GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

DESIGNING AND IMPLEMENTING AN EFFECTIVE INFORMATION SECURITY PROGRAM: PROTECTING THE DATA ASSETS OF INDIVIDUALS, SMALL AND LARGE BUSINESSES

GSEC Certification

Practical Assignment Version 1.4b

Option 1

© SANS Institute 2004, Author retains full rights.

Submitted March 24, 2004

Lee A. Kadel

Genoa City, Wisconsin

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

Attacks against computers, in both home and business environments, have grown steadily over the past several years. According to the U.S. Federal Bureau of Investigation, "…worldwide digital attacks reached an all-time high of nearly 20,000 in January, causing more than $8 billion in damages." (Mueller, 2003). Incidents of identity theft – the act of impersonating another person for profit or gain – are growing at an alarming rate. Identity theft is considered one of the fastest growing crimes in the United States, affecting an estimated 900,000 new victims every year (Pollock & May, 2002).

The need for information security should be apparent, but the knowledge and ability to design and implement an effective security program requires substantial research, and often a great investment of time and resources. To compound the problem, many home users lack the knowledge and experience to identify and understand their risk. Moreover, while small businesses may understand, they either do not grasp the severity of the problem, or lack the resources to rectify it.

While focusing primarily on the implications for individuals, this study presents a systematic approach to building an information security plan that can be tailored to meet the needs of both small and large businesses.

In researching the subject, several points become apparent:

1. Incidents of computer related crime are steadily rising.
2. Attacks against computers, in both the personal and business arenas, are becoming more sophisticated.
3. Software companies, including application and operating system vendors, are unable to keep up with the rapidly growing and ever-changing threat.
4. A properly designed and implemented security program can significantly reduce the exposure to these threats, and limit the damage caused in the event of an attack.
5. For a security program to remain effective, it must be reviewed and maintained on a regular basis.

The approach to information security presented in this paper will guide the user through the steps necessary to develop an information security plan, tailored to their individual needs. After describing several types and methods of attack, the reader is shown how to classify data and systems, and analyze risk..

The study then presents information on how to select appropriate counter-measures, including basic implementation guidelines. Finally, the legal and technical implications for individuals and businesses, both small and large, are examined.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

Statement of the Problem	1
Purpose of the Study	1
Importance of the Study	1
Scope of the Study	2
Rationale of the Study	2
Definition of Terms	3

CHAPTER 2 REVIEW OF RELATED LITERATURE

Examining the Need for Information Security	6
Investigating the Tools of the Hackers' Trade	6
Assessing Risk, and Developing Policy	8
Researching Appropriate Counter-measures	9

CHAPTER 3 METHODOLOGY

Approach	10
Data Gathering Method	11
Database of Study	11
Validity of Data	12
Originality and Limitations of Data	12

CHAPTER 4 DATA ANALYSIS

Security Defined	13
Data Classification and System Criticality	14
Common Threats	17
Risk Analysis	19
Security Policy	22
Passwords	24
Anti-Virus	25
Firewalls and Intrusion Detection	26
Vulnerability Scanning	27
Backups, UPS, and Encryption	33
Configuration and Patch Management	35

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS

Summary	36
Implications for Individuals	39
Implications for Business	39
Conclusion	40

BIBLIOGRAPHY 41

APPENDIX A Security Resources 42

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

LIST OF TABLES AND FIGURES

Table 1	Asset Inventory	14
Table 2	Data Class	15
Table 3	Confidentiality	16
Table 4	Asset Valuation	16
Table 5	Threat Matrix	18
Table 6	Vulnerability	19
Table 7	Risk Assessment by Value	20
Table 8	Risk Assessment by Rank	20
Table 9	Completed Risk Analysis	21
Table 10	Port Numbers	28

Figure 1	NeWT Scanner	29
Figure 2	GFI LANguard Scanner	29
Figure 3	LANguard Report	30
Figure 4	NeWT Report	31
Figure 5	Cain & Able Password Scan	32
Figure 6	Windows Backup Wizard	33

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CHAPTER 1 INTRODUCTION

Statement of the Problem

As computers become more commonplace in homes, and more necessary in businesses of all types, the incidence of information security related breaches has grown accordingly. Where once only large corporate environments were susceptible to attack, increasingly individuals and small business networks are being targeted. It is not, however, only from outside that these attacks originate; consider the following scenario:

> "A man comes home from work and sits down at the family computer to update his checkbook. After double-clicking on the program icon, he receives a message that his data file cannot be found; further searching reveals that the file no longer exists. Asking his wife if she knows anything about the problem, he is told, "The kids were playing around on the computer earlier today." Interrogation of his children reveals that they had deleted his checkbook file because they, "…needed more space on the hard drive for games."

While this illustration is not based on any known incident, it is certainly a plausible situation, and demonstrates the need for information security even at the individual level. What can be done to mitigate the risk of an information security incident, and how should people approach the task?

Purpose of the Study

This reason for this study is to identify the basic steps, processes and procedures necessary to design and implement an effective information security program – one that can be tailored to the needs of individuals, small and large businesses. The research is intended not only to support the premise that an information security program is a necessity in any computing environment, but also to offer practical advice on the design and implementation of such a program.

It is not the intent of this paper to endorse any particular product or technology, only to offer suggestions and guidance to computer users who are concerned about their security and privacy as related to computer use.

Importance of the Study

With the increase in computer related crimes in recent years, and particularly the rise in incidence of 'identity theft', it is imperative that people begin to take the proper precautions regarding their use of computers – particularly if they are connected to the Internet. Too often, information security is an afterthought, or is ignored altogether. This is especially true for individuals – those with a single computer, or a small home network – although many small businesses still fail to understand the importance of an information security plan in their business strategy. This study, and its supporting research, will educate the reader on the need for information security in general, assist them in determining their own risk factors and resulting information security needs, and lay the groundwork for building an information security plan to address those needs.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Scope of the Study

This study will cover three main areas:

1. Identification of security weaknesses
2. Assessment of risk associated with those weaknesses
3. Development of a plan to reduce or eliminate that risk

These three points will be dealt with in a general manner, as opposed to an in-depth treatment of every exploit, or of every possible solution.

First, in order to delineate between the varied needs of individuals and businesses, it is important to keep the discussion on a level where both environments can be examined equally.

Second, detailed research and studies have been done on most, if not all, of these weaknesses and exploits – it would be redundant to delve too deeply into those details in this study. Where applicable, these other more detailed studies are included by reference. For those readers who wish to do additional research, or require more detailed information, a list of security resources is included in Appendix A.

Actual implementation of an information security plan is likewise treated in a general manner. The disparities between environments, and even between individual computers, put detailed technical discussions outside the scope of this study.

This study focuses on the Microsoft Windows® computing environment. While the processes and procedures identified herein are, in many cases, also valid for other operating systems and environments, the Microsoft family of operating systems and applications is the system most widely used in business, and is all but exclusive in the home environment, making it a common factor upon which to draw comparisons and develop processes. Therefore, discussions of Unix, Linux, Macintosh, and other operating systems and environments will not be included unless the technology used to propagate or prevent an attack is based on one of these systems, in which case the system will be included by reference only. Again, for those wishing to do further research into these, and other operating systems and environments, a list of security vendors is included in Appendix A.

This paper will not discuss the relative strengths and weaknesses of individual pieces of technology or of multiple methodologies. Where a formula, process, or method is recognized as the preferred or most common, sufficient documentation to support that claim will be presented; alternatives, if they exist, will be included.

This study will result in a treatment of the subject sufficient for an individual or businessperson to make an informed decision on whether to pursue an information security program, and how to proceed with the planning and design of that program. Guidance will be given to direct the reader to the appropriate resources to complete and implement their plan.

Rationale of the Study

This study is based on the hypothesis that breaches in information security can be reduced or controlled by implementing proper security measures, and further that the deficiency of these security measures on many systems today is due to a general lack of education and understanding of proper security procedures. Even for those who understand the need for information security, the volume – and subsequent disparity – of available information is at times overwhelming.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This study will serve to bridge that education gap and create a common baseline for further discussion and investigation, while imparting a basic guideline for planning, creating, and implementing an effective security program suitable for the environment in which it is to be deployed.

Definition of Terms

In order to provide a common understanding of the terms and phrases used in information security, and in an effort to adhere to industry standard terminology, many of the following terms and definitions were taken from the SANS Institute website (SANS Institute, 2003)

Availability: The need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.
Authentication: The process of confirming the correctness of the claimed identity.
Authenticity: The validity and conformance of the original information.
Computer Network: A collection of host computers together with the sub-network or inter-network through which they can exchange data.
Confidentiality: The need to ensure that information is disclosed only to those who are authorized to view it.
Cost Benefit Analysis: A comparison of the cost of implementing countermeasures with the value of the reduced risk.
Cryptography: The process of garbling a message in such a way that anyone who intercepts the message cannot understand it.
Data Custodian: The entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.
Data Owner: The entity having responsibility and authority for the data.
Defense In-Depth: The approach of using multiple layers of security to guard against failure of a single security component.
Denial of Service: The prevention of authorized access to a system resource or the delaying of system operations and functions.
Dictionary Attack: An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.
Digital Signature: A hash of a message that uniquely identifies the sender of the message and proves the message has not changed since transmission.
Disaster Recovery Plan (DRP): The process of recovery of IT systems in the event of a disruption or disaster.
Domain: 1) A sphere of knowledge, or a collection of facts about some program entities or 2) a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or hosts. In Windows NT and Windows 2000, a domain is collection of computers on a network that share a common user database and security policy. A domain is administered as a unit with common rules and procedures by the domain administrator. The user need only log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Domain Name: A domain name locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.
Domain Name System (DNS): The way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.
Due Diligence: The requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.
Encryption: Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
Firewall: A network security device that ensures that all communications attempting to cross it meet an organization's security policy. Firewalls track and control communications, deciding whether to allow, reject or encrypt communications.
Hardening: The process of identifying and fixing vulnerabilities on a computer system.
Hijack Attack: A form of active wiretapping in which the attacker seizes control of a previously established communication association.
Honey pot: Programs that simulate one or more network services that you designate on your computer's ports. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.
Incident: An adverse network event in an information system or network, or the threat of the occurrence of such an event.
Incident Handling: An action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six-step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
Integrity: The need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
Internet: Multiple separate networks connected together.
Intranet: A computer network, usually based on Internet technology, that an organization uses for its own internal purposes, and that is closed to outsiders.
Intrusion Detection System (IDS): A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).
Least Privilege: The principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

NIST: The National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.
Network Address Translation (NAT): The translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.
Penetration: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.
Port: The endpoint of a communication stream, identified by a number. Only one process per machine can listen on the same port number.
Proxy: A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service.
Registry: The Registry in Windows® operating systems in the central set of settings and information required to run the Windows computer.
Risk Assessment: The process by which risks are identified and the impact of those risks determined.
Security Policy: A set of rules and practices that specifies or regulate how and why a system or organization provides security services to protect sensitive and critical system resources.
SYN Flood: A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.
Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
Trojan (a.k.a. Trojan Horse): A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Virtual Private Network (VPN): A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.
Virus: A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting – i.e., inserting a copy of itself into and becoming part of – another program.
Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CHAPTER 2 REVIEW OF RELATED LITERATURE

Examining the Need for Information Security

According to the CERT® Coordination Center (a.k.a. CERT/CC), located in the federally funded Software Engineering Institute at Carnegie Mellon University, "Your home computer is a popular target for intruders. Why? Because intruders want what you've stored there. They look for credit card numbers, bank account information, and anything else they can find. By stealing that information, intruders can use your money to buy themselves goods and services." (CERT/CC, 2002) This statement, while appearing self-obvious, is often overlooked or ignored by the general computing population. It seems to be a common belief that, "…it won't happen to me."

In the document *Before You Connect a New Computer to the Internet*, CERT/CC also states, "In recent months, we have observed a trend toward exploitation of new or otherwise unprotected computers in increasingly shorter periods of time. This problem is exacerbated by a number of issues, including:

- Many computers' default configurations are insecure.
- New security vulnerabilities may have been discovered between the time the computer was built and configured by the manufacturer and the user setting up the computer for the first time.
- When upgrading software from commercially packaged media (e.g., CD-ROM, DVD-ROM), new vulnerabilities may have been discovered since the disc was manufactured.
- Attackers know the common broadband and dial-up IP address ranges, and scan them regularly.
- Numerous worms are already circulating on the Internet continuously scanning for new computers to exploit.

As a result, the average time-to-exploitation on some networks for an unprotected computer is measured in minutes. This is especially true in the address ranges used by cable modem, DSL, and dial-up providers." (CERT/CC, 2001)

High speed Internet connections are fast becoming the de-facto standard for home users – if a computer owner has a telephone or cable television, they very likely have access to a high speed Internet connection. The problem with these connections is that they are always on; if the computer is powered on, it is connected to the Internet. This creates a situation where attackers can gain access to a computer even when the owner is not using it, or even when he/she is not at home. Dialup connections, which require a manual connection, are only slightly less vulnerable – once a connection is established to the Internet, the computer is visible to an attacker.

Investigating the Tools of the Hackers Trade

There are many programs, utilities, and other tools publicly available that an attacker may use to break into a computer. Many of these tools have been written by other hackers and are available on the Internet free of charge. An Internet search for the words 'free hacker tools' resulted in a list of thousands of links to websites containing freeware utilities. While publicly touted as 'security tools', these utilities are often used by attackers to gain access to, or exploit a computer system.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not all attacks are directed at an individual computer. Viruses, for example, are written and directed at the computing community in general. A virus's purpose is most often not to damage or destroy data, but simply to replicate by attaching itself to files, thereby infecting other computers. Increasingly, viruses are used to deploy other, more invasive, tools like trojan horses.

In the book *Maximum Security* (Anonymous, 2001), the author defines and explains several common attack types and the tools used:

First, there are trojan horse programs. Trojan horses are of several different types: destructive, privacy invasion, back doors, remote access tools, droppers, jokes, bombs, rootkits, denial of service agents, and worms. Each of these varieties has its own purpose, and each behaves differently.

Destructive trojans are intended, as the name suggests, to damage or destroy data (unlike a virus, whose purpose is to replicate). Privacy invaders are used to discover some information about the target; they are often used to capture passwords on the infected system. Back doors are used to open a dedicated communications channel that can be used by the attacker to gain control of the computer. Remote access tools take the back door strategy one step further – in addition to opening a channel, they are the means used to exploit it. Droppers are used as a means of deploying a virus or another trojan. Jokes, as the name implies, are generally non-harmful; bombs, on the other hand, are often used to render a program inoperable. Rootkits, most often seen in Unix systems, modify or replace legitimate system utilities, causing them to run illegitimate processes, often unknown to the user. Distributed denial of service (DdoS) agents coordinate, or participate in flooding attacks on other systems, sending large amounts of data in order to overwhelm the capacity of the target computers. Finally, worms seek to replicate themselves; unlike viruses, they do this without attaching to a file or program.

Many hacker tools are actually useful programs and utilities that are misused by attackers to do harm or gain access to a system. For example, port scanners and other vulnerability scanning programs are legitimate tools used to identify weaknesses in a computer system or network. When used by an authorized administrator to discover security flaws in a computer network, these tools perform a valuable function. However, in the hands of an attacker these same tools are used to discover and evaluate security holes, or ways to break into the computer.

Port scanners work by checking a computer's TCP/IP stack for ports that are in the LISTEN state – that is, they are waiting for something to begin communicating (Anonymous, 2001). An open port, even one that is legitimately in use, is a doorway into the system. Once that opening is discovered, an attacker can use it to connect to, and communicate with the target computer.

Password crackers are utilities that allow an attacker to discover and decrypt passwords on the target system. There are two basic types of password cracking tool: dictionary, and brute-force (Bragg, 2003).

Dictionary cracking tools work by trying common words and phrases against the password(s) discovered on a system, while brute-force tools attempt to discover a password by trying all possible combinations of characters (Bragg, 2003). Regularly changing your passwords, and using complex passwords – those containing a combination of capital and small letters, numbers, and punctuation – will defeat most dictionary crackers. Brute-force tools, on the other hand, are much harder to overcome.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Complex passwords will hamper the ability of an attacker to discover a password using a password cracking tool, but will not prevent it.

Assessing Risk, and Developing Policy

A security program, at its core, is about risk management – identifying, quantifying, and mitigating risks to computers and data. There are seven basic steps to risk management (Bragg, 2003):

1. Identify the assets
2. Assign value to the assets
3. Identify the risks and threats corresponding to each asset
4. Estimate the potential loss from that risk or threat
5. Estimate the possible frequency of the threat occurring
6. Calculate the cost of the risk
7. Recommend countermeasures or other remedial activities

Asset identification is more than creating a list of the hardware and software in the computer, it must include the information, or data, that is processed and stored on those computers. The value of data routinely transcends the value of computers and infrastructure by many orders of magnitude (Berger, 2003). If these assets are left out of the assessment, an inaccurate picture of the environment will be developed, and an ineffective security program will result.

Every asset has a value; the next step in performing a risk analysis is to determine what that value is for each asset. There are generally two approaches to asset valuation – the quantitative method and the qualitative method. The quantitative method functions by assigning a financial value to each asset, which is then compared to the cost and effectiveness of the counter-measure (Bragg, 2003). The qualitative system ranks threats and security measures relative to the system being analyzed, often by the use of a scoring, or classification system (Bragg, 2003). For the purposes of descriptions and examples in this study, the qualitative method will be assumed.

Having identified and valued the assets to be protected, threats to those assets must be examined. Any process or event that has the potential to harm an asset is considered a threat. Examples of threats include hackers, tornados, poor procedures, lightning, human error, and terrorists (Visintine, 2003). During this process, the analysis should focus on identification of potential threats; the likelihood of that threat occurring will be considered separately.

Once assets have been inventoried and valued, and threats identified, the potential for loss can be determined. For example, the loss potential from a hurricane in the upper Midwest would be very low, while for that same system in Florida, it would likely be much higher. This process must be thorough, cross-referencing every asset with every threat, the goal of which is to develop a complete picture of the current security environment.

With this assessment complete, and the threat matrix developed, the areas requiring security improvements should become obvious. Armed with this knowledge, and based on the information in the risk assessment, security policies can be defined.

Security policies describe security goals, usually in general terms; they do not define standards or procedures (Bragg, 2003). A password policy, for example, might state when and where passwords are considered necessary, and even if those passwords

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

need to be complex in construction, but would not dictate how to implement passwords in the target environment. For a home user, this might be as simple as stating, “I will use a complex password to control access to the checkbook balancing program and its data files.”

The next step is to identify the necessary tools and procedures to implement and enforce the security policy(ies). This includes, but is not limited to, passwords, anti-virus, firewalls, and backups.

Researching Appropriate Counter-measures

A password is a word or phrase used to authenticate a user to a system. It should be different for each user of the system and highly protected (Harris, 2002). The most common implementation of password security is the ‘challenge and response’ method – the user is presented with a challenge (“Enter your password”), and they must respond with the correct answer (i.e. enter the correct password). If the correct password is not entered, access to the system is denied. Often, access can be completely disabled for a length of time after several failed attempts.

Viruses and worms are the most common attacks against computers and data – exploiting vulnerabilities found in operating systems and application software. Melissa, Code-Red, Slammer, and MyDoom are all examples of what can happen if a system is not protected against these attacks. Anti-virus programs work either by monitoring for and detecting changes in files or in the computing environment or by comparing objects against a database of known infections (Anonymous, 2001). Most commercial anti-virus applications will attempt to clean the infected file or quarantine it if cleaning is not possible.

One of the best-known security measures is the firewall. A firewall is a very important part of a security program and belongs at the top of the list of counter-measures (Ogletree, 2000). Simply put, a firewall prevents unauthorized traffic from entering or leaving a network (Bragg, 2003). There are several types of firewall, each with their own strengths and weaknesses, but they generally fall into three categories – proxies, packet filters, and stateful inspection packet filters (Anonymous, 2001).

A packet filter is the simplest form of firewall, and functions by allowing or discarding traffic packets based on a set of defined criteria (Kaufman, Perlman & Speciner, 2002). These criteria are most often found in the packet header; and may include source and destination IP address, protocol, and port number. A stateful inspection packet filter takes this process further, examining the incoming traffic to verify that it is a response to a previous request (Ogletree, 2000).

A proxy intercepts the traffic, inspects it, and forwards it to the destination. In this way, it is actually acting as a ‘man-in-the-middle’, with the firewall acting as interpreter (Anonymous, 2001); the source computer never makes a direct connection to the destination (Ogletree, 2000). For this reason, application proxy firewalls are usually slower than their packet filter counterparts but are more secure (Anonymous, 2001).

Backups are arguably one of the most important aspects of a security program, falling in the category of ‘Disaster Recovery’. While not protecting the system from attack, the backup is used to rebuild the system after an incident occurs. At its core, a backup is a copy of the valid data stored on other media, most often in a different

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

location. If that data is later deleted, or otherwise compromised, the backup can be used to restore it (Bragg, 2003).

Other counter-measures include the use of biometrics, encryption, uninterruptible power supplies (UPS), and penetration testing. To include every possible type of preventative or restorative measure in this study would be near impossible – the reader would be overwhelmed, and the importance lost. However, one other security area must be addressed: maintenance.

Once a security program has been developed and implemented, it must be kept up to date. As changes to the system are introduced, the security measures and procedures must be re-evaluated to ensure that they are still appropriate, and that they are performing as required. The best way to accomplish this is through the use of vulnerability scanners, and penetration testing. Essentially, this means 'hacking your own system', otherwise knows as 'ethical hacking' (Bragg, 2003). By running popular tools and simulating attacks against the system, new vulnerabilities can be discovered and plans made to patch them.

While nothing will entirely prevent, or protect against a security-related incident, proper education, investigation, planning, and maintenance will significantly reduce the exposure to a manageable level.

CHAPTER 3 METHODOLOGY

Approach

This study is founded on the premise that computing is inherently an insecure environment. Research, both in books and on the Internet, confirms this.

By using the research compiled by others on the subject of information security, it becomes apparent that a truly effective information security program is made up of four distinct areas:

1. Identification
2. Evaluation
3. Remediation
4. Maintenance

It might be argued that a fifth area – education – should be included; however, as that is the purpose of this study, it was not treated as a subject for research.

In each of the subject areas, a combination of research methods was used. While the bulk of the research is based on the previous works of others (applied research), some measure of experimentation and experience was used to verify or corroborate the findings (pure research). When begun, it was assumed that a computer and, by inclusion, its data, could be fully secured against any threat. When, during the course of investigation, it became apparent that this could never be achieved, the focus changed to discovery of the processes and procedures necessary to prevent what could be prevented, prepare for what could not, and recover from an incident if/when it did occur.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Data Gathering Method

The primary method for research was through the use of books and other printed materials. By examining the works of previous researchers, and compiling their findings into a coherent whole, a foundation was built upon which testing could be performed.

Secondarily, direct experimentation was employed to corroborate and validate the findings previously published. A laboratory environment was created, and the physical and technical aspects of the proposed security program were tested.

Thirdly, a six-day boot-camp style class was attended. During this time, data was gathered by attending lectures, performing hands-on lab experiments, and surveying and interviewing instructors and other students.

Lastly, the author's work experience in the area of information security was used to correlate the compiled data.

Database of Study

Books, newsletters, and other media, both printed and electronic, were chosen for their relevance. Most print sources selected were textbooks and training manuals in the subject of information security, these being considered authoritative on the subject. Several papers submitted by other Kennedy-Western students were also accessed. These sources were used throughout the study, in all areas.

Government websites – including the Federal Bureau of Investigation and the Department of Homeland Security – containing whitepapers, newsletters, and other documentation, were reviewed for subject material. Most of this data was used to develop the first chapter material – defining the issues, and justifying the study.

In addition, the SANS Reading Room (http://www.sans.org/rr/) was used as a source of material written by information security professionals on a wide range of specific subject areas. The SANS Institute (http://www.sans.org), "…develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system – Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community." (SANS, 2003) With access to thousands of pieces of reference material, this was an invaluable resource in this study; primarily the section on security policy.

For the experimental portion of the investigation, a dedicated computer network was built, and various attack and prevention scenarios run against it. This network was made up of a Compaq Proliant 6500 server running Microsoft Windows 2000 Advanced Server, a Cisco 2500 router, two LinkSys firewall/routers, and four computers running Windows 2000 Professional, Windows XP Professional, and/or Windows 98. Using tools downloaded from the Internet, attacks were simulated against this network to observe how an attack could be mounted, what the effects were of that attack, and what preventative measures were most effective. This study method was employed to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

evaluate the technical aspects of the proposed security program – passwords, firewalls, anti-virus, etc.

In February of 2004, a six-day security training boot camp was attended – *Track 1: SANS Security Essentials and the CISSP 10 Domains*. In addition to classroom lecture and evening hands-on labs, this afforded an opportunity to interview information security professionals, including people from government, public, and private industry. The information gained was invaluable in researching and developing this paper in all subject areas.

Finally, the author has over seventeen years of experience in the field of information technology, three directly in security. He holds multiple industry certifications, including Microsoft Certified Professional (MCP), Microsoft Certified Systems Engineer (MCSE), Citrix Certified Administrator (CCA), Checkpoint Certified Security Administrator (CCSA), and NT Certified Independent Consultant (NT-CIP).

In combination, the resources form a comprehensive database of study sufficient to validate the research and findings.

Validity of Data

Many of the ideas under research are academic, and consensus has been established for many years. In the cases of risk analysis and security policy, multiple legal and actuarial reviews have taken place, and common criteria established – often referred to as 'best practice'.

While compiling the data, every attempt was made to cross-reference between sources to validate the data. In all cases where this was possible, the processes, procedures, and conclusions were the same. Concurrence of findings across sources is taken as a good indicator of data validity.

Further, technical assumptions were tested in a laboratory environment to prove, or disprove, the claim(s). Multiple tests were performed where indicated, and the results were consistent. This consistency was viewed as confirmation of the legitimacy of the source data.

Statistics were taken from government publications; while details of these statistics might differ somewhat, the implications and conclusions were identical. Specifically, statistics concerning numbers of identity theft victims, numbers of computer crimes, and loss calculations differed from agency to agency. However, the conclusion that computer crime is increasing, and further that it is increasing faster than the ability to prevent it, is consistent across all sources. Again, this served to confirm that the data was valid, and that the conclusions were justified.

Originality and Limitations of Data

While performing research for this study, many resources were found that deal in-depth with each specific subject; however, few presented the data in a manner that could easily be used to develop a functional security plan. Further, most of the resources were either academic or were prepared without distinction between the needs of different target populations.

The purpose of this study – being to create a systematic guide to designing and implementing an information security program – draws heavily on these previous works,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

correlating and compiling them into a concise program. Target audiences are differentiated, as there are significant distinctions in their individual needs.

Due to this differentiation, many assumptions and generalizations had to be made. In some cases, this will limit the data to simply being a basis for further individual research. If the plan presented in the Data Analysis and Summary chapters is too general for immediate use in a particular environment, reference is made to resources for further research and more detailed information. Wherever possible, specific recommendations are made; however, it is beyond the scope of this document to be a final authority on the individual needs of every entity.

Contradictory information is scarce; what is available is often singular and difficult to corroborate. The overwhelming volume of data supporting the position of this study, and the lack of verifiable evidence to the contrary, makes objectivity a difficult task. During the course of the study, and particularly during the laboratory experimentation portion, attempts were made to disprove the majority opinion; these attempts were made, as much as possible, without prejudice. The results were invariably in line with consensus; contrary opinions were discarded in the light of evidence.

The age of the data sources was not considered a significant limiting factor in the compilation of the data, for two reasons:

1. Little new information has been compiled in recent years – most new writings are simply reinterpretations or restatements of the original or existing information.
2. All data sources are less than four years old – generally considered current by industry standards.

CHAPTER 4 DATA ANALYSIS

Security Defined

The foundational principles of information security are confidentiality, integrity, and availability (Bragg, 2003). Confidentiality is the assurance that only those who are authorized to access data can access it; integrity is the assurance that the data is accurate, and unaltered; and availability is the assurance that the data will be accessible when it is required. The goal of an information security program is insure these three principles.

Security is not an absolute; rather, information security is about managing risk (Anonymous, 2001). In real terms, this means that no amount of security can fully protect a system from loss – there will always be risks to the confidentiality, integrity, and/or availability of the data. Understanding that risk, and implementing appropriate controls to minimize and manage it, is the best insurance against loss.

The risk and severity of a security breach must be identified, and quantified wherever possible. Then, appropriate steps must be taken to reduce the probability of an attack; controls identified to reduce the impact if one should occur; and plans developed to respond to, and recover from, the incident. This process of risk management begins by identifying and valuing the assets to be protected. Before any measures are considered, the user must know what is to be protected, and why.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Data Classification and System Criticality

The first process in developing any information security program is identification. Without a clear understanding of what needs to be protected and why, the plan will be incomplete, and the security program ineffective. The first step in this process is inventory. This can be accomplished by simply creating a list of every computer, and the data stored therein. No thought need be given at this point to the value of the asset, or the criticality of the data – the focus should be on completeness.

All individual assets need to be considered – it is not enough to simply list 'computer system' as the asset. The system is made up of several components, any of which could cause a breakdown in one or more of the three areas of security – confidentiality, integrity, or availability. For example, if the monitor were to fail, confidentiality and integrity would be unaffected, but the system, and its data, would be unavailable until the monitor was replaced. While not catastrophic, it emphasizes the need for separation of assets when creating the inventory.

On the other hand, it is also unnecessary to delve too deeply into detail. There is no need to list every component inside the computer, for instance. If one component fails, the computer fails (in this case, possibly affecting the integrity of the data, as well as the availability).

The following table illustrates one way a home user might approach this task:

Item					
Computer					
Monitor					
Speakers					
Connective Equipment					
Printer					
Other Hardware					
Operating System Files					
Checkbook Application					
Other Financial Application					
Other App 1					
Other App 2					
Checkbook Data Files					
Other Financial Data Files					
Resume					

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Employment Related Files					
Music Files					
Movies					
Other Data					
Inventory					
File Cabinet					
Hard Files					

Table 1 – Asset Inventory

For a business, the list would be much larger, and would likely contain more detail on each asset; however, the focus is the same – identification of all the assets to be protected.

If possible, this list should be compiled using a spreadsheet program, database, or other data collection program. As new assets are identified, or new data files created, the list will need to be updated to reflect those changes. Maintaining the list in an electronic form will make it much easier to update, and recalculate. The asset list should also be included in the inventory – it will likely be one of the more important assets.

Once the list has been compiled and reviewed for accuracy, a value needs to be assigned to each item. There are two common methods used to accomplish this: the quantitative method, and qualitative method – both are effective; neither is easy (Bragg, 2003).

The quantitative method assigns a dollar value to each asset, so that calculations of loss can be performed. This method is more often used in business, usually involving intervention by accountants and insurance experts. For the average home user, mathematical calculations of revenue loss, replacement cost, and loss expectancy are generally beyond their scope of experience, and the resulting confusion could lead to an inaccurate assessment, and an ineffectual plan.

The qualitative method, on the other hand, uses a more subjective scale to assign a relative importance to each item, such as High, Medium, and Low. For a home user, this is a much more effective approach.

There are no hard and fast rules for assigning these values; what is critical in one system might have no value at all in another. For that matter, the values themselves may have different meanings to different people. It is often a good idea to define the terms before using them:

HIGH	Loss would constitute a serious setback, with severe legal, financial, or other setbacks
MEDIUM	Loss would constitute a major setback, with possible legal, financial, or other consequences
LOW	Loss would cause an inconvenience, but the possibility of legal, financial, or other consequences is low

Table 2 – Data Class

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

While these definitions will likely vary from person to person, and situation to situation, it is important to insure consistency throughout the assignment process.

Depending on the amount and types of data stored on a system, it may be necessary to assign a rating to the confidentiality of the data as well.

CONFIDENTIAL	Exposure would result in severe legal or financial consequences
SENSITIVE	Exposure would possibly result in legal or financial consequences, but not severe
PUBLIC	Exposure would have no legal or financial consequences

Table 3 – Confidentiality

For the purposes of this study, the qualitative method will be used, with a scale consisting of Critical, High, Medium, and Low. Table 4 on the next page illustrates the application of these values to the inventory produced earlier:

Item	Importance				
Computer	Medium				
Monitor	Medium				
Speakers	Low				
Connective Equipment	Medium				
Printer	Low				
Other Hardware	Low				
Operating System Files	High				
Checkbook Application	High				
Other Financial Application	Medium				
Other App 1	Medium				
Other App 2	Low				
Checkbook Data Files	Critical				
Other Financial Data Files	High				
Resume	High				
Employment Related Files	Medium				
Music Files	Low				
Movies	Low				

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Other Data	Medium				
Inventory	High				
File Cabinet	Medium				
Hard Files	Medium				

Table 4 – Asset Valuation

With the asset evaluation complete, the process continues with the identification of vulnerabilities, and corresponding threats to the assets.

Common Threats

A threat requires a vulnerability. This means that in order for a threat to be realized, the associated vulnerability must exist, and be exploitable. Most threats can never be eliminated – fire, tornado, virus – but the vulnerabilities that they exploit can be controlled, thereby reducing the probability of the threat becoming an incident. In order to control these threats, they must first be identified.

A threat, as previously defined, is any event that can exploit a vulnerability to cause damage, loss, or other harm to an asset. Therefore, it is not just hackers and viruses that must be acknowledged; fire, flood, tornado, power outage, all these must be accounted for in the threat matrix. At this stage, it is not necessary to consider the likelihood of the threat occurring, but only to list the threat as a possibility. Common threats include – but are not limited to – data theft, data corruption, data loss, computer failure, power failure, and/or catastrophic events.

Theft is the unauthorized acquisition of the data – most often by an unknown entity. This can be accomplished by several means, from interception and/or redirection of the data stream to 'dumpster diving' (going through the garbage receptacles of the intended victim). The theft usually goes unnoticed until/unless the data is used by the attacker, often illegally. Data theft is primarily a contravention of the principle of data confidentiality, but can also affect integrity and availability.

Data corruption can be intentional or unintentional. Strictly defined, data corruption is any unauthorized or inappropriate change to the data; it is most often regarded as rendering the data unreadable or unusable. Data corruption is sometimes reversible, thereby differentiating it from data loss. For example, mistyping a credit card number on a web page could be considered data corruption – incorrect data was presented, resulting in a failure of the intended process. Corruption is a violation of data integrity, although it can also be considered an interruption of data availability.

Data loss is related to data corruption in that both leave the data unavailable; however, loss is considered irretrievable. Data loss can also be intentional or unintentional – a virus that deletes files on the hard drive would be an intentional loss. The example given in Chapter 1 (Statement of the Problem) constitutes unintentional data loss – the man's checkbook file was deleted, but his children never intended any harm. Data loss affects the principle of availability.

Computers contain many parts – both electrical and mechanical. The failure of any of these parts could leave the system unusable. In this situation, the information stored on it would be unavailable, and potentially corrupted or destroyed. Computer failure is considered one of the most common threats, and is the one that is the most difficult to guard against.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Power failures are also one of the more common threats, however they are somewhat easier to prevent. Technically, any variation in the quality or quantity of power to the system is considered a failure – this includes spikes, surges, brownouts, blackouts, and even accidentally pressing the power button. Power failures, like computer failures, primarily affect the availability of the data however corruption and loss are also possibilities.

Tornado, earthquake, fire, insurrection, war – these are all examples of catastrophic events. While rare, any of these would cause irreparable damage to the systems and data, and could violate all three principles of security. There are few if any preventative measures that can be taken, but there are procedures that can assist with the recovery of the data.

During the threat identification phase it is important to be thorough. As with asset identification, the value of the security plan depends on the accuracy and comprehensiveness of the threat list. The table on the next page illustrates how these threats would be added to the list begun earlier.

Item	Importance	Virus	Fire	Failure	Theft
Computer	Medium				
Monitor	Medium				
Speakers	Low				
Connective Equipment	Medium				
Printer	Low				
Other Hardware	Low				
Operating System Files	High				
Checkbook Application	High				
Other Financial Application	Medium				
Other App 1	Medium				
Other App 2	Low				
Checkbook Data Files	Critical				
Other Financial Data Files	High				
Resume	High				
Employment Related Files	Medium				
Music Files	Low				
Movies	Low				

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Other Data	Medium				
Inventory	High				
File Cabinet	Medium				
Hard Files	Medium				

Table 5 – Threat Matrix

Risk Analysis

Having identified assets, assigned values, and ascertained threats, the next step is to determine what vulnerabilities exist. A complete and accurate vulnerability assessment is essential to the development of a sound security plan. The presence or absence of a firewall, for example, will change the risk level associated with an external attack; having an up-to-date virus scanner will lower the risk of a virus. The assessment will result in a picture of the current security posture - including strengths, weaknesses, and areas for improvement. Again, a scale of High, Medium, and Low may be used to rank threats based on the vulnerabilities identified. For instance, if the system has a virus scanner that is kept up to date, and the user never opens suspicious emails, the level of vulnerability to a virus would be Low. If, on the other hand, the virus signature files are not kept current or the user does not exhibit caution when opening and reading email, then the vulnerability level would be higher – Medium, or even High.

During this analysis, the assets themselves should not play a major role in the ranking process. The purpose of this exercise is simply to discover the level of exposure to the threats identified in the previous step. For the purpose of this demonstration, it has been assumed that the virus scanner is up to date, the user is cautious about email, the user smokes at the computer, it is an older system, and there is no firewall.

Item	Importance	Virus	Fire	System Failure	Data Theft
	Risk -→	Low	Medium	High	High
Computer	Medium				
Monitor	Medium				
Speakers	Low				
Connective Equipment	Medium				
Printer	Low				
Other Hardware	Low				
Operating System Files	High				
Checkbook Application	High				
Other Financial Application	Medium				
Other App 1	Medium				
Other App 2	Low				
Checkbook	Critical				

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Data Files					
Other Financial Data Files	High				
Resume	High				
Employment Related Files	Medium				
Music Files	Low				
Movies	Low				
Other Data	Medium				
Inventory	High				
File Cabinet	Medium				
Hard Files	Medium				

Table 6 - Vulnerability

With all of the threats and associated vulnerabilities identified, an analysis of risk can be done. A risk analysis will compare the assets to the threats, taking values and vulnerabilities into account. This will result in a representation of the level of risk associated with each asset. The tables below show two methods of ascertaining these values.

	LOW (.1)	MEDIUM (.5)	HIGH (1.0)
CRITICAL (100)	10	50	100
HIGH (75)	7.5	37.5	75
MEDIUM (50)	5	.25	50
LOW (25)	2.5	12.5	25

Table 7 – Risk Assessment by Value

	LOW	MEDIUM	HIGH
CRITICAL	Medium	High	High
HIGH	Medium	High	High
MEDIUM	Low	Medium	High
LOW	Low	Medium	Medium

Table 8 – Risk Assessment by Rank

The first method assigns a numeric value to each factor, multiplying them to arrive at a risk value. The second method works similarly, but uses the familiar High, Medium, and Low ranking system. As shown in the shaded areas, both methods result in a determination of risk level.

These risk levels may now be applied to the asset matrix, producing a view of the assets with their associated risk level. It is this information upon which a security plan is built, with those items that are ranked higher receiving more attention than those with a lower level of risk.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Item	Importance	Virus	Fire	System Failure	Data Theft
	Risk -→	Low	Medium	High	High
Computer	Medium	Low	Medium	High	High
Monitor	Medium	Low	Medium	High	High
Speakers	Low	Low	Medium	Medium	Medium
Connective Equipment	Medium	Low	Medium	High	High
Printer	Low	Low	Medium	Medium	Medium
Other Hardware	Low	Low	Medium	Medium	Medium
Operating System Files	High	Medium	High	High	High
Checkbook Application	High	Medium	High	High	High
Other Financial Application	Medium	Low	Medium	High	High
Other App 1	Medium	Low	Medium	High	High
Other App 2	Low	Low	Medium	Medium	Medium
Checkbook Data Files	Critical	Medium	High	High	High
Other Financial Data Files	High	Medium	High	High	High
Resume	High	Medium	High	High	High
Employment Related Files	Medium	Low	Medium	High	High
Music Files	Low	Low	Medium	Medium	Medium
Movies	Low	Low	Medium	Medium	Medium
Other Data	Medium	Low	Medium	High	High
Inventory	High	Medium	High	High	High
File Cabinet	Medium	Low	Medium	High	High
Hard Files	Medium	Low	Medium	High	High

Table 9 – Completed Risk Analysis

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

With the analysis complete, the response to those risks can be now determined. There are four possible responses that can be applied to any risk scenario (Harris, 2002):

- Reduce the risk
- Transfer the risk
- Accept the risk
- Ignore the risk

Reducing the risk involves identifying and implementing counter-measures, and generally applies to those areas where the risk factor has been identified as High. Risk reduction includes things like setting up a firewall, performing regular backups, buying a fire extinguisher, and/or installing a UPS (uninterruptible power supply).

Transfer of risk is accomplished by purchasing insurance. Many homeowners' policies allow riders to be added that will cover computer equipment, software, and data files. This is most often done where the risk level is Medium.

Risk acceptance is the acknowledgement of the risk and the choice to do nothing to mitigate it. If the cost of the counter-measure exceeds the value of the loss, then this is a viable option. It is most often selected when the risk level is Low.

Unlike risk acceptance, ignoring the risk is denial of its existence or potential impact. Ignoring risk is not recommended, as it demonstrates a lack of due care and diligence. For a home user, this might be an acceptable option; however, in a business scenario this could lead to legal and possibly criminal consequences, even if the loss is minor.

The determination of risk response should be undertaken with great care. Applying a counter-measure whose cost exceeds the value of the asset would be wasteful; accepting a high-cost risk that could easily be countered with an inexpensive solution would likewise be irresponsible. Therefore, it is necessary to develop policy(ies) to guide the decision process, and assure that the correct measures are implemented to meet the defined need.

Security Policy

A security policy is the document that establishes how a security program will be set up, dictates the goals of the program, assigns responsibilities, and demonstrates the strategic and tactical value of security (Harris, 2002). In short, the security policy is the foundation on which all security decisions are based.

While referred to as if it was a single entity – the security policy – it is, in fact, made up of many smaller individual policy documents covering a wide range of topics. An Acceptable Use policy, for example, defines what are and are not considered proper and correct usage of the systems and the data held within them.

In a business setting, the security policy may be a long, complicated set of documents; for the home user it is often a much simpler task. An anti-virus policy, for example, could simply state that, "…an anti-virus program will be installed, and the program and virus signature files will be kept up to date.", whereas a backup policy might read, "…backups of all Critical or High risk data will be made weekly and stored in a fire-proof safe."

The security policy should reflect the findings of the risk analysis. It is used as a basis for determining what counter-measures may, or may not be appropriate. Using the matrix previously developed, the following policies could be written:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Anti-Virus Policy – The computer will have an anti-virus program installed. The anti-virus program and all its supporting files – virus signatures, etc. – will be updated regularly, based on the schedule set by the software vendor. Further, the program will be configured to provide maximum protection, except where to do so would affect overall system performance.
- Backup Policy – All data files rated Critical or High risk will be backed up to tape weekly. Two alternating sets of tapes will be used; if one set of tapes should be corrupted, the other can be used to restore the data. For safety, the backup tapes will be stored in a separate room in a fireproof box or safe.
- Computer Recovery Policy – The homeowner's insurance policy will be amended by adding a rider covering the replacement cost of the computer system hardware and software. This rider will be reviewed annually and updated to reflect changes in the cost of replacement.
- Firewall Policy – A small office/home office (SOHO) firewall will be installed and configured to block unauthorized access to the computer from the Internet. At a minimum, the firewall will provide network address translation (NAT) and dynamic host configuration protocol (DHCP) services.
- Password Policy – Access to the computer will be controlled by the use of system passwords. Individual user accounts will be created and a password assigned to that account. Passwords must be no less than eight characters in length, and must contain at least three of the following four types of character: small letters, capital letters, numbers, and/or punctuation marks.
- Access Policy – The checkbook program and its related files will be restricted by the use of file system permissions. Only those persons who maintain the checkbook data will be allowed to run the program or access the files. Further, employment related data files will only be accessible to the person who owns them, unless that person grants access to others. All other access to programs and data will be controlled in a manner consistent with its importance.
- Confidentiality Policy – All documents that are no longer of use, particularly those containing credit card numbers or other personally identifiable information, will be shredded prior to being disposed of.
- Infrastructure Environment Policy – An uninterruptible power supply will be installed and the computer, monitor, and firewall will be plugged into it. The printer, speakers, and other hardware will be plugged into a surge protected power strip, which will be plugged directly into the wall socket.

It is evident from these policies what steps must be taken, what items and/or devices must be purchased, and what results are expected. Items to purchase include a tape drive, a fireproof safe, a firewall device, a UPS unit, and one or more surge protectors. Notice that the specifications for these items are not stated in the policy – this allows for changes when makes/models are upgraded, or when new technology becomes available, without having to revise the underlying policy document(s).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The risk analysis and security policy should be reviewed regularly to make certain that it continues to reflect the needs of the system and the environment. Any time a new program is installed, new hardware is added, or changes are made to the environment, the associated risk factors should be assessed and the appropriate security measures implemented. By diligently following the policy, an acceptable level of security can easily be maintained.

Passwords

To anyone who works in a corporate environment, passwords are a familiar concept. In order to access the network, a user ID and password must be entered; often, individual applications will require a user ID and password. A common complaint of corporate computer users is, "…too many passwords." Those same people, however, are the ones who are most at risk on their personal computers because they do not use passwords at home.

A password is simply an authentication mechanism – it acts as 'proof' that the person accessing a computer, application or data file is authorized to do so. Passwords, however, are easy to break – a weak password is little better than no password at all. A strong password, on the other hand, is much more difficult to crack, and offers a last line of defense against data theft. So what exactly is a strong password?

A strong password – one that is difficult to crack – is one that is at least eight characters in length, uses a combination of characters, numbers, and symbols, and does not contain any words that can be found in a dictionary (Harris, 2002). A good method for creating a strong password is shown below.

- Begin with a sentence – preferably one that is easy to remember:
  "This is going to be my new, STRONG password!"
- Take the first letter of each word and include punctuation:
  "Tigtbmn,Sp!"
- Change letters into numbers or symbols where possible:
  "T1g+bmn,Sp!"

The resulting password will be much more difficult to crack, yet is still easy to remember. Practicing typing the new password will build familiarity and make it easier to remember.

Another method for creating a strong password is to use a passphrase. The strength of a passphrase is in its length; the drawback to using a passphrase is that some systems will only allow up to a certain number of characters. A passphrase can be nothing more than a sentence with the spaces removed. Creating a good passphrase is similar to the process of creating a strong password, as demonstrated next.

- Begin with a sentence – preferably one that is easy to remember:
  "This is going to be my new, STRONG password!"
- Remove spaces and punctuation:
  "ThisisgoingtobemynewSTRONGpassword"
- To make it easier to type, change capital letters to small:
  "thisisgoingtobemynewstrongpassword"
- Change letters into numbers or symbols where possible
  "th1sisg0!ingtob3myn3wstr0ngpa##word"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Either method – strong passwords or passphrases – will create a password that will be extremely difficult to crack. No password scheme is perfect - any password can eventually be broken. If an attacker can steal a file, it is only a matter of time before he/she will be able to access it, regardless of the strength of the password or passphrase. The purpose of a good password is to make it so difficult and time-consuming that the thief gives up before finding the correct combination.

So, where should passwords be used? Everywhere! For a home user this may appear to be 'overkill', but the relatively minor inconvenience of having to type a password, or passphrase, is far less than the major legal and financial consequences of having credit card numbers, bank account numbers, and other personal information posted and spread all over the Internet. For any application that allows a password, one should be entered; for any critical or high-risk data file that can be password-protected, one should be used.

Passwords are used primarily to protect the confidentiality of data, although they also help guarantee integrity. Without the password, a data file cannot be accessed; therefore, it cannot be changed. This can be a problem if the user forgets the password assigned to a program or file, and demonstrates the legitimate need for password cracking utilities. Appendix A contains references to several such tools and their vendors.

Anti-Virus

Viruses are the most common form of attack against systems and data. According to McAfee's Anti-Virus Emergency Response Team (AVERT) there are more than 81,000 viruses currently in circulation, with over five hundred new viruses discovered every month (McAfee Security, 2004). Protecting against these threats is an important step in ensuring the integrity and availability of data.

The best way to prevent infection by a virus is never to let it get into the system. An anti-virus program will help prevent infection and damage after a virus is triggered; by exercising caution, the virus will never be allowed into the system. There are several steps that, if followed, can significantly reduce the exposure to a virus (McAfee Security, 2004):

1. Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
2. Do not open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
3. Do not open any files attached to an email if the subject line is questionable or unexpected. If the need to do so is there always save the file to your hard drive before doing so.
4. Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
5. Do not download any files from strangers.
6. Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.

7. Update your anti-virus software regularly. Over 500 viruses are discovered each month, so you'll want to be protected. These updates should be at the least the products virus signature files. You may also need to update the product's scanning engine as well.
8. Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.
9. When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats. Check with your product vendors for updates which include those for your operating system web browser, and email. One example is the security site section of Microsoft located at http://www.microsoft.com/security.

Anti-virus programs are available from a number of sources; two of the best known are McAfee VirusScan (http://us.mcafee.com/default.asp) and Norton AntiVirus (http://www.symantec.com/nav/nav_9xnt/). While it may not be entirely possible to prevent a virus, use of programs like these will help stop the virus from destroying files, or damaging the system.

Because anti-virus program work by comparing files to known patterns, or signatures, it is extremely important to keep these signature files up to date. Most programs have an automatic update feature that will check for new signature files on a regular basis, even downloading and installing them with no user intervention required. With so many new viruses being discovered every day, this is the best way to maintain a high level of protection against infection.

Firewalls and Intrusion Detection

Strictly defined, a firewall is, "…a system of components designed to control access to and from your network and an external network, based on the security policies in effect at your site." (Ogletree, 2000) In practice, a firewall is usually a device or program that controls and/or blocks traffic based on a set of user-defined rules. Either definition is correct; a firewall's purpose is to prevent intruders from accessing the system(s) it is in place to protect.

There are two classes of firewall – hardware and software. A hardware firewall is a device that is physically connected between the external network (usually the Internet) and the internal network, or home system. Hardware firewalls are usually of the packet filter type, examining packets as they enter and allowing or discarding them based on information found in the packet header. These can be stateful – checking to verify that the packet is a response to a previous request – or non-stateful – simply allowing the traffic to pass if the packet header information meets certain conditions, or rules (Ogletree, 2000). Of these two, the stateful is the more discriminating, and offers better protection.

Hardware firewalls often also provide network address translation, or NAT. This process effectively 'hides' the source computer by assigning a different IP Address to the packets as they pass through the device. The computer is most often configured to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

use a private address (a non-routable address that cannot be used on the Internet); the NAT feature of the firewall translates that into a public address (which can be used on the Internet) and back again. Devices from LinkSys (http://www.linksys.com), NetGear (http://www.netgear.com/products/routers/firewallvpn.php), and SMC (http://www.smc.com/index.cfm?sec=Products&pg=Barricade-Matrix&site=c) offer both firewall and NAT capabilities.

A software firewall, as the name implies, is actually a program installed on the computer, and is usually of the application proxy type. Instead of relying on the information contained in the packet header, an application proxy intercepts the traffic, inspects the data, then makes the connection to the external network, acting as a middleman for the communication (Ogletree, 2000). By acting in this way the computer never makes an actual connection to the target system; instead, the proxy makes and maintains the connection, inspecting every packet – both inbound and outbound – to make sure it is a valid piece of the communication.

Another advantage of software firewalls is the ability of some programs to detect suspicious or abnormal activity, such as alterations to files, and block the action - this is referred to as intrusion detection, or intrusion prevention. Intrusion detection functions in one or both of two ways, either by taking a 'snapshot' of the files on the system and watching for changes, or by examining the behavior of programs and traffic packets. Programs such as BlackIce from ISS (http://www.blackice.iss.net) and ZoneAlarm from Zone Labs (http://www.zonelabs.com/store/content/home.jsp) offer both firewall and intrusion detection features.

The best protection is offered by using a combination of hardware and software firewalls. For a home user with a cable Internet connection, this might mean inserting a firewall device between the cable router and the computer, and installing a software firewall product on the computer. This combination assures that if an attacker gets past one defense, the others are there to prevent access to the data. This strategy – having multiple levels or layers of protection - is commonly known as 'defense in depth'.

A firewall works to ensure the confidentiality, integrity and availability of the system and its data, but only against attacks from outside. And, as with all other security measures, it must be configured and maintained correctly to be effective; as changes are made to the system, the firewall must be checked to make certain that it is still functioning as desired.

Vulnerability Scanning

Investing large quantities of both time and money in identifying and securing assets implies that the system is, indeed, secure; many people stop at this point only to find out later that something was missed, and their data is gone. In order for the system to be considered secure, tests should be conducted to verify that the applied security measures are sufficient, and that they are functioning as desired. Testing can be accomplished by scanning the system for vulnerabilities using the same tools that an attacker would use.

There are many programs available freely on the Internet that may be used to test a system for vulnerabilities. Many of these tools are written for the Unix/Linux environment and, as such, will not be discussed in this study; the reader is encouraged to investigate these programs and make a determination as to their efficacy in the security program.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The first test that should be performed is a port scan. A port is used as a channel for communication between systems; usually they are opened by services like telnet, FTP, and others. If these ports are allowed to remain open, they can by used by an attacker to gain access to the system. A port scanner, as the name implies, scans the system for open ports; once identified they can be closed, or blocked by the firewall. The following table lists several common ports and their use; a complete list is available at http://www.sockets.com/services.htm.

PORT #	DESCRIPTION
20 - 21	FTP (file transfer)
23	Telnet (remote session)
25	SMTP (email)
53	DNS (name resolution)
80	HTTP (Internet)
137	NetBIOS (name resolution)
139	NetBIOS (session)
443	HTTPS (secure Internet)
546 - 547	DHCP (IP Addressing)
1433	Microsoft SQL Server (database)
1494	Citrix ICA (remote session)
5190 – 5193	America Online

Table 10 – Port Numbers

NmapWin is the Windows version of the well-known port scanning utility Nmap – short for network mapper. Nmap is a command-line tool and, while very powerful, it is rather difficult for the average home user to learn. Nessus - and its Windows counterpart NeWT - use the Nmap engine to perform scans however, NeWT has a graphical Windows front-end, making it easier to understand and use. GFI's LANguard is also a Windows-based scanning tool, with a very clean interface and a thorough help file. Regardless of the tool chosen, the process is roughly the same.

For the purposes of this study, both NeWT and LANguard will be used; the next page shows screenshots of both utilities with scans in progress.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

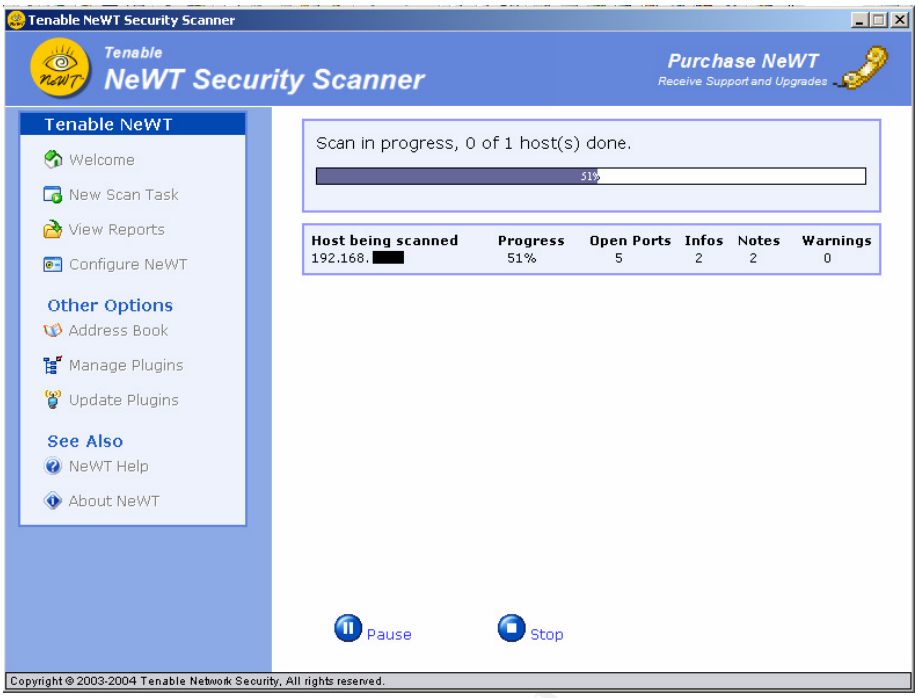


Figure 1 – NeWT Scanner

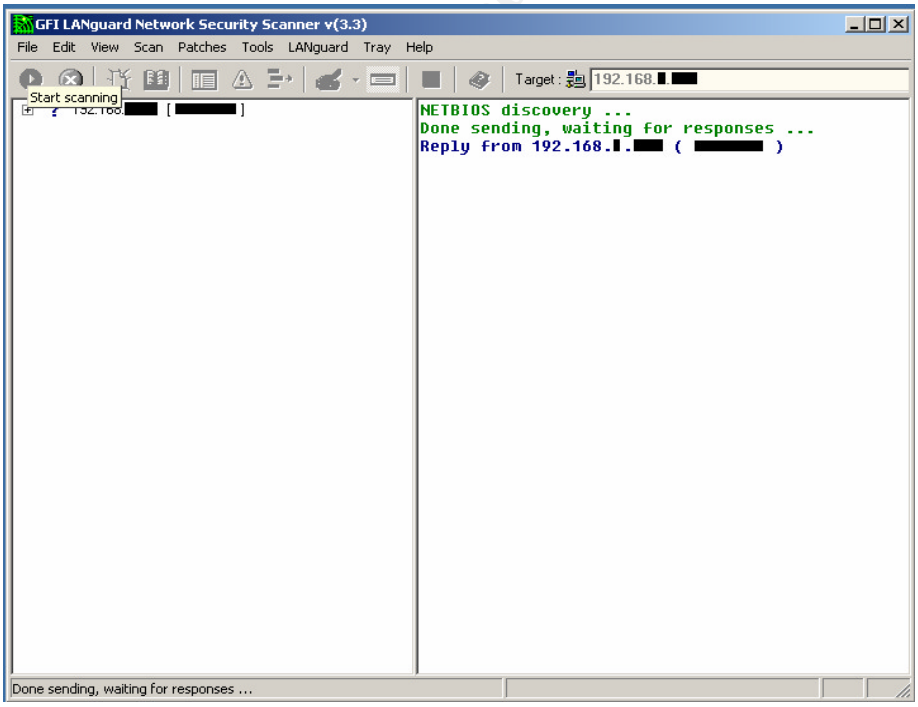


Figure 2 – GFI LANguard Scanner

Once complete, a report will be generated showing open ports and, in some cases, warnings or cautions about other vulnerabilities that were found. The screenshot on the next page shows a partial report from LANguard, the one on the following page is a partial report from NeWT:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

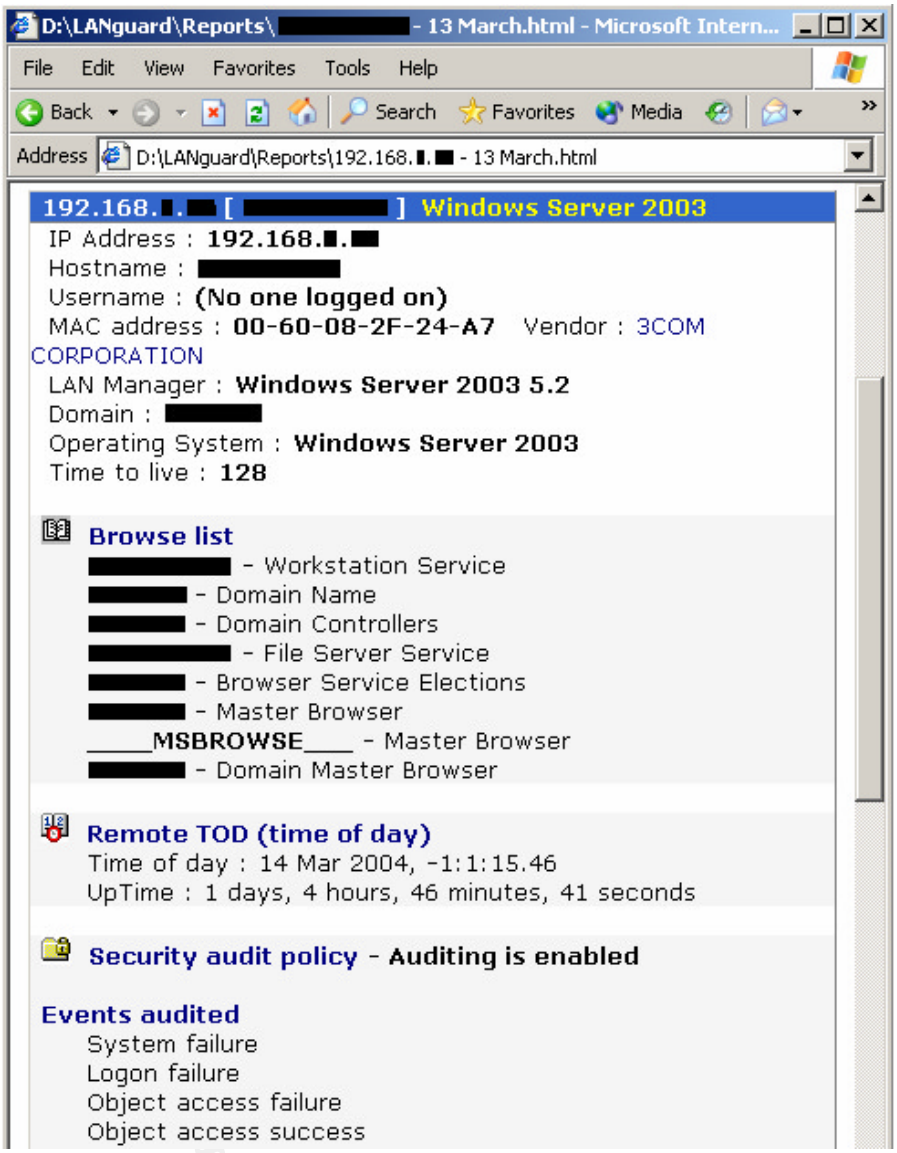


Figure 3 – LANguard Report

© SANS Ins

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

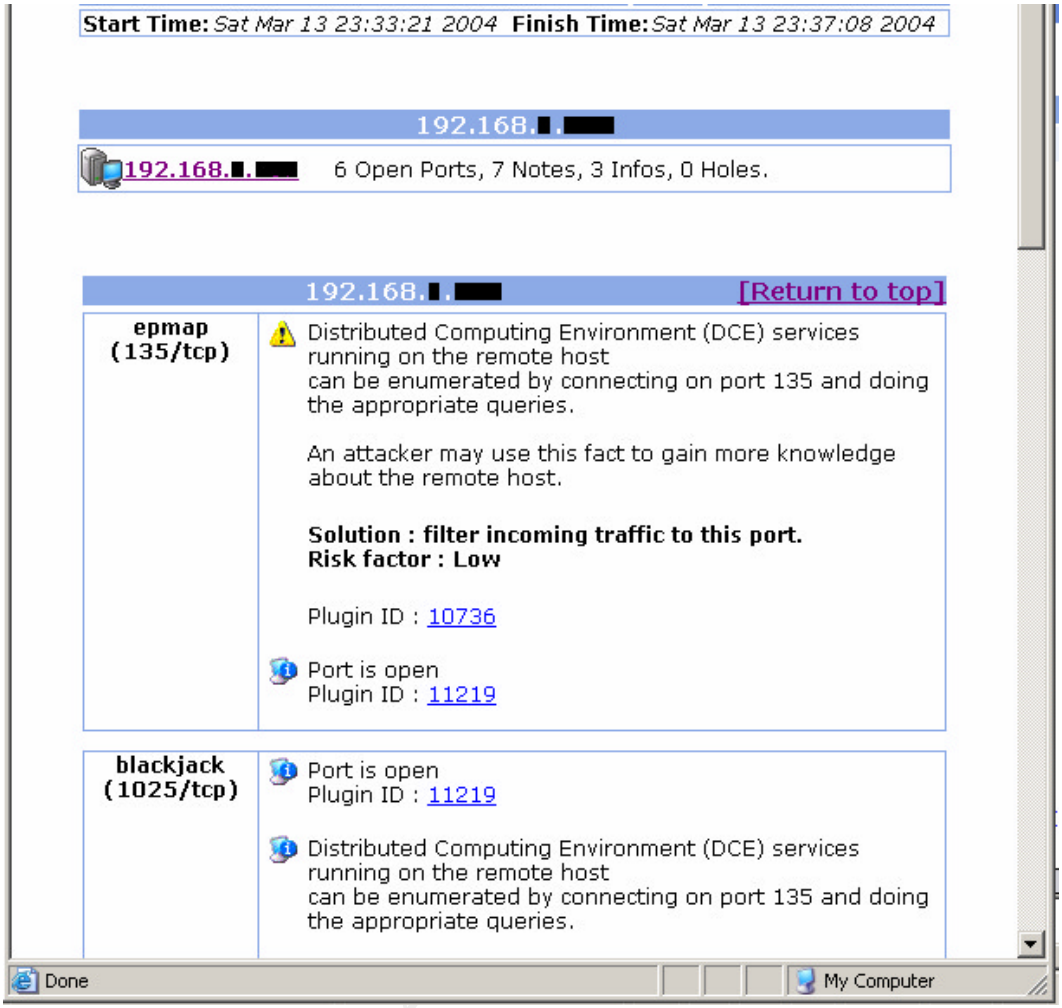


Figure 4 – NeWT Report

Although not shown in same manner, both programs found open ports; additionally, it was possible to determine the operating system in use, the domain or workgroup membership, and even the user name of the person logged into the computer. This shows how easy it is for an attacker to gain knowledge that can be used to illegally break into the system and either damage or steal information.

A word of caution: in the laboratory, while obtaining these screenshots, the inadvertent use of a dangerous setting caused one of the test systems to crash. Exercise extreme care when running these, or any other tools to avoid data corruption or loss. Both utilities have 'safe mode' settings; it is recommended to use these unless absolutely certain that no damage will result. If in doubt, a professional should be consulted.

Once an attacker has scanned the system and discovered things like operating systems, user names, and open ports, the next thing he/she will do is attempt to obtain passwords. Again, it is important to use strong passwords to prevent, or at least delay this from happening. Running a password cracking utility on the system will assist in finding accounts that are vulnerable to this type of attack.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

L0phtCrack (LC4) and John the Ripper (JtR) are the two most popular password cracking utilities available. LC4 is commercial software and is very easy to use, however because of its cost it is probably better suited to a business environment than home use. JtR is freeware, but has no Windows interface; instead, it is run from a command prompt. For this reason it is not a good choice for the average home user.

Cain & Abel (C&A) is freeware and has a Windows GUI interface. It allows not only password cracking but discovers other system information as well. The C&A tool was used for password cracking in this study; the following screenshot shows the utility in use.

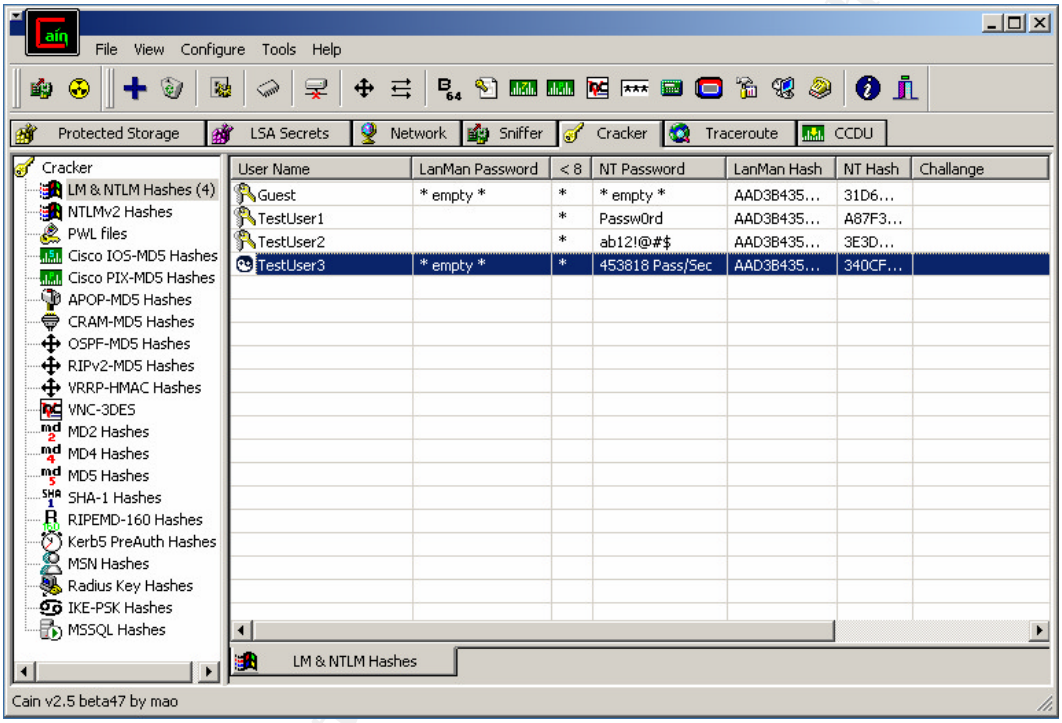


Figure 5 - Cain & Able Password Scan

It is important to note that any password can be cracked, given enough time. In the figure above, the Guest account has no password (blank), TestUser1 has a password of 'Passw0rd', TestUser2 is 'ab12!@#$', and TestUser3 is in the process of being cracked. The password for TestUser1 was found in approximately 20 minutes; it took well over an hour to crack the password for TestUser2. The process was stopped after six hours; the password for TestUser3 was not discovered in that time (the password was T#1s!sAstr0ngPwd).

This clearly demonstrates the benefits of using complex passwords. By using strong passwords and testing them with a password cracking utility (particularly in the case of administrative level account) the security of the system is greatly enhanced.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Backups, UPS, and Encryption

If a data file is accidentally or maliciously deleted, or is somehow corrupted, the only recourse is to either recreate the data from scratch or restore from a backup. Recreating the data invalidates its integrity; there is no way to prove that the 'new' data is the same as the original. In some cases, re-creation may not even be possible; in others, it may too time consuming or labor intensive to do so. Restoring from backup is the only reliable way to recover from data loss.

Backups can take many forms – saving a copy of a file to a floppy disk, and storing the disk in a safe location, is considered a simple form of backup. The most common type of backup is through the use of a backup utility; most often these backups are made to disk or tape.

The Windows operating system includes a backup utility that is fast and easy to use. When the program is run, a backup wizard walks the user through the process of selecting files, choosing a backup destination, and running the process; for the home user, this is probably the best solution.

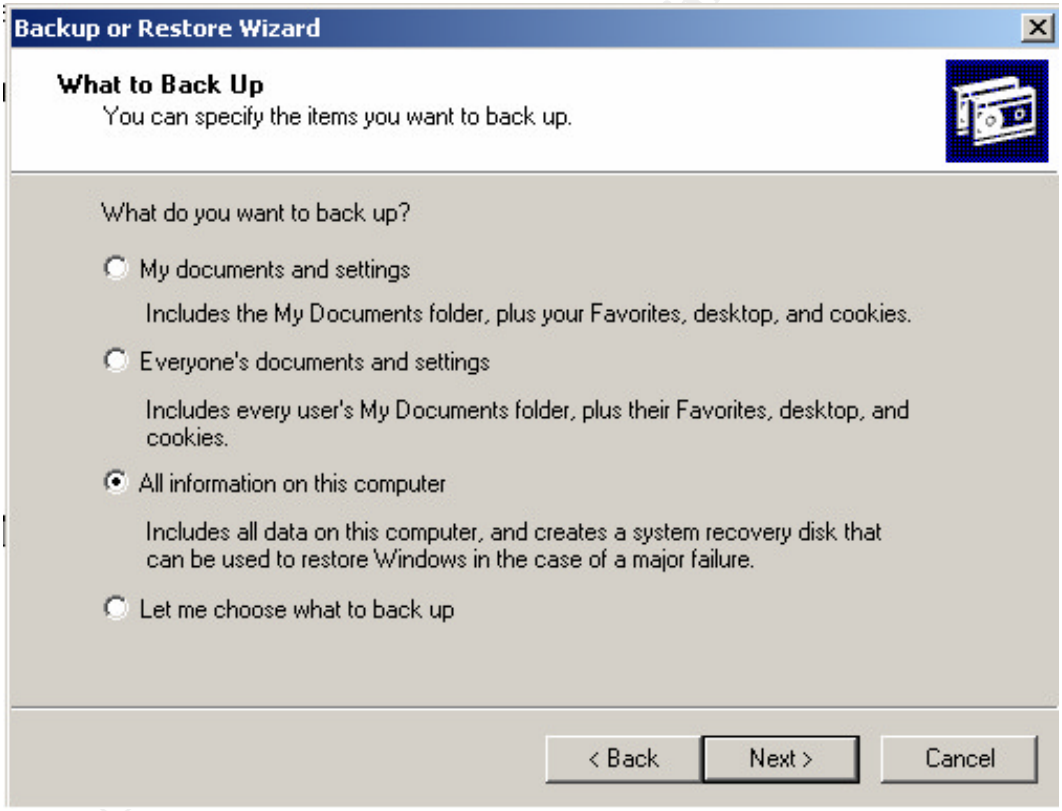


Figure 6 – Windows Backup Wizard

It is important to perform backups on a regular basis to insure that the data contained in the backup set is current. The frequency of backups will depend on how often new files are created, how often data changes, and the criticality of the data; generally, home users should perform a backup on a monthly basis. Businesses, on the other hand, will need to do this more often – weekly, or even daily backups are common. The backup frequency and other related details should be stated in the backup policy.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

When scheduling backups, it is important to create multiple backup sets. One of the most common methods is to rotate between three different sets of disks or tapes, as illustrated below:

- WEEK 1 – backup set #1
- WEEK 2 – backup set #2
- WEEK 3 – backup set #3
- WEEK 4 – backup set #1
- WEEK 5 – etc….

In this way, if one of the backups is lost, damaged, or corrupted, the backup set from the previous week can be used to restore the data. While the older version may not be completely up to date, it is still better than losing the data entirely.

If possible, backups should be kept off-site, or in a fireproof safe. This helps to insure that the backups will be available when needed, and will not be damaged or destroyed in the event of a fire or other catastrophic event.

Finally, backups should be tested regularly to verify that the data can be restored if needed. Testing consists of restoring one or more files to an alternate location, to make sure that the data can be read from the disk or tape, and that the hardware and software are functioning correctly. Again, the frequency and degree of testing will be defined in the backup policy.

Reliable power is probably the most common problem facing home computer users. A summer thunderstorm or winter ice storm can render whole neighborhoods without power for extended periods. Even something as simple as a car hitting a power pole has been known to leave homes in the dark for hours. If the power fails while the computer is on – particularly if there are files open – the results could be disastrous. An uninterruptible power supply (UPS) can mean the difference between an inconvenience and a corrupted computer.

A UPS is essentially a battery backup – if the power goes out, the UPS supplies power from its internal battery, allowing time to perform a clean, safe shutdown of the computer. The UPS is connected in-line between the computer and the home power source – the unit is plugged into the wall socket, and the computer equipment is then plugged into the UPS.

The more equipment that must be protected, the larger and more powerful the UPS must be. Power supplies are rated by voltage, most often expressed as VA (Volt-Amps). The average home system consisting of a computer, monitor, and printer can be powered for up to 20 minutes on a small, entry-level unit running at 400-500 VA. For an environment with more equipment, or if a longer battery life is required, a higher rated unit is recommended.

A more advanced UPS may also be able to act as a line conditioner. A conditioner filters the incoming power, eliminating or reducing spikes and surges to deliver consistent power to the device(s). It is not uncommon to use a surge suppressing power strip in conjunction with a UPS to obtain the cleanest, most reliable power possible.

If an attacker manages to bypass the firewall, obtain an administrative password, and get to the data, the last line of defense is encryption. By encrypting the data, the files are rendered unreadable by anyone except the person who originally encrypted them.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

There are many different algorithms in use for encrypting data; the most common are DES, 3DES, and AES. The strength of an algorithm is measured in bits – DES, a 56-bit key, is considered insecure by today's standards (Kaufman, Perlman, Speciner, 2002). 3DES encryption is achieved by performing a DES encryption process on the data three times using two different keys, resulting in the equivalent of a 112-bit encrypted cyphertext. By contrast AES256, which uses a 256-bit key, is considered the most secure encryption algorithm available; it is the standard used by the federal government for encrypting data.

Some versions of Windows have encryption capabilities built in; others require a third party solution. The most common of these is Pretty Good Privacy (PGP) from PGP Corporation. PGP Mail encrypts email, files, and instant messages and also provides the ability to manage PGP keys. PGP Disk transparently creates volumes whose contents are encrypted when not in use (PGP Corporation, 2004).

The diligent use of backups to recover lost or corrupted data, the installation of a UPS to ensure system availability, and the use of encryption to guarantee confidentiality, are important considerations when implementing an information security program. The security policy should address all of these areas - either justifying their use, or stating the reason for their exclusion while acknowledging the risk.

Configuration and Patch Management

Proper configuration of the system is important if a security program is to be effective. The Microsoft Windows operating system is known to have many bugs and vulnerabilities; the impact of these bugs can be reduced or eliminated by properly configuring the computer.

As stated previously, communication services function by using ports. These ports are often left open when the service is not in use; attackers use these open ports to exploit vulnerabilities in the system. Many of these services are unnecessary and can be shut down, thereby closing the port and eliminating the associated vulnerability.

The File and Print Sharing service is a good example of this. Installed and enabled by default, the service allows users to share files and other resources on the computer with other users on the same network. Most home users only have a single computer, or the computers do not connect to a network, and have no need for this service. By removing this service the ports are closed and the associated vulnerabilities are eliminated.

Similarly, the Workstation service is usually not required on a home system; this service is normally needed only in a network environment. By disabling it, the computer is safe from attacks using the associated port.

Care should be taken when deciding which services to disable or remove. The removal of a needed service may render the computer unstable or unusable. If the user is unsure about disabling a service, or making any configuration changes to the computer, a professional should be consulted.

Maintaining the computer in proper working condition is essential to the ongoing security of the system. Just as the anti-virus program must be kept up to date, so must the operating system and application programs. Vendors release patches and/or service packs to address vulnerabilities found over time, and to enhance the overall security and functionality of the system.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Patches and hot-fixes are small pieces of code meant to address a single issue. Service packs are larger, more complete upgrades that often contain many previous patches and hot-fixes. Generally speaking, a patch is released fix a specific problem, while service packs address overall system functionality.

When a new vulnerability is discovered in a program, the vendor will write and release a patch to address the problem. Many of today's worms and viruses take advantage of these vulnerabilities; systems that are not kept up to date with patches and hot-fixes are the target, and are one of the reasons that these new threats spread so quickly and have such a great impact. Vendors write patches to try to prevent these threats from harming systems; people often do not understand the need, and never bother to install them.

Microsoft and other vendors have taken great strides to make patch management easy – the Windows Update website will scan the system for needed patches, and install them automatically. This same functionality is also available for the Microsoft Office productivity suite. Windows XP even has the capability built in to check the website regularly for patches, and can be configured to install them automatically. The trade-off is that a port must remain open on the system for this to function; while no vulnerability currently exists, it is likely only a matter of time before one is found.

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS

Summary

This study has attempted to show that computers, particularly those connected to the Internet, are inherently insecure. Operating system flaws, application program bugs, and misconfigured systems all contribute to this situation; by taking the time and effort to investigate and remediate these vulnerabilities, a relatively secure computing platform can be achieved.

A vulnerability, by definition, is a flaw or weakness in a system that could be exploited to gain unauthorized access; a threat is defined as the means to exploit a particular vulnerability. By carefully evaluating the system, identifying vulnerabilities, and implementing appropriate counter-measures, the risk associated with these threats can be significantly reduced. While there will always be security risks associated with a computing system – no security plan can eliminate risk entirely – the level of residual risk can be controlled.

The process of identifying vulnerabilities, threats, and risks to a system is known as risk analysis. A thorough risk analysis is the foundation of a good security plan, and helps define the measures that will be taken to reduce or control the risks. This process begins with an inventory of the assets to be protected, and involves several steps (Bragg, 2003):

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Asset Identification – create a list of the assets to be protected
2. Asset Valuation – determine the relative value of the assets
3. Threat Identification – identify the threats to each asset
4. Loss Potential – evaluate the impact of each threat to an asset
5. Risk Assessment – determine the likelihood of the threat occurring
6. Risk Cost – evaluate the impact relative to risk probability
7. Remediate – investigate and implement counter-measures

The result of following these steps will be a security policy, or policies, that define – at a high level – the processes and procedures needed to secure the system(s). This policy becomes the baseline for all remediation efforts, and defines the correct and appropriate measures to be taken. By following the policy, the computing environment can be made secure and the residual risk can be managed.

In the first step it is important to identify and include all types of assets: hardware, software, and data – both electronic and hardcopy. The more thorough the inventory, the more accurate the risk assessment will be. As this is the foundation of the rest of the process, comprehensiveness and accuracy are essential.

Having the inventory, the second step is to assign a value to each asset. This can be accomplished in either of two ways – the quantitative method is based on actual dollar value; the qualitative uses a more subjective scale, such as High, Medium, and Low. Of these two methods, the qualitative is the more common, as it is easier to understand and implement.

Threat identification, as its name implies, lists the vulnerabilities and threats to each asset. At this stage, there is no consideration given to the likelihood of the threat occurring, only the identification and definition of the various threats.

Loss potential is a cross-reference of the threat to the asset with the value of that asset. This process results in a clear understanding of the impact that the stated threat would have on the asset, and on the overall system. This impact analysis still does not take into consideration the probability of the threat – that is done in the next step.

It is in the risk assessment step that likelihood of the threat occurring is taken into account. This can also be done in either of two ways; again, the most common is to assign a probability of High, Medium, or Low. The result is a clear picture of the actual, quantifiable risks to the system; with this knowledge, the final cost of the risk can be determined.

While the loss potential might be very high, the actual risk could be very low, resulting in a low risk cost. In this step, the relative cost of the risk is ascertained, and an understanding of the cost to value ratio gained. It is this value that is used to justify the cost of any remediation efforts.

The result of the first six steps is the development of a security policy that defines and documents the appropriate processes and procedures to be used to counter the threats identified. This is generally a high-level treatment of the subject; no specific technology or process is mandated. Security policy is the framework within which all security efforts are defined and justified.

The remediation step is where the actual technology, processes, and procedures are investigated and implemented. The cost of a particular counter-measure is weighed against the risk cost to determine if the measure is appropriate for the situation; in this

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

way, a cost-effective solution can be attained that meets the individual needs of the system to be protected.

The study then attempted to identify and explain some of the more common counter-measures available – strong passwords, anti-virus, firewalls, and other means of risk reduction. In each of these areas, some level of detail was provided and, where appropriate, recommendations made for implementation and use.

The use of passwords is a cost-effective means of providing both confidentiality and integrity to systems and files. By applying passwords to critical systems and files, confidentiality and integrity are enhanced; using strong, complex passwords further improves this effort. The cost and effort required to implement a password policy is negligible and the process is easily understood by most users, making it one of the first remediation efforts that should be explored.

An anti-virus application should also be at the core of a good security program. Viruses and worms are the most common threat against systems today; an anti-virus program will protect against this threat with little effort and cost. In order for this effort to be effective, the application must be kept up to date; most anti-virus programs available today have built in capabilities to automatically update the program when new virus signature files or software upgrades become available. Anti-virus programs work to insure the integrity and availability of systems and files.

The firewall is likely the best known, and least understood, security device available today. Firewalls come in both hardware and software varieties, and function in several different ways, including packet filters, application proxies, and stateful inspection. Many firewalls also have the ability to perform intrusion detection, blocking activities that appear to be hostile in nature. The firewall is also considered part of the core of the security program. Firewalls help to guarantee the confidentiality and integrity of the system.

Once a security program is developed and implemented, it must be tested to insure that it is functioning as intended, and that the desired reduction in risk is obtained. The use of vulnerability scanners will help to verify the security posture of a system, and identify those areas that are still vulnerable. Care should be taken when using these tools, as serious damage can result from the inadvertent use of a feature in the program.

No security plan would be complete without a backup policy. Backups of critical files are used to restore those files in the event of loss, damage, or corruption. The backup policy insures that the integrity and availability of needed files is maintained, and allows recovery from even catastrophic events.

An uninterruptible power supply helps prevent system damage or file corruption due to a sudden loss of power. Some UPS units also function as line conditioners, delivering clean power in the event of a spike or surge in the main power supply. In the event of a power outage, the UPS supplies battery power to the system, allowing time to safely close any open data files and perform a clean shutdown of the computer. This helps insure the integrity and availability of the system and its data.

Encrypting data files renders them unreadable to anyone except the person who originally encrypted them, or anyone who has the correct decryption key. Encryption algorithms are rated by their key length; the AES-256 algorithm is considered the strongest encryption available today. Encryption can be applied to data at rest (stored

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

on a hard drive or other disk) or in transit (as in email). The ability to encrypt data is built in to some Microsoft operating systems; third party applications are available that extend this functionality. Encrypting data helps to guarantee its confidentiality and integrity.

Attacks against computers are made via open ports; vulnerability scanning identifies which ports are open on the system. Ports are most often controlled by services; disabling or removing unnecessary services closes the corresponding ports, and secures the computer against attacks that may use them. The File and Print Sharing and Workstation services are examples of services that can usually be disabled. Proper system configuration also serves to help prevent data loss from system crashes or other unexpected events. By maintaining the system configuration in an optimal state availability, and to a lesser extent integrity, is assured.

Patch management is the process of upgrading the system when new software, patches, or fixes become available. As new vulnerabilities are discovered, a patch or hot-fix is generally available to address the issue. By diligently applying patches and service packs, exposure to new threats is reduced and the confidentiality, integrity, and availability of the system is secured.

Implications for Individuals

With the advent of broadband Internet service, the individual home user has become a greater target for attackers. These type of direct connections, most often provided by cable and phone companies, present an 'always on' connection – as long as the computer is powered on, it is connected to the Internet. This situation provides a wide-open opportunity for attackers to gain unauthorized access to the computer and its data. There are two security solutions that should be considered essential for the home user: a firewall and an anti-virus program.

While it may seem excessive for a home user to spend the time and effort to perform a complete risk analysis and develop a security policy, it is through this exercise that vulnerabilities are found, needs are identified, and solutions are justified. The cost, both in time and money, is far less than the expense that would be incurred if credit card or other personal information were to be stolen and used by an attacker.

It may be impractical for a home user to perform a vulnerability scan on his/her own system, or implement encryption on data files, therefore due diligence must be exercised in disabling services, patching systems, and identifying and implementing other appropriate security measures. This can only be achieved by analyzing their exposure to threats, and gaining an understanding of the benefits of developing a security program.

Implications for Business

Businesses rely more on the Internet for sales, customer support, and advertising than ever before. This increase in Internet exposure also means an increase in exposure to attack. Where an individual need only worry about protecting their personal information, businesses must be concerned with safeguarding customer information as well. This places an extra security burden on the business, and requires a much more formal approach to information security.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

There has recently been an increase in the number of government regulations around information security. HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley – these government acts all seek to legislate the privacy and confidentiality of information, with severe penalties for non-compliance. This added pressure makes an information security program a necessity in most business scenarios.

A formal risk analysis is essential to the development of a security plan; in some cases, federal regulation requires that one be performed. From this analysis, business owners and managers can begin to asses their level of exposure, and from there to determine what must be done to achieve or maintain regulatory compliance. The cost of non-compliance far exceeds the cost of developing and implementing a formal policy, and from there, a security plan.

Again, a firewall and an anti-virus program appear to be essential components of a security plan. In addition, a backup policy, password policy, and – in some cases – encryption policy are important areas to consider. In a slow economy these measures may not appear to be cost effective; one need only look at the possible penalties to see that this is not the case. A risk analysis, if done properly, will likely show that these are important considerations in the security plan. Further, it should be apparent that the security plan needs to be a part of the overall business plan if it is to succeed.

Conclusion

In today's interconnected world - with the increase in viruses, worms, and identity theft – it is no longer an option to avoid implementing an information security program. The home computer user is rapidly becoming the favorite target of computer attacks, and businesses are finding themselves hard-pressed to comply with new regulations.

By following the program outlined in this study, both individuals and businesses can enhance the security of their systems and data. While the level of detail required will differ from case to case, the principles laid forth in this paper will guide the process to a satisfactory conclusion.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

BIBLIOGRAPHY

Anonymous. (2001). *Maximum security: A hacker's guide to protecting your internet site and network* (3rd ed.). Indianapolis IN: SAMS

Berger, B. (2003). *Data-Centric Quantitative Computer Security Risk Assessment*. Retrieved February 1, 2004, from http://www.sans.org/rr/papers/index.php?id=1209

Bragg, R. (2003). CISSP: Certified Information Systems Security Professional Training Guide. Indianapolis IN: QUE Publishing

CERT® Coordination Center. (2002). *Home Computer Security*. Retrieved January 31, 2004, from http://www.cert.org/homeusers/HomeComputerSecurity/home_computer_security.pdf

Harris, S. (2002). *Mike Meyers' CISSP Certification Passport*. Berkley, CA: McGraw-Hill/Osbourne

CERT® Coordination Center. (2001). *Before You Connect a New Computer to the Internet*. Retrieved January 31, 2004, from http://www.cert.org/tech_tips/before_you_plug_in.html

Kaufman, C., Perlman, R, & Speciner, M. (2002). *Network security: private communication in a public world* (2nd ed.). Indianapolis IN: QUE Publishing

McAfee Security (2004). *McAfee Security Anti-Virus Tips: Virus Detection and Prevention Tips*. Retrieved March 6, 2004, from http://www.networkassociates.com/us/security/resources/av_tips.htm

Mueller R. (2003). *The FBI: Meeting New Challenges*. Retrieved January 23, 2004, from http://www.fbi.gov/pressrel/speeches/npc062003.htm

Ogletree, T. W. (2000). *Practical firewalls*. Indianapolis IN: QUE Publishing

PGP Corporation. (2004). PGP Personal Desktop (Windows XP version). [Computer Software]. Palo Alto, CA: PGP Corporation

Pollock J., & May, J. (2002). *Authentication technology - identify theft and account takeover* [Electronic version]. FBI Law Enforcement Bulletin, Retrieved January 23, 2004, from http://www.fbi.gov/publications/leb/2002/june2002/june02leb.htm

SANS Institute. (2003). *SANS Glossary of Terms Used in Security and Intrusion Detection*. Retrieved January 23, 2004, from http://www.sans.org/resources/glossary.php

SANS Institute. (2003).*The SANS Security Policy Project*. Retrieved February 6, 2004, from http://www.sans.org/resources/policies

Visintine, V. (2003). *An Introduction to Information Risk Assessment*. Retrieved February 1, 2004, from http://www.sans.org/rr/papers/index.php?id=1204

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

APPENDIX A - Security Resources

@Stake - http://www.atstake.com
Cain & Abel – http://www.oxid.it
CERT Coordination Center – http://www.cert.org
Cisco Corporation – http://www.cisco.com/security
Federal Bureau of Investigation - http://www.fbi.gov/hq.htm
GFI Software – http://www.gfi.com
Insecure.org – http://www.insecure.org
Internet Security Systems - http://www.iss.net
LinkSys Corporation – http://www.linksys.com
McAfee Security - http://us.mcafee.com/default.asp
Microsoft Corporation – http://www.microsoft.com/security
Nessus – http://www.nessus.org
Network Associates – http://www.nai.com
SANS Institute – http://www.sans.org
Security Focus – http://www.securityfocus.com
Snort – http://www.snort.org
Symantec Corporation – http://www.symantec.com
Tenable Network Security - http://www.tenablesecurity.com
U.S. Computer Emergency Readiness Team - http://www.us-cert.gov
Zone Labs – http://www.zonelabs.com

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.