system resides on a separate computer from the server and monitors all network traffic and audit data between the server and the clients. The Network ID system monitors information flow at all layers of the OSI model as depicted in Figure 3. Each approach has its strengths and weaknesses, and each is complementary to the other. A truly effective intrusion detection system will employ both technologies, providing a defense-in-depth. The personal ID systems evaluated in this thesis will incorporate a combination of these technologies.
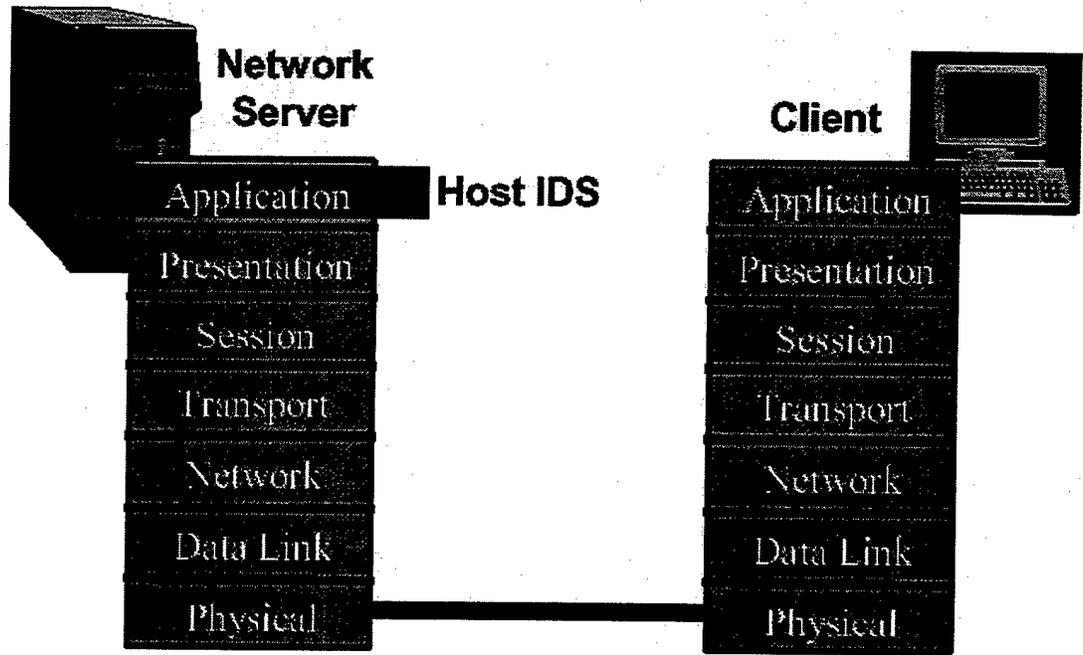
Figure 2 – Traditional Host-based ID System vs. OSI Model [From Ref 3]
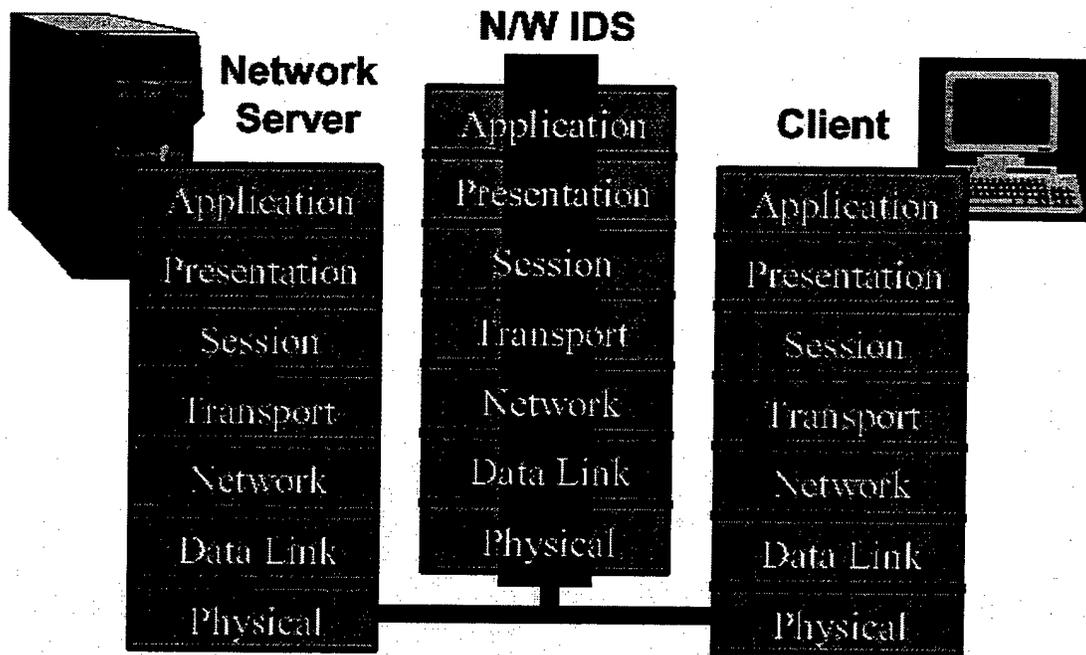
Figure 3 – Network ID System vs. OSI Model [From Ref 3]

D. ID SYSTEM METHODOLOGY

There are generally two intrusion detection models:

1. The **Signature based detection model** monitors system traffic for known attack signatures. The ID system evaluates packets to see if they correspond to a known intrusion pattern. Most successful intrusion detection systems rely on the signature detection model. Attacks, like viruses, are always changing, so the success of this model relies on maintaining a current signature library.

2. The **Anomaly based detection model** looks for trends that deviate from a system's normal usage pattern or deviations from a user's normal behavior. The anomalies are detected by building up a profile of the system being monitored, and detecting significant deviations from this profile. Although the anomaly detection model doesn't rely on an up to date signature database, it is more difficult to engineer than the signature based model and is seldom utilized in the industry. The theory behind anomaly detection is based on metrics that are derived from system operations. These metrics are computed from available system parameters such as average CPU load, number of network connections per minute, number of processes per user, etc. ID systems that utilize the anomaly model often look for inconsistencies in the Operating System audit trails. Audit trail data forms a *footprint* of system usage over time and establishes a baseline. From these observations, the ID system can analyze system metrics to detect a possible intrusion. An anomaly may be a symptom of a possible intrusion, but it can also be a change in an authorized user's activity. Anomaly detection is more challenging than misuse detection since one cannot simply monitor for any known malicious patterns or

signatures, thus it requires a more flexible approach which is far more complicated to develop.

An ID system may also performs its own system monitoring and anomaly detection. It may keep aggregate statistics that provide a system usage profile. These statistics can be derived from a variety of sources such as CPU usage, disk I/O, memory usage, activities by users, number of attempted logins, etc. These statistics must be continually updated to reflect the current state of the system. The statistics are correlated with an internal model that allows the ID system to determine if a series of actions constitute a potential intrusion. This model may describe a set of intrusion scenarios or possibly encode the profile of a clean system.

E.   EVALUATING ID SYSTEMS

Personal host-based ID systems need to enforce particular security policies. They should have the ability to identify and block known port scans, Trojans and Denial of Service attacks, as well as protect against new or unknown attacks by blocking applications and traffic that violate a defined profile's security rules. These rule-based security policies should include any combination of the following:

- Application – allowing each application access privileges to only certain required IP addresses, ports, or protocols
- Trusted IP Addresses – allowing access privileges to specific IP addresses
- Ports – allowing access privileges to specific ports
- Protocols – allowing access privileges to specific protocols

- Schedule – allowing automatic implementation of different security policies at different times.

Intrusion detection monitoring and reporting is not full proof and error free. It is important to identify and minimize potentially misleading error reports. These errors can be categorized as either false positive, false negative or subversion errors. A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. These reports will normally be ignored since they are legitimate actions simply classified as intrusions. If too many false positives are generated, the operators will come to ignore the output of the system, which may lead to actual intrusions being detected but ignored over time. A false negative occurs when an actual intrusive action has occurred but the system allows it to pass as a non-intrusive behavior. False negative errors are more serious than false positive errors because they give a misleading sense of security. By allowing all actions to proceed, a suspicious action will not be brought to the attention of the operator. The intrusion detection system is now a liability as the security of the system is less than it was before the ID system was installed. An effective ID system will minimize these false alarms and missed attacks, while maximizing valid detections through proper configuration and monitoring, maintaining updated software patches and signature databases, and effective training of users and administrators.

Additionally, ID systems can be susceptible to subversion. A subversion error occurs when an intruder modifies the operation of the intrusion detector to force false negatives. An intruder could use knowledge about the internals of an intrusion detection

11

system to alter its operation, possibly allowing anomalous behavior to proceed. A human operator examining logs may discover this, but the intrusion detection system would appear to be working correctly. This is sometimes done by slowly altering the system's footprint or metrics over time. An intruder slowly introduces anomalies into the system to permit the ID system to allow greater anomalies, until it is safe for the intruder to launch an undetected attack.

A good ID system should address certain basic issues, regardless of what mechanism it is based on. It ought to:

- Run continually
- Be fault tolerant
- Resist subversion
- Operate with minimal overhead
- Be easily tailored to observe deviations and changes in system behavior
- Be difficult to fool
- Be able to back trace and identify the source of intrusion attempts

It is difficult to identify and evaluate the processes, procedures, tools, software, hardware, and databases that comprise the full range of intrusion detection technologies. Since the technology is continually evolving, the methods and processes of ID systems continue to develop and change. The process for evaluating an ID system requires setting up a network, controlling the operating environment, generating traffic samples, determining the required supporting data, and evaluating the results. Implementing intrusion detection systems on networks and hosts requires a broad understanding of

computer security. The complexity of information technology infrastructures is increasing so quickly that is has become nearly impossible for any one person to fully understand, let alone administer, systems in a way that is operationally secure. Vendors are rapidly releasing new ID systems and aggressively competing for market share in the ever-expanding market. Many products started out as point solutions, but in response to consumers' inability to fully understand and use them, many vendors are attempting to integrate approaches to solve a broader range of computer security problems. This illustrates the value of establishing a baseline for reviewing ID systems in order to determine their usefulness on government systems. Given the complexity of the problem outlined above, this thesis will focus on analyzing the current vulnerabilities inherent to Windows 2000 Server and demonstrating how off-the-shelf products like ZoneAlarm, BlackICE and Sygate Personal Firewall can improve the security of government systems. Recommendations will be made for follow-on tests that would help further understand the benefits, utilities and operations of ID systems.

The diagram on the following page (Figure 4) illustrates how a typical network-based intrusion detection system works. The picture shows the flow of an attack being launched, the ID system sniffing the packets, comparing the packets to the database of known attacks, reacting to the attack, blocking dangerous traffic, and alerting the system operator/administrator to the attack.

Intrusion-detection systems: How they work
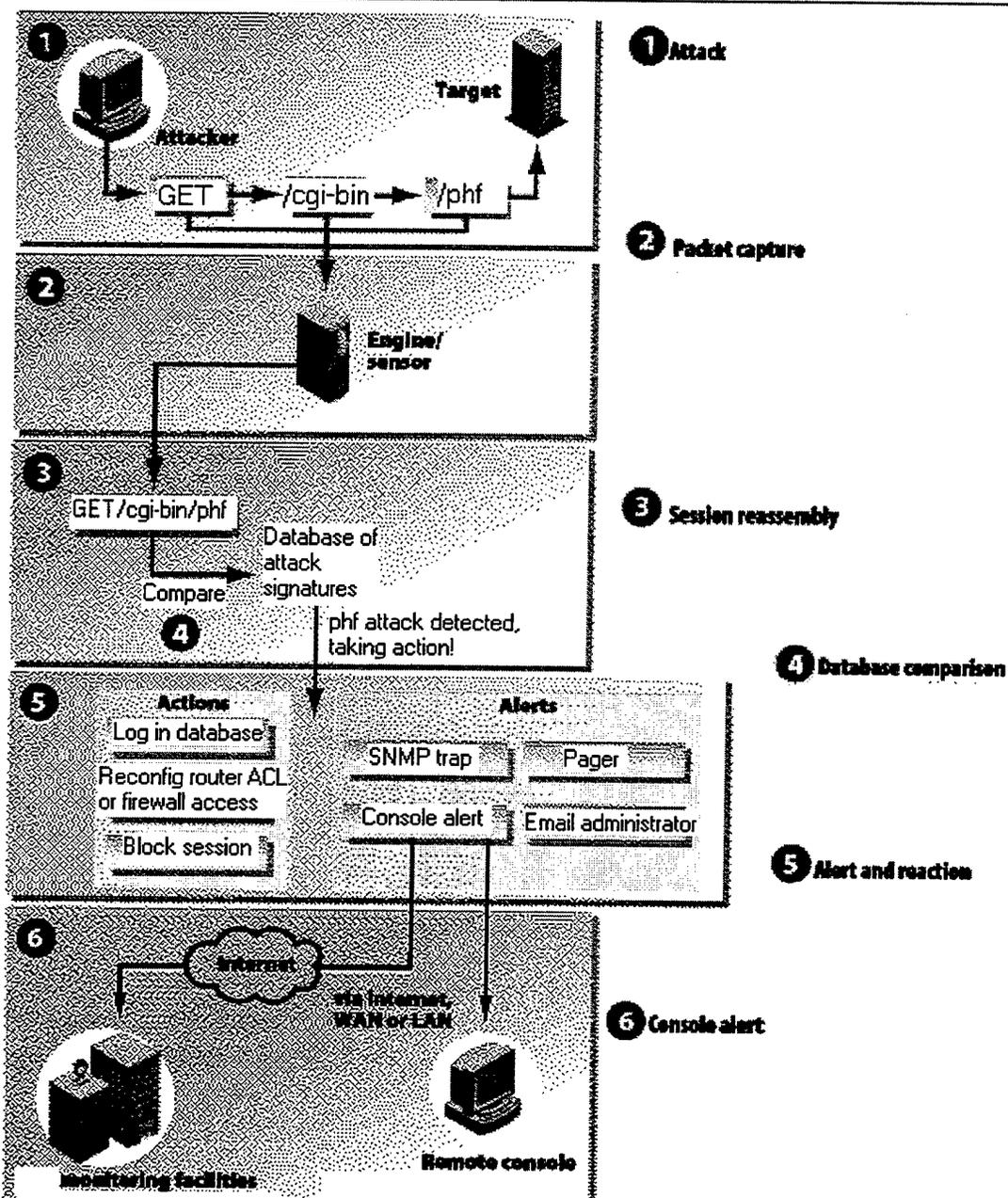
Figure 4 – Network-based ID System Operation [From Ref 4]

14

II. PROBLEM PROPOSAL

It doesn't take long to figure out the security problem with these port technologies: If a port lets data flow out, it also lets data flow in. A port is essentially an opening into your computer, and it can be hacked. Someone can infect your machine with a Trojan horse in this way, and that's only one of a host of distressing possibilities. If you open your computer to the outside world, you're vulnerable to attack -- period.

Randall, Neil, "Freeware Port Scanners: Plug the Holes", PC Magazine, URL:
http://www.zdnet.com/products/stories/reviews/0,4161,2651662,00.html
(16 November 2000).

A. INTRODUCTION TO ID SYSTEM PROBLEM

Many networks administrators do not realize the value of employing host-based and network-based ID systems simultaneously. Host-based ID systems could be used to assist network-based ID systems in protecting client stations inside the firewall as well as providing a much needed layer of protection for the vital servers that lie outside the network firewall – DNS, mail, and web. In making these servers available to the outside world, they are vulnerable to attacks. Host-based ID systems could provide protection from this security risk.

Recent research conducted at the NPS illustrates the vulnerability of systems located outside the network firewall. Data collected and analyzed in the NPS RIDLR lab demonstrated how often unprotected servers were penetrated for exploitation.

A Honeypot is a set of systems that simulates a real network. The Honeypot is used to observe accesses and attempted accesses. This provides advanced warning of a more concerted attack. [Ref 5]

15

The Honeypot, in a sense, provides the ability to 'get into the head' of the attacker: analogous to preparing for a game by watching films of the rival team. The results of Honeypots has proved not only beneficial in identifying patterns and methods of attack but also in identifying the need for a capable host-based intrusion detection system. These results endorse the need for research, testing and evaluation of commercial intrusion detection systems.

To develop a defense-in-depth approach requires an understanding of the strengths and weaknesses of commercial intrusion detection systems. There are a vast number of commercial ID system products available on the market today. The evaluation of all these products is impractical, so a small sampling will be taken and a test site configured. Host-based ID systems are one possible step toward enhancing the protection of servers located outside the firewall and improving security on client computers within the firewall. This thesis will compare three host-based ID systems installed on a Windows 2000 Server and present the strengths and weaknesses of each. Consideration will also be given to the benefit of installing host-based ID systems on the client machines within a network.

The principle reason for system security is to protect systems from the numerous vulnerabilities inherent to computers networks. These vulnerabilities are predominantly:

- Software bugs
- System configuration
- Password cracking
- Sniffing unsecured traffic and
- Design flaws.

Attackers will attempt to exploit any and every available weakness in a system. The Internet contains a plethora of information regarding software design flaws and hacking tools that render a system vulnerable. The availability of this information makes it difficult to continually patch every hole in a network to prevent exploitation.

The attacker's methodology begins with **scanning** a range of network IP addresses to determine which individual systems are alive and what services are available. **Enumeration** is then done to identify valid user accounts or poorly protected resource shares. Finally, the attacker uses **escalation** to increase permission to gain access to vital information and services.

This thesis will focus on the first step of this process. Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a LAN or connected to the Internet via a modem run various services that listen to ports, both well-known and some not so well-known. Port scanning allows the attacker to find which ports are available, being listened to by a service, on the computer. Ports provide access to services and services provide access to applications and data which can lead to exploits. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is available and can therefore be probed further for weakness. A TCP/IP port is a logical communication portal by which information can flow. All Internet protocols communicate via ports, and specific information is normally designated to use a specific port. Examples of well known ports are listed below:

- Echo　　　　　7/tcp　　　　Echo
- FTP-Dta　　　20/udp　　　File Transfer [Default Data]
- FTP　　　　　21/tcp　　　File Transfer [Control]
- SSH　　　　　22/tcp　　　SSH Remote Login Protocol
- Telnet　　　　23/tcp　　　Telnet
- SMTP　　　　25/tcp　　　E-mail
- Domain　　　53/udp　　　Domain Name Server
- WWW/HTTP　80/tcp　　　World Wide Web/HTTP

The simplest port scan attempts to send a carefully constructed packet to each possible port, 0-65535, on the target system to see which ports are open. Using a system call such as connect() the port scan utility attempts to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port is not reachable. Once an open door is identified, the hacker has achieved the first objective towards exploiting a target computer. This fact makes it imperative to have a reliable and effective intrusion detection system. Port scanning will be the initial test conducted in the lab on our test server.

III. TEST BED SETUP AND CONFIGURATION

A.   EQUIPMENT

The equipment required to conduct the tests includes: three desktop computers - one to act as the network server, one to execute the attack and one for connectivity to the Internet for research and resources; one hub to enable connectivity between the network computer and the attack computer; one copy of Windows 2000 Server; one copy of Windows 2000 Professional; one copy of SuperScan and LanGuard port scanning programs; and licensed copies of ZoneAlarm, BlackICE and Sygate intrusion detection systems. All hardware and software were checked to ensure they were compatible and the minimum system requirements were met.

The following illustration (Figure 5) depicts the lab configuration.
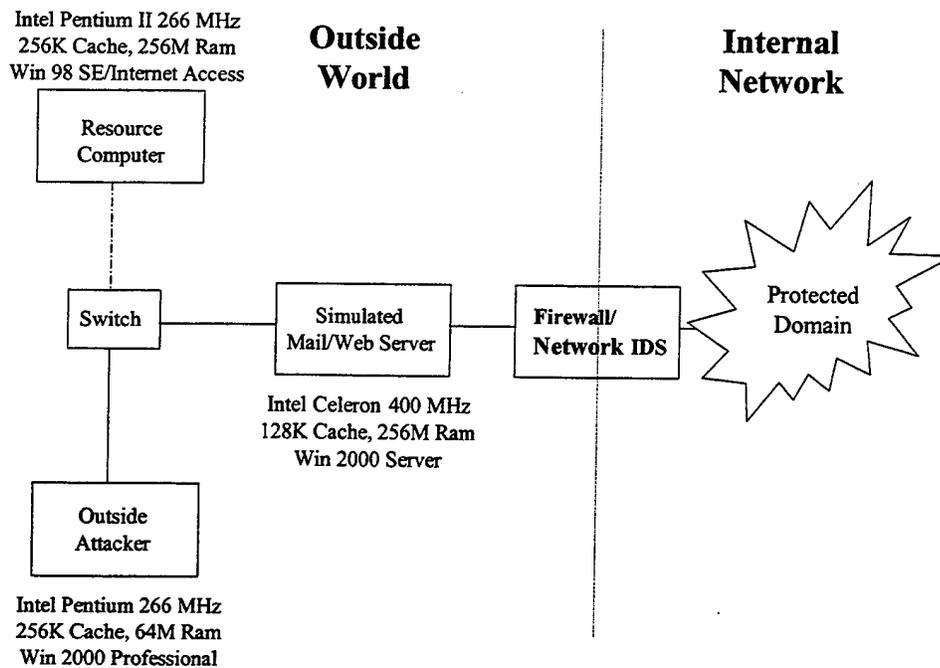
Figure 5 – Lab Configuration

The network server installation included:

- Windows 2000 Server installed with the following specifications:
  - Enabled as a Domain Controller
  - Active Users and Directories enabled
  - TELNET disabled (by default)
  - IP security was disabled by default (no specific port restrictions)
- Microsoft Office 2000
- User accounts were created and share folders designated
- IP address 192.168.100.40 was configured
- Additionally, no specific security measures were implemented and the system was run for a period of time to ensure that it was functioning properly. No intrusion detection system was installed for the baseline tests.

The attack computer configuration included:

- Windows 98 and Windows 2000 Professional in a dual boot configuration

20

- IP address was configured to 192.168.100.80
- SuperScan 3.0, LanGuard software installed

To evaluate the integrity of the network server, a series of <u>attacks</u> were run to interrogate the overall security of the Windows 2000 Server machine. To simulate the first step in a typical attack, the attack computer used commercial scanning software available for free off the Internet.

The primary test program used was SuperScan 3.0. SuperScan is a connection-based TCP port scanner, pinger and hostname resolver. This program performs ping scans and port scans using any IP range. In addition it will resolve and reverse-lookup any IP address or range. A second series of scans were run to validate the SuperScan test results using LanGuard. LanGuard port scanner is a freeware tool that allows you to scan a network for active ports and identify unused applications such as web servers that could be a security hole.

Resident programs and commands within the Microsoft Operating System such as FTP and ping were used to further verify the level of security provided by the ID system. Connection attempts were made to determine if the ID system was actually protecting ports or simply making them invisible to scans.

The tests were conducted and information collected and compared against four system configurations:

- A Windows 2000 Server with no ID system
- A Windows 2000 Server protected by ZoneAlarm
- A Windows 2000 Server protected by BlackICE

21

- A Windows 2000 Server protected by Sygate

Additionally, various security levels or configurations of each intrusion detection system was tested and evaluated. The results were analyzed to determine the overall strengths and weaknesses of each ID system. Snap shots of the program windows from the attack computer and the host server are included to help illustrate the findings and facilitate the comparison.

B.   INTRUSION DETECTION SYSTEMS

1.   Zone Alarm

ZoneAlarm is one the most widely disseminated ID system programs. Its popularity is primarily due to the fact that the software is available at no cost for personal use. This fact and the positive reviews of the program supported the selection of ZoneAlarm as one of the ID systems tested.

> ZoneAlarm combines the safety of a dynamic firewall with total control over applications' Internet use. ZoneAlarm gives rock-solid protection against thieves and vandals. ZoneAlarm now features MailSafe to stop email-borne Visual Basic Script worms, like the "I Love You" virus, "dead-in-its-tracks", thwarting its spread, and preventing it from wreaking havoc on your PC. ZoneAlarm makes ironclad Internet security easy-to-use. [Ref 6]

The ZoneAlarm program is based on TrueVector technology. TrueVector is basically a software engine made by Zone Labs that runs on the operating system (Win32) to report Internet connection activity to client applications. TrueVector performs all monitoring, logging and filtering work, and is responsible for intercepting process-

loading and unloading. It keeps a list of currently active processes, and intercepts certain keyboard, mouse and other user activities in order to determine the active application. TrueVector can check for various characteristics including executable name, version numbers, executable file checksums, version headers, and configuration settings.

ZoneAlarm with TrueVector is designed to:

- Give notification when applications are accessing the Internet
- See the type of access: URL, site, IP address, port address
- See the protocol being used
- See the type of data being sent or used
- Determine the time and the date of data requests
- Control bandwidth consumed per application

ZoneAlarm has security-level controls for both local (trusted) communications and external Internet connections. Each category has three choices – low, medium and high. The user can select six different security configurations (L/L, L/M, M/M, L/H, M/H, H/H).

Table 1 below describes each security setting:

SETTING	LOCAL	INTERNET
HIGH	- Enforces application privileges. - Internet Lock blocks all traffic. - Hides all ports not in use by a program (sometimes called Stealth Mode) - Blocks local access to Windows services and shares	- Enforces application privileges. - Internet Lock blocks all traffic. - Hides all ports not in use by a program (sometimes called Stealth Mode) - Blocks Internet access to file and print sharing.
MEDIUM	- Enforces application privileges. - Internet Lock blocks all traffic. - Allows access to Windows services and shares. - Leaves your computer and server applications visible to the local network.	- Enforces application privileges. - Internet Lock blocks all traffic. - Blocks Internet access to file and print sharing. - Leaves computer visible to the Internet
LOW	- Enforces application privileges - Internet Lock blocks only application traffic. - Allows access to Windows services and shares. - Leaves your computer and server applications visible to the local network.	- Enforces application privileges - Internet Lock blocks only application traffic. - Allows Internet access to file and print sharing. - Leaves computer visible to the Internet

Snapshot #1 illustrates the Security Settings menu for ZoneAlarm:
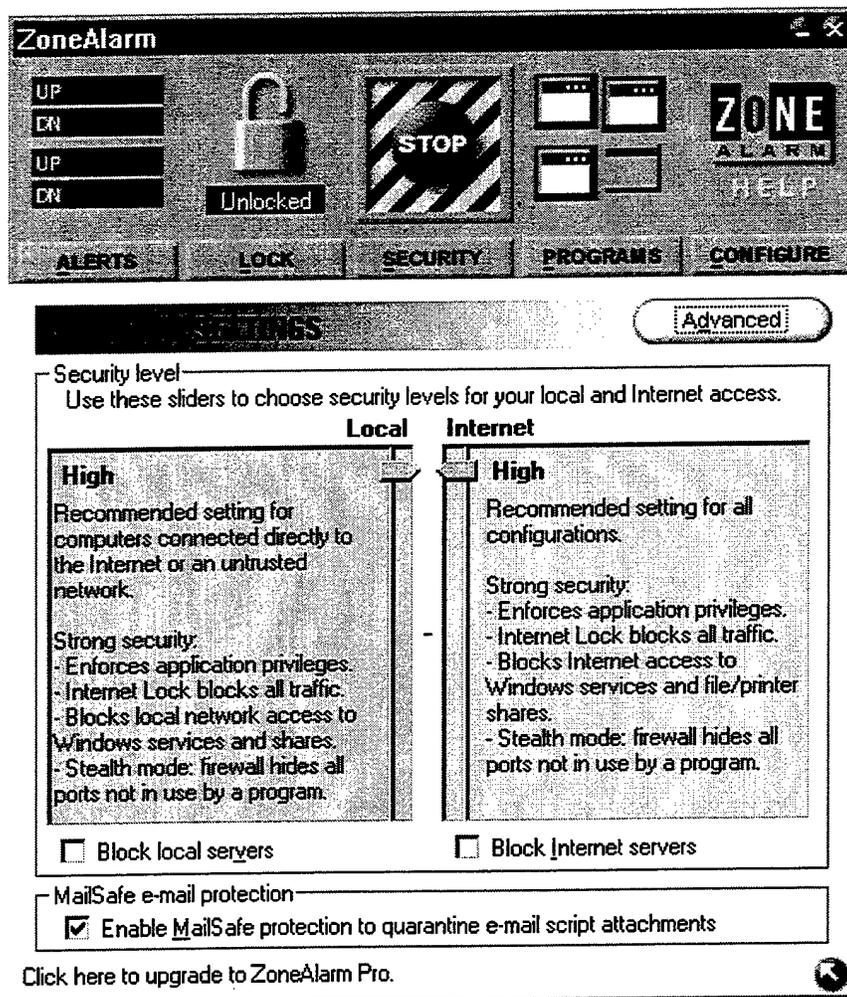
Snapshot 1 – ZoneAlarm Security Settings

The tests conducted only focused on the Internet security settings. Additional features of ZoneAlarm included pop-up windows alerting the user of possible intrusions and a log file of all activity on the computer it is monitoring. In medium and high security mode ZoneAlarm blocks all traffic until the user grants permission.

2.   BlackICE

BlackICE was developed by Network Ice Corporation and claims to be a full-featured personal firewall.

> BlackICE works continually to defend servers and workstations from over 200 hacker signatures including the Melissa Worm, "Slow Scans" and "Back Orifice." Even if hackers bypass firewalls or intrusion defenses, BlackICE bars entry at the desktop and server. [Ref 7]

BlackICE has four security levels as described in the Table 2 below:

SECURITY LEVEL	DESCRIPTION
PARANOID	Blocks all unsolicited inbound traffic. May restrict some web browsing and interactive content
NERVOUS	Blocks all unsolicited inbound traffic except for some interactive web site content. (such as streaming media)
CAUTIOUS	Only blocks unsolicited network traffic that accesses operating system and networking services
TRUSTING	All ports remain open and unblocked, and therefore allows all inbound traffic

In addition to the security levels, BlackICE has 3 protection tabs to further define the program configuration:

- ENABLE AUTO BLOCKING – This feature automatically blocks all attempts to break into a system. If unchecked, an attack will still be reported and logged, but not automatically blocked.

- ALLOW INTERNET FILE SHARING – When enabled, an external connection can be made to a computer over the Internet to upload or download files. If unchecked it prevents systems from connecting to the computer and accessing the shares.

- ALLOW NETBIOS NEIGHBORHOOD – When enabled the host computer will appear in the Network Neighborhood of other computers, and the host name is resolved on scans.

Snapshot #2 illustrates the security settings menu for BlackICE Defender:

BlackICE Settings

| Detection | | ICEcap | | Preferences |
| Protection | Packet Log | Evidence Log | Back Trace |

Manage the BlackICE protection levels and network file sharing capabilities.

Protection Level
- ⦿ Paranoid — Blocks all unsolicited inbound traffic.
- ○ Nervous — Blocks most unsolicited inbound traffic.
- ○ Cautious — Blocks some unsolicited inbound traffic.
- ○ Trusting — Allows all inbound traffic.

- ☑ Enable Auto-Blocking
- ☐ Allow Internet file sharing
- ☐ Allow NetBIOS Neighborhood

[OK] [Cancel] [Apply] [Help]

Snapshot 2 – BlackICE Settings Menu

BlackICE Defender is composed of a detection and analysis engine that constantly monitors the inbound and outbound traffic between your computer and the Internet or other computers on a network. The core of the BlackICE product is the patent-pending seven-layer decoding engine. This engine analyzes incoming and outgoing network traffic in real-time for intrusions. Unlike most modern intrusion detection systems, which use "pattern matching" technologies, BlackICE

27

uses sophisticated protocol analysis algorithms. Protocol analysis examines the structure and composition of network communications. BlackICE considers this a more efficient way to detect and identify attacks while allowing it to detect sophisticated intrusions that pattern matching software cannot catch.

3.   Sygate

Sygate Technologies has recently entered the host-based intrusion detection market with Sygate Personal Firewall 4.0. According to Sygate's website their product is:

> Sygate is more than an advanced, user-friendly personal firewall – it is a bi-directional intrusion detection system. [Ref 8]

Sygate's serves as a firewall by controlling access to communications ports and monitoring port-scanning activity. As an intrusion defense agent, Sygate hopes to allow only trusted communications and considers any other network activity as malicious.

Using a *guilty until proven innocent* approach, Sygate claims to preserve system resources by maintaining a 60,000-signature library of known attacks, but only uses it for reporting purposes. This rules-based approach is less memory intensive but requires more user interaction.

Sygate has three security level configurations as described in Table 3 below:

SECURITY LEVEL	DESCRIPTION
BLOCK ALL	Prevents all information entering or leaving your computer from any outside source.
NORMAL	Automatically blocks any access from your computer until the user grants access. Allows user to alter the "status" of different applications.
ALLOW ALL	Permits the transmission of all network traffic to and from your computer. Still logs all traffic

Sygate Personal Firewall 4.0 provides users with performance enhancing features

including:

- **Dynamic Interface Support** – Allows users to configure separate security policies for each network interface card directly from the user interface

- **Application Learning Mode** – Enables Sygate Personal Firewall to remember which applications have been allowed or blocked by the user

- **Application Authentication** – Uses MD5 cryptographic signatures to check application attributes such as checksum, path and file name, warning users to applications compromised by a hacker or Trojan

- **Dynamic Port Blocking** – Automatically blocks ports when applications that otherwise use them are idle, reducing exposure to attack

- **High Performance Security** – Ensures top-notch security while minimizing impact to system performance

Sygate Personal Firewall provides pop-up window notification of any new or

modified applications, detected attacks or user-specified events, and has a box to check to

remember these notification responses to eliminate redundancy. The illustrations below

(Snapshots 3 and 4) are examples of the user interface notification provided by Sygate.

Sygate Personal Firewall

RealPlayer is trying to connect to realguide.real.com [207.188.7.117] using remote port 80. Do you want to allow this program to access the network?

☐ Remember my answer, and do not ask me again for this application.

[Yes]   [No]   [Detail <<]

Detail information of RealPlayer and the connection it tries to establish:

```
File Version :          6.0.9.450
File Description :       RealPlayer
File Path :             D:\Program Files\Real\RealPlayer\realplay.exe
Process ID :            FFFC1F23 (Hexmial) 4294712867 (Decimal)

Connection origin :     local initiated
Protocol :              TCP
Local Address :         10.0.6.190
Local Port :            1726
Remote Name :           realguide.real.com
Remote Address :        207.188.7.117
Remote Port :           80

Ethernet packet details:
Ethernet II (Packet Length: 62)
        Destination:    00-d0-b7-25-41-df
        Source:         00-a0-cc-57-46-99
Type: IP (0x0800)
Internet Protocol
```

Sygate notifies the user when a program is attempting to connect and provides helpful details regarding the application.

Snapshot 3 – Sygate Alert Window

30

Time	Security Type	Severity	Direction	Protocol	Remote Host
02/28/2001 09:32:16	Denial of Service	Major	Incoming	ICMP	10.0.6.125
02/28/2001 09:31:45	Denial of Service	Major	Incoming	ICMP	10.0.6.125
02/27/2001 14:14:54	Port Scan	Minor	Incoming	TCP	10.0.6.125
02/27/2001 14:14:40	Port Scan	Minor	Incoming	TCP	10.0.6.125
02... Back Trace...	Trojan horse	Critical	Incoming	TCP	10.0.6.125
02/...	Port Scan	Minor	Incoming	UDP	10.0.0.3

The security log identifies the intrusion type and severity. It also provides a description of the intrusion

Description:

Trojan horse "SubSeven 2.1 Gold" de
Description:
 SubSeven 2.1 Gold

Snapshot 4 – Sygate Security Log

C. DATA COLLECTION PROCESS

A series of standard attack methods was launched against the Windows 2000 Server computer simulating a network server located outside a firewall. All activity on both the attack and network computers were monitored and snapshots of the resulting data copied. The evaluation was conducted against the following configurations:

- Windows 2000 Server with no ID system.
- Windows 2000 Server with ZoneAlarm 2.6 installed.
- Windows 2000 Server with BlackICE 2.5 installed.

31

- Windows 2000 Server with Sygate Personal Firewall 4.0 Build 671 installed.

The same set of exploits will be conducted against each of the four system configurations and the resulting data will be evaluated to determine the effectiveness of each ID system at securing the network server from exploitation. Consideration will be given, not only to stopping attacks, but also to how well the ID system alerts the user and system administrator to the real-time existence of attacks.

The evaluation criteria key elements will include:

- Effectiveness of intrusion detection
- Effectiveness of security protection
- Effectiveness of reaction
- User interface

The questions considered will include:

- What is the benefit of a host-based ID system to overall network security
- How effective is a host-based ID system
- Are host-based ID systems a possible solution to a defense in-depth posture for networks
- How easy is an ID system to implement and use, is it any more difficult than a virus scanning program
- Does the security benefits justify the additional cost of implementing host-based ID systems
- What follow-on testing should be conducted
- Should a standard test platform be developed for commercial ID systems

The above criteria and questions will be used during the process of the evaluation and to determine the effectiveness of adding host-based intrusion detection systems to network servers outside the firewall as well as client stations within the firewall.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TEST DATA RESULTS AND EVALUATION

A.   INTRODUCTION

The tests conducted emulate the first step in the intrusion process, port scanning. Most attackers only focus on the available ports detected through the use of a scanning tool. To properly identify how each of the ID systems performs in each of the key criteria elements, we evaluated the results of each system against an identical port scan using SuperScan 3.0. LandGuard port scanner was also used to validate the SuperScan results. An FTP connection was attempted to TCP port 21 in an effort to determine whether the ID systems masked the opened ports or actually blocked the available ports. The ping command was used to verify the ID systems were actually hiding the IP address from scanners. Snapshots from the attacking computer and the server will highlight the effectiveness of each ID system and indicate the array of features each ID system offers.

1.   NO ID SYSTEM INSTALLED

The initial test consisted of a port scan utility run against Windows 2000 Server with no ID system. The scan was conducted using SuperScan against ports 0-65,535. The results of this scan indicated 21 ports located on the host server (NPS-TESTSERVER) were available as seen in Snapshot 5 below.

SuperScan 3.00

Hostname Lookup

192.168.100.40
Resolved

Lookup
Me   Interfaces

Configuration
Port list setup

IP
Start 192.168.100.40
Stop 192.168.100.40
PrevC   NextC   1..254
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping
400
Connect
2000
Read
4000

Scan type
☑ Resolve hostnames
☐ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
● All list ports from 1   65535
○ All ports from   1   65535

← Note: IP address scanned and
number of ports to check (1-
65,535). Also, scanning options
available.

Scan
Pinging   -0-
192.168.100.40   0
Scanning   -0-
192.168.100.40   0
Resolving   -0-
192.168.100.40   0

Start   Stop

Speed
Max

☑ 192.168.100.40 NPS-TESTSERVER
•   7 Echo
•   9 Discard
+ • 13 Daytime
+ • 17 Quote of the Day
+ • 19 Character Generator
+ • 21 File Transfer Protocol [Control]
+ • 25 Simple Mail Transfer
• 42 WINS Host Name Server
• 53 Domain Name Server
+ • 80 World Wide Web HTTP
• 88 Kerberos
+ • 119 Network News Transfer Protocol
• 135 DCE endpoint resolution
• 139 NETBIOS Session Service
• 389 Lightweight Directory Access Protocol
• 443 https MCom
• 445 Microsoft-DS
• 464 kpasswd
• 563 snews
• 636 ssl-ldap
• 1030 BBN IAD

← Host IP address, name
and 21 open ports listed to
the left.

Active hosts and open port
windows to the right. →

Active hosts
1
Open ports
21

Save
Collapse all
Expand all
Prune

Min

Snapshot 5 – SuperScan vs. Win2K Server with no ID system

The results of this scan indicate that quite a large amount of information regarding

the network server: IP address, host name, available port numbers, and services available

on those ports.

The following ports and services were available with no ID system installed. This

list represents the default ports Windows 2000 Server makes available in order to perform

routine tasks. The available ports can be modified depending on the requirements of the

server and will be discussed in greater detail in chapter four.

36

A brief description of the port identified and any known Trojans used against these port is listed below:

7   Echo - Echoes back every line of text typed at it.

9   Discard (sink null) - Everything sent to this server should silently disappear.

13   Daytime - The server returns a packet in ASCII character string containing the date in readable form.

17   Quote of the Day - Sends a "Quote of the Day" regardless of input.

19   Character Generator (ttytst source) - Server spits characters in an endless stream.

21   File Transfer [Control] - Allow transfer of files from one computer to another. It uses two channels, one a control channel ftp/tcp and the other a data channel ftp-data/tcp. The DarkFTP Trojan also uses this port.

25   Simple Mail Transfer/* - De facto email standard for the internet. Also used by following Trojan horses: Ajan, Antigen, Email Password Sender, Haebu Coceda, Happy 99, Kuang2, NewApt, Promail Trojan, Shtrilitz Stealth, Tapiras, Terminator, WinPC, WinSpy.

42   Host Name Server - This is the old DNS. Replaced by the domain protocol. Microsoft's WINS may also support directory replication at this port.

53   Domain Name Server.

80   World Wide Web HTTP/* - Known Trojan horses: Executor, Hooker, and RingZero.

88   Kerberos - Implements a trusted third-party authentication protocol.

119   Network News Transfer Protocol/* - nntp=provides a client-server news feed protocol to allow clients to read "news". Happy 99 Trojan uses this port.

135   Microsoft DCE endpoint resolution/Location Service.

139   NETBIOS Session Service - "File and Printer Sharing" on a Windows machine uses this port extensively, which is frequently an exploitable security hole.

389   Lightweight Directory Access Protocol - Allows access via TCP to an X.500 directory. Used by NetMeeting - Internet Locator Server (ILS) using LDAP.

443   http protocol over TLS/SSL.

445   Microsoft-DS - It is used by Windows 2000 for SMB over TCP and UDP, concurrently or alternatively with the traditional implementation over ports 137, 138 and 139.

464   Kpasswd.

563   nntp protocol over TLS/SSL (was snntp) - Supported by MS Exchange.

636   ldap protocol over TLS/SSL (was sldap) - This is used by NetMeeting.

1030 BBN IAD.

Additionally, we were able to connect to the server (Snapshot 6) using the File Transfer Protocol (FTP). These results indicated in Snapshots 5 and 6 highlight the availability of information from the network server and the need to have a mechanism in place to protect the security of the server.
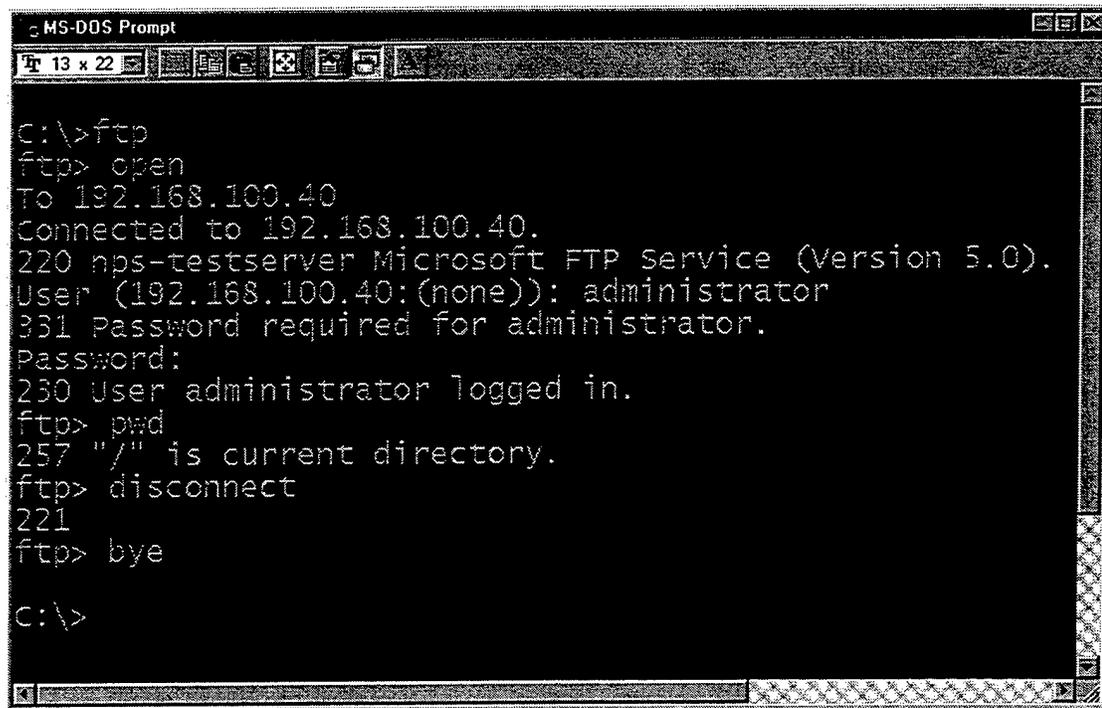
```
MS-DOS Prompt                                                    [_][□][X]
[Tr 13 x 22 ▾] [▣][▣][▣] [▣] [▣] [▣] [A]

C:\>ftp
ftp> open
To 192.168.100.40
Connected to 192.168.100.40.
220 nps-testserver Microsoft FTP Service (Version 5.0).
User (192.168.100.40:(none)): administrator
331 Password required for administrator.
Password:
230 User administrator logged in.
ftp> pwd
257 "/" is current directory.
ftp> disconnect
221
ftp> bye

C:\>
```

Snapshot 6 – Attack computer connected to server with FTP

2.   ID Systems Installed

Each of the three Intrusion Detection Systems was separately installed on the host computer. The same ports scan and FTP connection tests were run against all three ID systems. All of the various configurations of each ID system were selected and tested. To maintain continuity, nothing else was altered on the Window 2000 Server platform. The following are the results of the tests conducted.

a.   ZoneAlarm

ZoneAlarm was loaded and configured in each of its six possible security setting. Table 4 below highlights the results of the tests conducted:

39

| SECURITY SETTING LOCAL/INTERNET	PORT PROBE ALERTS REPORTED	SUPERSCAN RESULTS	FTP CONNECT
LOW/LOW	0	21 ports resolved	YES
LOW/MEDIUM	6	18 ports resolved	YES
MEDIUM/MEDIUM	6	18 ports resolved	YES
LOW/HIGH	MORE THAN 500	0 ports resolved	NO
MEDIUM/HIGH	MORE THAN 500	0 ports resolved	NO
HIGH/HIGH	MORE THAN 500	0 ports resolved	NO

The only configurations in which ZoneAlarm provided complete protection against the port scan utility were when the Internet security level was configured to HIGH. The Internet security setting was the only relevant factor due to the port scan test running from an external connection. In the Low and Medium Internet configuration ports were still available and an FTP connection was possible. The Internet Low setting revealed all 21 available ports and no alerts were generated in the logs. The Internet Medium setting effectively blocked access to 3 ports. These 3 ports (ports 135, 139 and 445) all perform file and print sharing services. The Internet Medium setting is designed to block Internet access to file and print sharing, so the test results validate the claims.

Snapshot 7 shows total protection from discovery when configured in Internet High. The host name was not detected and no open ports were revealed. On the host, ZoneAlarm provided pop-up alerts identifying the intrusion attempt, IP address and

port number of the attacking computer (Snapshots 8 and 9). The built-in alert log tracks

all activity and stores it in a text file.
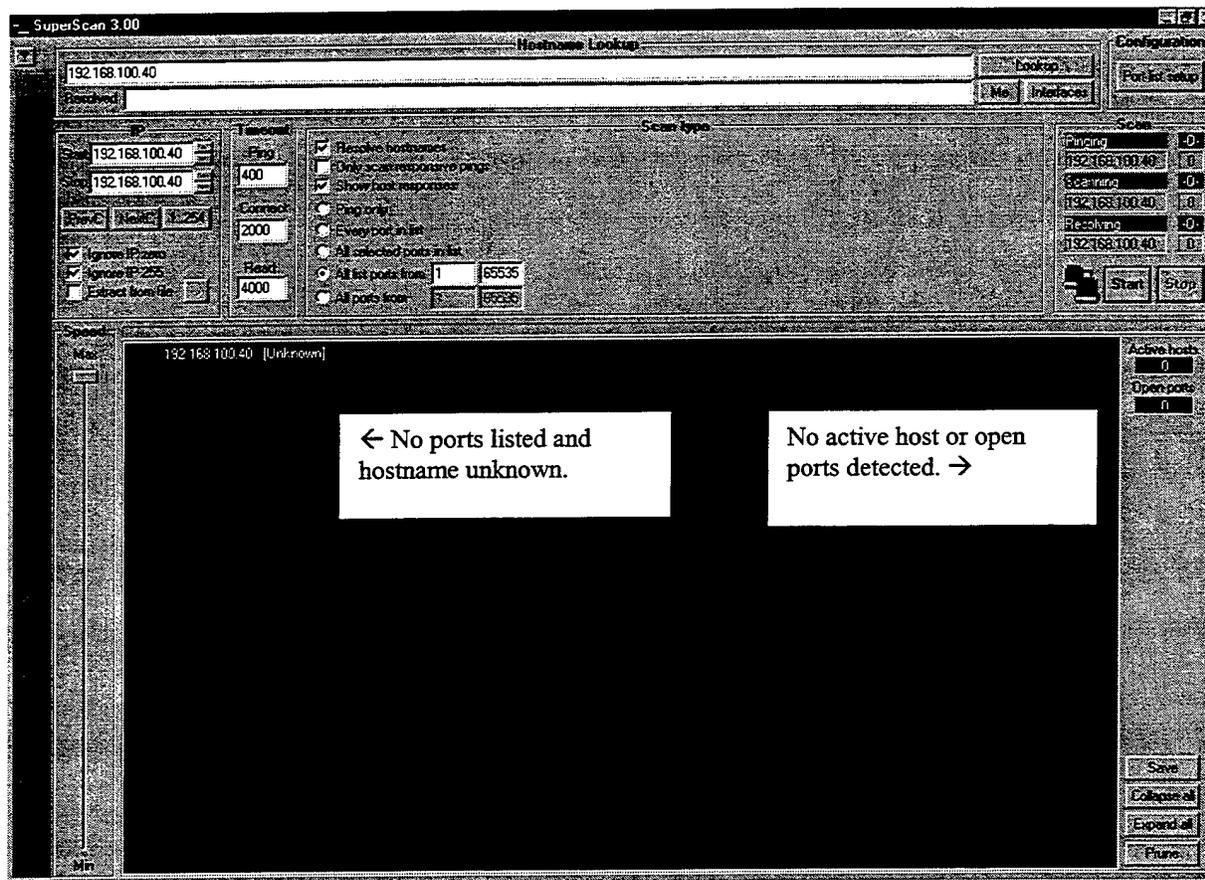
Snapshot 7 – SuperScan vs. Win2K Server with ZoneAlarm Internet High
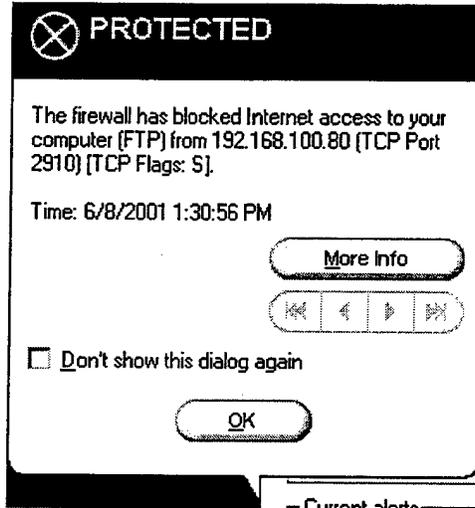
Snapshot 8 – ZoneAlarm Pop-up message
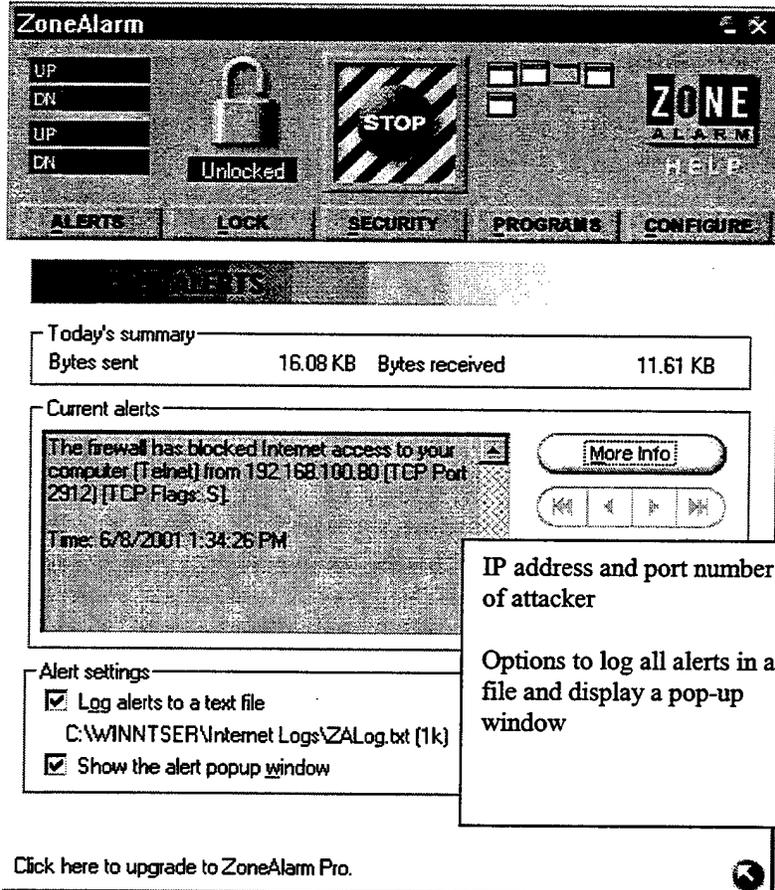
Snapshot 9 – ZoneAlarm Current Alert Message

b.   *BlackIce*

BlackICE was installed, configured and tested in each of its four security levels. In Cautious mode BlackICE blocks only unsolicited traffic that accesses operating system and network services; therefore, all but 2 ports (563 and 636) that do not access these services were blocked. The results are captured in Table 5 below:

SECURITY SETTING	PORT PROBE ALERTS REPORTED	SUPERSCAN RESULTS	FTP
TRUSTING	1953	21 PORTS RESOLVED	YES
CAUTIOUS	5,200	2 PORTS RESOLVED	NO
NERVOUS	11,727	0 PORTS RESOLVED	NO
PARANOID	16,000	0 PORTS RESOLVED	NO

In Paranoid mode, BlackICE blocked all the ports and concealed the hostname; however, the host IP address was still identified by SuperScan as seen in Snapshot 10.
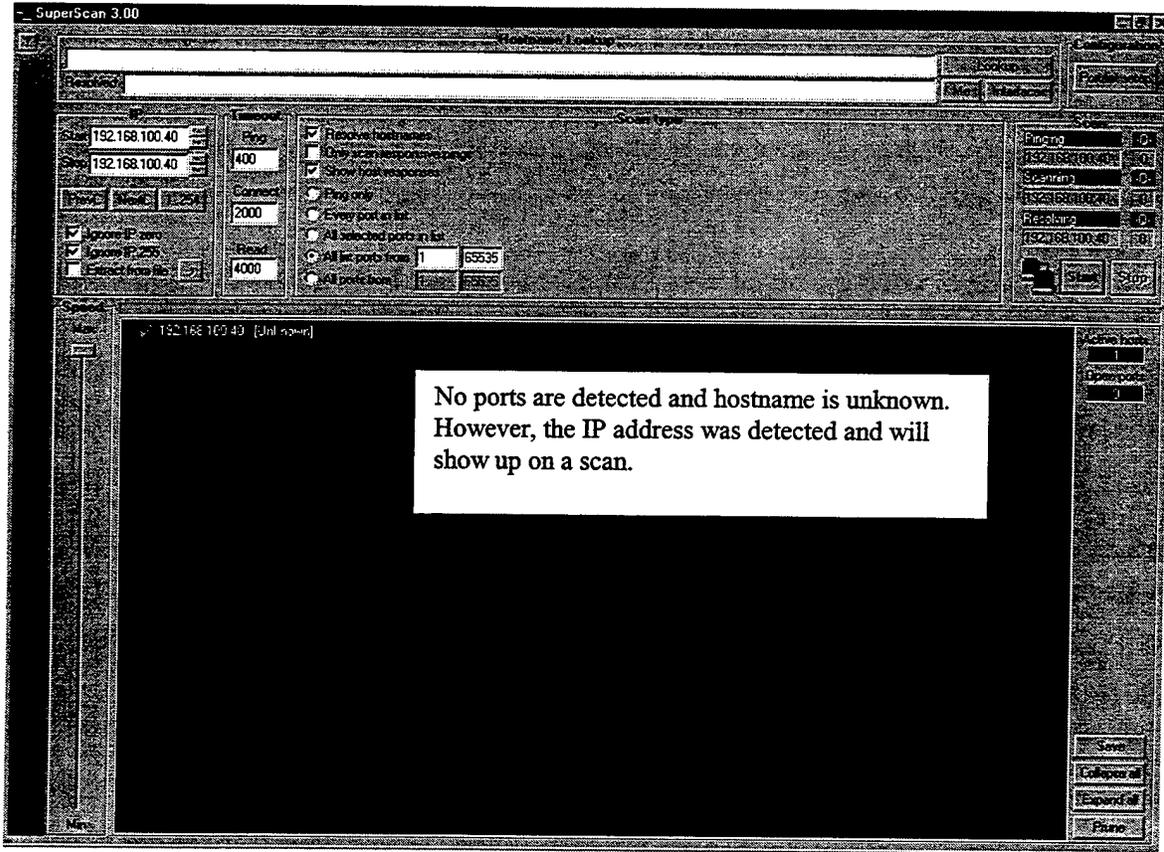
Snapshot 10 – SuperScan vs. Win2K with BlackICE in Paranoid Mode

Snapshot 11 below shows the reporting mechanism BlackICE uses to alert the host computer of the intrusion attempts. It properly identifies the intruder address, date, time, attack type and the number of attacks.

Time	Attack	Intruder	Count
06/01/01 12:13:46	TCP port scan	192.168.100.80	3326
06/01/01 12:13:45	TCP SYN flood	192.168.100.80	62
06/01/01 12:12:43	TCP port probe	192.168.100.80	322
06/01/01 12:12:32	TCP port scan	192.168.100.80	2628
06/01/01 12:12:32	TCP SYN flood	192.168.100.80	56
06/01/01 12:11:46	TCP port scan	192.168.100.80	1079
06/01/01 12:11:37	TCP SYN flood	192.168.100.80	10

[Scan] Attacker systematically scans through many ports on a system looking for those that are open.

Snapshot 11 – BlackICE Attack Log

c. *Sygate*

Sygate Personal Firewall was installed, configured and tested in Allow, Normal and Block modes. The results of the SuperScan test are listed in Table 6 below.

SECURITY LEVEL	PORT PROBE ALERTS REPORTED	SUPERSCAN RESULTS	FTP CONNECT
ALLOW ALL	0	21 PORTS RESOLVED	YES
NORMAL	1300	0 PORTS RESOLVED	NO
BLOCK ALL	0 (Everything shut down)	0 PORTS RESOLVED	NO

Similar to ZoneAlarm in its most secure mode, Sygate also blocked all information in its most secure mode as seen in Snapshot 12 below.
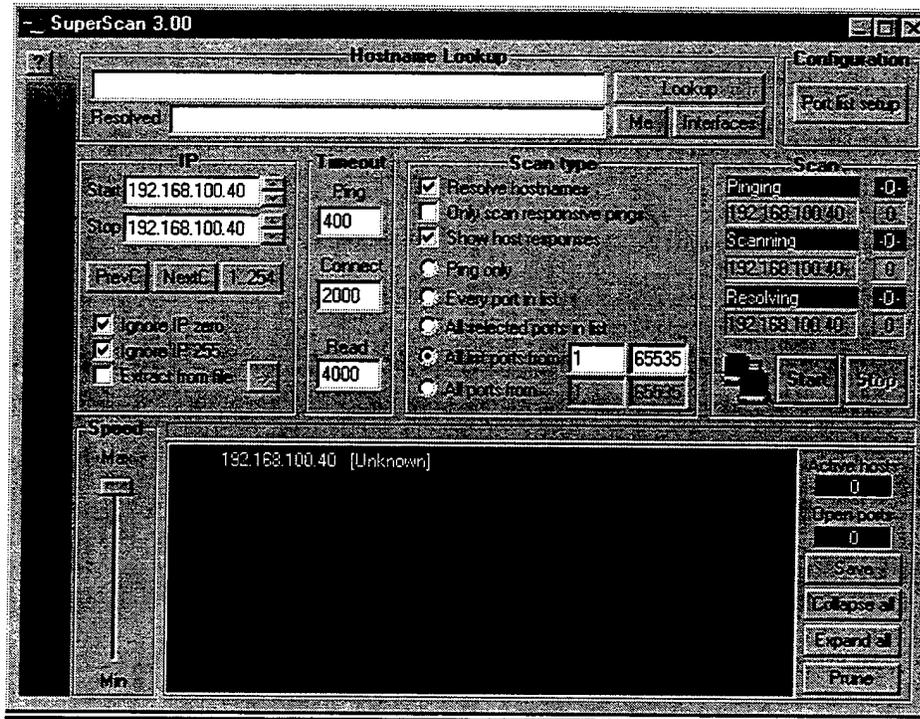
Snapshot 12 – SuperScan vs. Win2000 Server with Sygate Block All mode

Sygate's reporting utilities were extensive as seen in Snapshot 13. The program blocked all access to the host ports and correctly identified the intruder's IP address and port number.

Snapshot 13 – Sygate Traffic Log

In addition to a Traffic Log, Sygate offers a Packet Log (Snapshot 14) that identifies each packet and its contents.

Time	Remote Host	Remote Port	Local IP	Local Port	
06/08/2001 11:43:11	192.168.100.80	1341	192.168.100.40	192	
06/08/2001 11:43:11	192.168.100.80	1343	192.168.100.40	194	
06/08/2001 11:43:11	192.168.100.80	1342	192.168.100.40	193	
06/08/2001 11:43:11	192.168.100.80	1344	192.168.100.40	195	
06/08/2001 11:43:11	192.168.100.80	1345	192.168.100.40	196	
06/08/2001 11:43:11	192.168.100.80	1346	192.168.100.40	197	
06/08/2001 11:43:12	192.168.100.80	1348	192.168.100.40	199	
06/08/2001 11:43:12	192.168.100.80	1347	192.168.100.40	198	
06/08/2001 11:43:12	192.168.100.80	1349	192.168.100.40	200	
06/08/2001 11:43:12	192.168.100.80	1351	192.168.100.40	202	
06/08/2001 11:43:12	192.168.100.80	1350	192.168.100.40	201	
06/08/2001 11:43:12	192.168.100.80	1352	192.168.100.40	203	
06/08/2001 11:43:12	192.168.100.80	1353	192.168.100.40	204	
06/08/2001 11:43:12	192.168.100.80	1355	192.168.100.40	206	
06/08/2001 11:43:12	192.168.100.80	1354	192.168.100.40	205	
06/08/2001 11:43:12	192.168.100.80	1356	192.168.100.40	207	

Packet Decode:

```
Transmission Control Protocol (TCP)
        Source port: 1349
        Destination port: 200
        Sequence number: 88939596
        Acknowledgment number: 0
        Header length: 28
        Flags:
```

Packet Dump:

```
0000:   00 50 04 D4 65 2A 00 E0 : 29 0E 3B 7E C
0010:   00 30 B3 02 40 00 80 06 : FD FB C0 A8 E
0020:   64 28 05 45 00 C8 05 4D : 1C 4C 00 00 C
0030:   20 00 F1 AF 00 00 02 04 : 05 B4 01 01 C
```

Snapshot 14 – Sygate Packet Log

48

B. FTP RESULTS

FTP was used to verify the ID systems were actually protecting ports and not simply making them invisible to scans. FTP was not able to establish a connection with any of the ID systems in their more secure modes. Snapshot 4 below shows the failed connection that resulted from an FTP with the server when an ID system was installed. 10060 is a FTP error message that means a connection could not be established. The ID systems not only hide all ports, but close them down as well.

```
C:\>ftp
ftp> open
To 192.168.100.40
> ftp: connect :10060
ftp> disconnect
Not connected.
ftp> bye

C:\>
```

Snapshot 15 – FTP reaction vs. Win2K Server with ZoneAlarm, BlackICE and Sygate

C. PING RESULTS

The ping command was used to determine if the ID system was hiding the host IP address when SuperScan reported no active host found as indicated by the red "X" next to the IP address in the SuperScan windows included above. It was determined that Ping did not receive a response back from the server when the ID systems were configured such that the no active host was found, i.e. ZoneAlarm in High Internet security setting and Sygate in Normal and Block All modes.
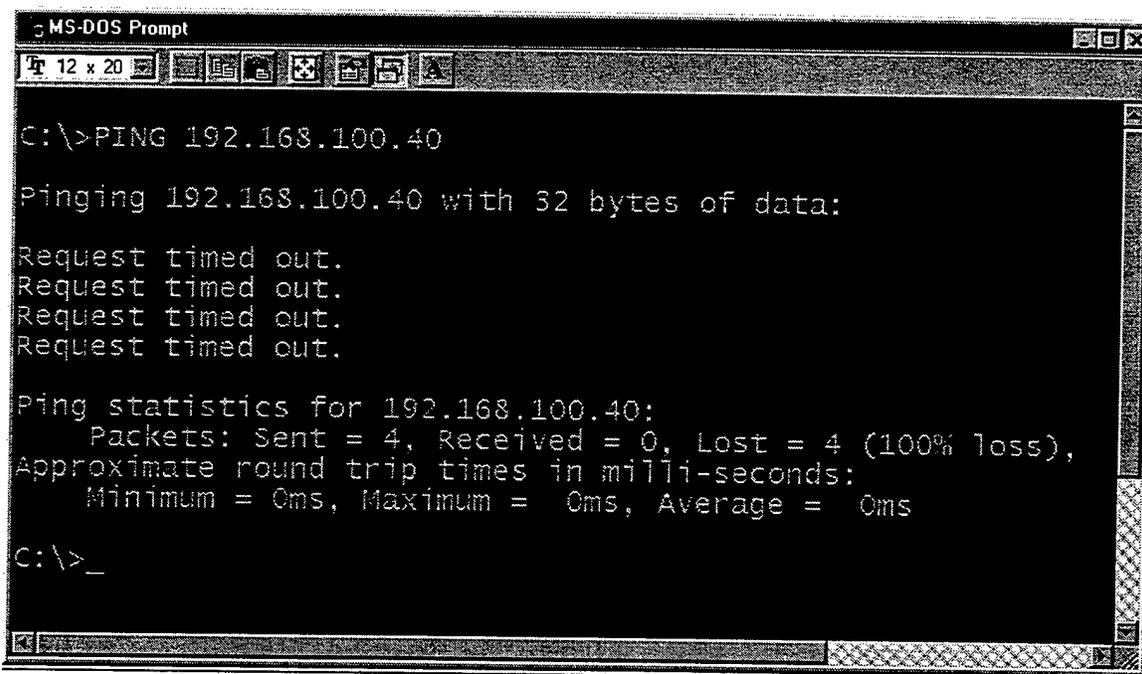
```
MS-DOS Prompt
12 x 20

C:\>PING 192.168.100.40

Pinging 192.168.100.40 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.100.40:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

Snapshot 16 – Ping Results against ID System configurations that did not detect an active host IP address

D.   ADDITIONAL TEST DATA

Windows 2000 Server provides the network administrator with the flexibility to modify the available port listing. Test data was collected to determine the effectiveness of the TCP/IP filtering utility. Snapshot 17 indicates that only ports 21 and 80 were enabled. Snapshot 18 reveals that even with no ID system installed all ports were successfully blocked except ports 21 and 80. Subsequently, tests were conducted with each ID system running to determine if the ID system would run more efficiently or still report a port scan of the ports that were disabled using TCP/IP filtering. All 3 ID systems recognized and reported port scan alerts identical to the initial tests run with all ports open. There appeared to be no benefit to the ID systems to restrict access to any specific ports.
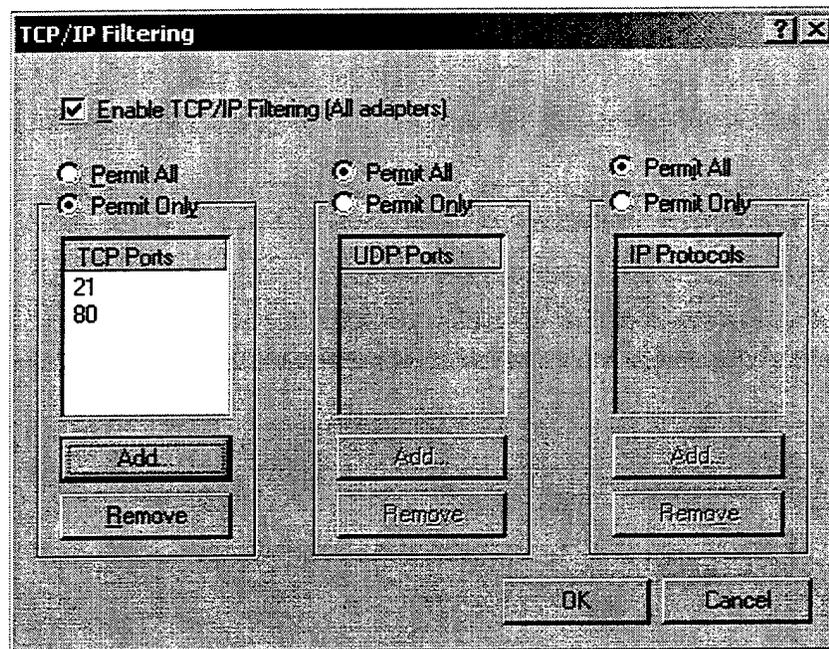
Snapshot 17 – Win2K TCP/IP Filtering Menu
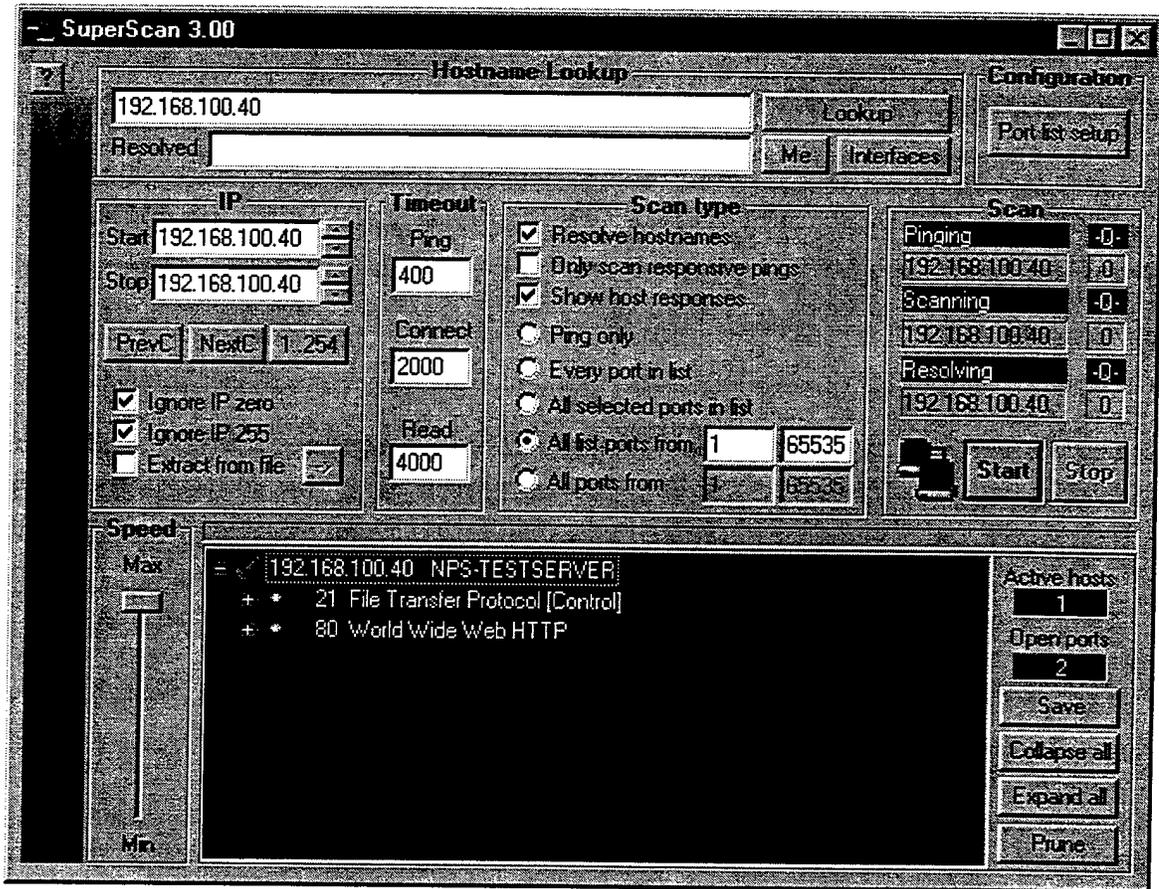
Snapshot 18 – SuperScan vs. Win2K with only ports 21 & 80 open

The TCP/IP filtering utility is a helpful tool for knowledgeable network administrator who has a clear understanding of the ports necessary for a server to perform its operations. However, restricted port access does not circumvent the need for a quality ID system. The ID system will still generate valuable alerts notifying the user and administrator of port scans and possible intrusion attempts in addition to providing the ability to trace the source of the attack. In the absence of a host-based ID system, port restrictions would be recommended.

E. SUMMARY OF DATA COLLECTED

Table 7 below depicts the overall performance of each ID system in its various

configurations. Explanation of table contents:

- Column one: name of ID system installed
- Column two: configuration of ID system
- Column three: was host IP address identified
- Column four: was hostname identified
- Column five: number of open ports detected
- Column six: could FTP connection be established
- Column seven: was a ping response received

IDS	IDS MODE	ID HOST	RESOLVE HOSTNAME	# OF OPEN PORTS	FTP ACCESS	PING RETURN
NONE	N/A	YES	YES	21	YES	YES
ZONEALARM	LOW/LOW	YES	YES	21	YES	YES
"	LOW/MED	YES	NO	18	YES	YES
"	MED/MED	YES	NO	18	YES	YES
"	LOW/HIGH	NO	NO	0	NO	NO
"	MED/HIGH	NO	NO	0	NO	NO
"	HIGH/HIGH	NO	NO	0	NO	NO
BLACKICE	TRUSTING	YES	N/A*	21	YES	YES
"	CAUTIOUS	YES	N/A*	2	NO	YES
"	NERVOUS	YES	N/A*	0	NO	YES
"	PARANOID	YES	N/A*	0	NO	YES
* USER SPECIFIED, SEE BLACKICE WRITEUP.						
SYGATE	ALLOW	YES	YES	21	YES	YES
"	NORMAL	NO	YES	0	NO	NO
"	BLOCK	NO	NO	0	NO	NO

F. COMPARISON OF ID SYSTEMS

The previous snapshots and tables help to illustrate that all three Host-based Intrusion Detection Systems perform well in preventing a port scan run against a Windows 2000 Server platform. Properly configured, they also successfully prevented a direct connection through FTP port 21. Further analysis of these three programs indicates that differences do exist.

One significant difference, not highlighted in the test data since only inbound traffic was reported, involves the ID systems ability to control and restrict outbound traffic. ZoneAlarm and Sygate use a "rules-based approach", meaning that the user is asked to allow or disallow all outbound program connections. BlackICE does not employ this methodology and therefore lacks this feature. This is a significant pitfall for BlackICE because the potential exists to download utilities that may contain Trojan horse programs, such as the "Back Orifice" Trojan, with any client computer that has Internet access using an application proxy and a firewall. A Trojan of this nature can infest itself within the machine and initiated (outbound) traffic from the host to connect to Internet Relay Chat (IRC) servers and such. If the harmful program is initiated from the host then BlackICE will not provide protection and the system is vulnerable to widespread attacks. The danger of this makes it imperative that a good host-based ID system be complete with outgoing traffic monitoring as well as screening all incoming traffic.

BlackICE also lacked the ability to block ping replies. Both ZoneAlarm and Sygate do not reply to ping attempts in their more secure modes. At first glance this may not seem significant because a ping flood cannot be stopped, and if a specific IP address is targeted, this feature has no benefit. However, if an IP address is not widely known and is not specifically targeted, this feature is key. By not replying to a ping, the computer is basically in stealth mode, and an attacker scanning a range of IP addresses will not detect the machine. This feature can prevent an attacker from ever launching an attack.

All three ID systems offer the benefit of being able to back trace a suspicious packet. This feature provides system administrators the ability to identify and report the source of illegal activity to the proper authorities. Although most attackers will take measures to guarantee their anonymity, it is still a useful feature for reporting intrusion attempts. It is critical to protect networks from intrusions, but it is also important, to identify if possible, the source of the intrusion attempts.

Analysis of the evaluation criteria key elements outlined in Chapter 3 follows:

- Effectiveness of intrusion detection – All three programs performed adequately at detecting, reporting and preventing intrusions.
- Effectiveness of security protection – All three programs provided good protection when configured in their most secure mode (Internet High for ZoneAlarm, Paranoid for BlackICE and Block All for Sygate). Sygate blocks all inbound and outbound communications in this configuration isolating the system. ZoneAlarm and BlackICE both allowed communications to continue while maintaining a tight security posture. In more promiscuous configurations the protection suffered. BlackICE revealed 2 open ports in

Nervous mode, 18 open ports in Cautious mode and 21 open ports in Trusting mode. Sygate blocked all ports but allowed the host name to be resolved in Normal mode. In Allow mode, Sygate correctly logged all the port scan activity but revealed all open ports. ZoneAlarm revealed open ports in both Internet Medium and Internet Low modes.

- Effectiveness of reaction – All three programs performed sufficiently by quickly and effectively blocking port scans and denying access to connection attempts from FTP. However, BlackICE and Sygate lack a pop-up window alerting the user to the attack. Users must keep their eye on the system tray to look for a "blinking" icon.

- User interface – All three systems were easy to install and configure. BlackICE, based on the fact that it doesn't employ rule-based monitoring, was extremely user friendly and hands off. ZoneAlarm and Sygate have numerous pop-up screens that require the user to allow or disallow communications.

Based on the results of tests conducted and the interaction with each of the ID systems, Table 8 below shows a breakdown of how each system compares. Each feature is graded using a scale of 1 – 10, with 10 being most favorable.

ID SYSTEM	ZONEALARM	BLACKICE	SYGATE
EASE OF INSTALLATION & USE	8	9	8
CONFIGURABILITY	9	8	9
OVERALL EFFECTIVENESS	9	8	9
USER INTERFACE	9	7	8

Although, none of the ID systems evaluated satisfy all the expectations of what an ideal ID system should provide. Each system did provide obvious improvements over an unprotected system and they all had strengths that were unique to their program. Sygate offered password protection capability so that an administrator could install the program on a client computer and prevent the user from changing the security settings. BlackICE was the least intrusive and offered the widest selection of security profiles. However, ZoneAlarm's ability to control outbound traffic, hide the IP address from scans and display pop-up window alerts made it the best of the three systems tested.

THIS PAGE INTENTIONALLY LEFT BLANK

V.   SUMMARY AND CONCLUSION

A.   SUMMARY

Secure systems are essential to ensure effective information operations and protect network security. A high percentage of crackers are opportunists who run scanners to check massive numbers of hosts for remote system vulnerabilities. A typical DoD organization may have 5 external web servers, 2 external mail servers, and a firewall protecting the network. Crackers wanting to gain access to the organization's network will commonly target these servers. Servers located outside the firewall must exchange information with servers within the network firewall. This provides attackers with an enticing target of opportunity to gain access to the internal network and jeopardize the security of the entire system. Utilizing a host-based ID system on all government network computers located outside the firewall would provide an additional level of security and a method of real-time monitoring.

In addition, using a defense-in-depth approach, host-based ID systems would provide system administrators with a valuable utility if installed on all client computers throughout the network. Similar to the common practice of utilizing anti-virus software as a security precaution to protect networks, a properly designed and configured host-based ID system should be implemented to add additional safeguards to government networks. The effective deployment of host-based ID systems would consist of individual systems installed on each machine throughout a network with a centralized

reporting mechanism to one location. This would enable network administrators to efficiently monitor the entire network for malicious activity.

B.   CONCLUSION

Although the ID systems tested offer significant benefits to network security, none of them can satisfy all the requirements of an ideal program for government use. However, with more than 150 commercial vendors currently in the industry, a system can be designed to meet the needs of protecting government networks. As a result of this research the following conclusions have been reached. First and foremost, the Host-based ID system designed for the government must come from a trusted vendor. The risks are too great to install software on every government system that could contain potentially hazardous code. The following is a list of recommendations to be considered in determining the design requirements for an ideal host-based ID system:

- Impose minimal overhead on the system
- Observe deviations from normal behavior, yet be able to adapt to changes in the system profile that occur over time
- Run on client computers but report to a central monitoring location
- Have password protection to prevent individuals from changing the configuration once it is set-up
- Block all unauthorized incoming and outgoing traffic
- Accurate signature database, with timely updates
- Be extremely difficult to fool
- Be able to monitor itself to recognize if it has been subverted
- Allow its internal working to be examined from the outside
- Be able to back trace any intrusion attempts to help identify intruders

As network security concerns continue to increase, the need for additional security measures is paramount. The tests conducted have adequately supported that host-based ID systems can help facilitate such security enhancements. Host-based ID systems can be utilized to increase network security in two manners: they can provide a shield of protection on the susceptible servers located outside the network firewall, and they can work in conjunction with the network ID system by providing an additional layer of protection on client workstations within the network firewall. Host-based ID systems are relatively inexpensive and easy to operate, similar to anti-virus programs, and can provide the overall defense-in-depth network security architecture needed to safeguard today's systems.

> A security vulnerability exists that affects every computer system in the world -- regardless of hardware or software. This vulnerability extends worldwide; it's massive, severe, and just plain scary. Despite years of modifications and real-time testing, no patch is currently available. First discovered in a place known as "The Garden of Eden," a serpent convinced a woman called Eve that eating an apple would provide her knowledge of good and evil. While knowledge of good and evil was indeed imparted, differentiating between the two was apparently not part of the package. [Ref 9]

Vulnerabilities may always exist, but they can be made difficult to find. Knowledge of an impending attack gives the defender the advantage. Host-based ID systems can accomplish both tasks.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Associated Press, The New York Times, September 11, 2000.

2. Brunker, Mike, MSNBC, URL: http://www.msnbc.com (17 March 2000).

3. Axent Technologies, Inc, *"Everything You Need to Know About Intrusion Detection."* Axent.com, URL: http://www.axent.com (November 1999).

4. Scambray, Joel, *"IDS: How they work and when they won't."* Inforworld.com, URL: http://archive.infoworld.com/pageone/gif/980504how.gif (4 May 1998).

5. Cassi, Richard, SAIC, *"What is a honeypot and how is it used?"*, Sans.org, URL: http://www.sans.org/newlook/resources/IDFAQ/honeypot.htm (2001).

6. Zone Labs, Inc. Homepage, URL: http://www.zonelabs.com (May 2001).

7. Network Ice Corporation, Homepage, URL: http://www.networkice.com (1998-2000).

8. Sygate Technologies, Inc., Homepage, URL: http://www.sygate.com (1997-2001).

9. Fennelly, Carole, & Dyson, Jay, D., *"Advisory: Wetware v2001 Still Vulnerable to Common Attacks"*, URL: http://www.ph.utexas.edu/security/ (3 May 2001).

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Allen, Julia; Christie, Alan, Fithen, William; McHugh, John; Pickel, Jed; Stoner, Ed.
Tech Report: *State of the Practice of Intrusion Detection Technologies*. URL:
http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstra
ct.html

Boran, Sean, "Personal Firewalls/Intrusion Detection Systems." *Securityportal.com,*
URL: http://securityportal.com/articles/pf_main20001023.html (23 October
2000).

Cohen, Fred; Phillips, Cynthia; Swiler, Laura Painton; Gaylor, Timothy; Leary, Patricia;
Rupley, Fran; Isler, Richard; and Dart, Eli; *A Preliminary Classification Scheme
for Information System Threats, Attacks, and Defenses; A Cause and Effect
Model; and Some Analysis Based on That Model*; Sandia National Laboratories,
September, 1998.

Crosbie, Mark; Spafford, Gene; *Active Defense of a Computer System using Autonomous
Agents*; Technical Report No 95-008, COAST Group, Dept. of Computer
Sciences, Purdue University, February 15, 1995.

Crosbie, Mark; Spafford, Gene; *Defending a Computer System using Autonomous
Agents*; Technical Report No 95-022, COAST Group, Dept. of Computer
Sciences, Purdue University, March 11, 1994.

Heikkila, Pia, "*FBI report shows cybercrime hits nine out of ten*", Silicon.com, URL:
http://www.silicon.com/bin/bladerunner?30REQEVENT=&REQAUTH=21046&
14001REQSUB=REQINT1=37969 (8 June 2000).

Internet Security Systems White Paper. *Network vs. Host-based Intrusion Detection: A
Guide to Intrusion Detection Technology*. URL:
http://documents.iss.net/whitepapers/nvh_ids.pdf

Kumar, Sandeep; Spafford, Eugene H.; *An Application of Pattern Matching in Intrusion
Detection*; Technical Report CSD-TR-94-013, The COAST Group, Dept. of
Computer Sciences, Purdue University, June 17, 1994.

McHugh, John; Christie, Alan; Allen, Julia. *Defending Yourself: The Role of Intrusion
Detection Systems*. URL:
http://www.computer.org/software/so2000/pdf/s5042.pdf.

Meeks, Brock N. *Hackers hit 155 government sites*. URL:
http://www.msnbc.com/news/555308.asp

Network Ice Corporation, Homepage, URL: http://www.networkice.com (1998-2000).

Parker, Donn B.; *Fighting Computer Crime*; Wiley Computer Publishing, New York, 1998.

Pfleeger, Charles P.; *Security in Computing, Second Edition*; Prentice Hall PTR, Upper Saddle River, NJ, 1996.

Rosenblatt, Kenneth S.; *High Technology Crime;* KSK Publications, San Jose, 1995.

Scambray, Joel; McClure, Stuart; Kurtz, George; *Hacking Exposed -- Network Security Secrets and Solutions, Second Edition,* McGraw-Hill Publishing, Berkeley, CA, 2001.

Scambray, Joel, *"Network Intrusion-Detection Solutions"*, Inforworld.com, URL: http://archive.infoworld.com/cgi-bin/displayTC.pl?/980504sb6-how.htm (4 May 1998).

Sygate Technologies, Inc., *"Enforcing Rule-Based Security."*, Sygate.com, URL: http://www.sygate.com (May 2001).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
    8725 John J. Kingman Road, Ste 0944
    Fort Belvoir, VA 22060-6218

2. Dudley Knox Library.. 2
    Naval Postgraduate School
    411 Dyer Road
    Monterey, California 93943-5101

3. Professor Richard Harkins.. 1
    Code PH/Hr
    Naval Postgraduate School
    Monterey, CA 93943

4. Professor Dan Warren 1
    Code CS/Wd
    Naval Postgraduate School
    Monterey, CA 93943

5. LT Ron Yun.. 1
    3219 Morning Trail
    San Antonio, TX 78247

6. LT Steve Vozzola. 2
    2500 Hollywood Blvd. #202
    Hollywood, FL 33020