



Network System Architects
Engineering Solutions For Business Problems

NETWORK SECURITY ASSESSMENT

WHITE PAPER

Will Spencer
Network System Architects, Inc.
<http://www.nsai.net>

© Network System Architects, Inc.
20 April 2000

COPYRIGHT NOTICE

Network System Architects, Inc. (NSAi)

This document and the information contained here is the subject of copyright and intellectual property rights under international convention. All rights reserved. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided "as is" without any expressed or implied warranty.

Network System Architects, Inc. (NSAi)

1550 Larimer St., Suite 222
Denver, CO 80202

1. EXECUTIVE SUMMARY

Network security assessment is the single most effective method for assuring your organizations information assets are secure against intrusion. This document discusses the process of conducting an effective network security assessment.

2. INTRODUCTION

Enterprise networks are becoming more complicated every day. At the same time, greater amounts of sensitive and valuable corporate information are being stored on computers connected with those networks. It is imperative to the survival of any business enterprise that data on the corporate enterprise Intranet be protected from both business competitors and malicious hackers.

In the past, managing a small number of network connections could adequately protect a corporation's information assets. The integration of business Intranets and the Internet have increased the complexity of this task exponentially. Likewise, the move toward employees working at home and on the road has significantly increased the difficulty of controlling access to the corporate Intranet.

Clearly, protecting the corporate Intranet is a business critical task. Unfortunately, the use of information technology is growing at a pace far exceeding the ability to manage that growth. Departments within corporations and end users at all levels have the capability to implement systems and procedures that make corporate information assets open to outside attack. A single modem residing on a personal computer can provide an attacker all he or she needs to gain access to the total information assets of a corporation.

Management needs some method of assuring that every information asset of the corporation is protected. It is not enough to create security policies; management must have a method for assuring that those policies are being followed. It is easy enough to force a user to change a password; however, changing the password after a break-in is not enough. Management must be assured that the corporate Intranet is secure today, before any damage is done.

The FBI's National Computer Crime Squad estimates that between 85 and 97 percent of computer intrusions go undetected. This alarming statistic proves that there is a far greater problem than corporations not knowing that their networks are vulnerable; most actually fail to realize when valuable corporate information has already been stolen. Clearly, these undiscovered breaches of network security represent a great risk to the financial health of the corporation.

How do you ensure that your corporate information assets are protected? Good Information Technology (IT) practices play an important role. Communication of corporate security policies to all users plays a role. Centralized control of network connectivity plays a role. None of these, however, is sufficient.

The single most effective method for assuring your network is secure against intrusion is to attack it. By entrusting a highly skilled engineering team with the task of attacking your network, you can be made aware of security vulnerabilities in your network that would not be known to you by any other method.

The engineering team places itself in the mindset of your top competitor, or of a malicious hacker determined to penetrate into the depths of your information infrastructure. The engineering team then analyzes your information resources with the intent of discovering the vulnerabilities in your corporate security. Your Internet connections are examined, as well as your telephone connections and any connections to other networks. The management of most corporations are amazed to discover how many external connections into their network are available to the determined attacker.

A written report, often accompanied by a presentation is issued. After the Information Systems staff has been given an opportunity to correct the vulnerabilities outlined in the report, a second attack is recommended to confirm the new, more effective, security posture.

3. THE ASSESSMENT PROCESS

Several phases are required to provide a complete attack against any network in order to provide a comprehensive picture of the overall security posture of a network. The first phase in an external assessment of enterprise security is the Remote Data Collection Phase. In this phase, the engineering team will determine where your enterprise network may be vulnerable to attack. The Engineering team will search for Internet domains and addresses belonging to your company. They will also search for ranges of telephone numbers that your company leases from the telephone company. Online research is often accompanied by research of your company at the library and telephone calls to selected employees.

Once this information is collected, the Engineering team will conduct a Data Sorting Phase in which they determine where to attack your network. The Engineering team gives the highest priority to corporate information assets that are vulnerable and potentially valuable. Once the Data Sorting Phase is completed, work will continue with the Remote Attack Phase. The Remote Attack Phase is concerned with actually penetrating your corporate Intranet. The engineering team takes extreme care to ensure that no interruption of service is caused. Servers and workstations belonging to your corporation are accessed and a working map of accessible portions of your corporate Intranet is made. The engineering team makes every attempt to gain access to as much of your corporate Intranet as possible.

The penetration exercise continues with the Local Attack Phase. The purpose of the Local Attack Phase is to expand the level of access gained within each host on your network. For example, if the Engineering team is able to access a machine HR-SERVER as user Bob, they then attempt to upgrade access to SUPERVISOR.

The last of the penetration phases is the Local Data Collection Phase. In the Local Data Collection Phase, the hosts and accounts accessed are searched for information. Data collected in this phase is then used in a new Remote Attack Phase. These three phases are repeated until no new data is collected in a Local Data Collection Phase.

This effort is followed up with the Reporting Phase. In the Reporting Phase, you are presented with a written report detailing the vulnerable spots in your corporate information infrastructure. Your Information Systems staff can take this data and shore up your network defenses against attack. Common measures that have to be implemented are changing user passwords to secure passwords, removing analog telephone lines to user workstations, applying recent patches to server operating systems, and securely configuring servers that provide services to the Internet.

3.1. The Remote Data Collection Phase

The Remote Data Collection Phase can be started from a number of different points.

- Analysis of only specific systems.
- Analysis of all systems, some of which are known beforehand.
- Analysis of all systems, with no data known beforehand.

An analysis of only specific systems occurs when you have a list of systems under your management and authorize a penetration analysis of only those systems. This type of penetration analysis is appropriate when you manage only a subset of hosts within an enterprise or when you cannot allow certain mission critical systems to be analyzed. In this type of penetration, the Chief Information Officer will provide a conclusive list of hosts to be attacked and the specific authorized methods of connecting to those systems.

An analysis of all systems, some of which are known beforehand, is the most common type of analysis. Most Chief Information Officers can provide information as to the IP address ranges used by their organizations, telephone number ranges assigned to their organizations, and X.25 or other network addresses used by their organizations. However, a penetration analysis often discovers access methods to the corporate network that were previously unknown to the CIO.

An analysis of all systems, with no data known beforehand, is the most difficult type of analysis. This simulates an attack by someone with no prior knowledge of your corporate information infrastructure. In this type of penetration, the Chief Information Officer gives no information at all to the Engineering team. This greatly extends the time and effort required in the Remote Data Collection Phase, but also yields the most realistic results.

3.2. The Data Sorting Phase

The Data Sorting Phase does not involve any contact with your corporate Intranet. The Data Sorting Phase is a strategy phase in which the Engineering team determines where to attack your network. The Engineering team reviews all information discovered in the Remote Data Collection Phase, which usually consists of thousands of pages of data. The Engineering team bases its decisions on two criteria:

- How vulnerable is the information?
- How valuable is the information?

The Engineering team determines how vulnerable a system might be based upon the data collected in the Remote Data Collection Phase. If it is possible that the system contains valuable data, or that the system might be used as a gateway to other systems in your corporate Intranet, the system is attacked in the Remote Attack Phase.

3.3. The Remote Attack Phase

The Remote Attack Phase is when the skills and experience of the Engineering team really come into play. Unlike the Remote Data Collection Phase, which often utilizes automated tools; the Remote Attack Phase is a largely manual process. For example, if the Remote Data Collection Phase discovered that one of your hosts was exporting a file system using NFS, the Engineering team would attempt to break into that system using approximately 30 known vulnerabilities in various NFS implementations.

At NSAi, we maintain a database of over 1,400 known security vulnerabilities. NSAi engineers maintain this vulnerability database utilizing a variety of sources, including: Hardware and software vendors

- Security organizations (CERT, etc...)
- Security mailing lists (Bugtraq, etc...)
- Monitoring the "hacker underground"

- Research by NSAi Engineers

This extensive database allows us to be extremely confident when we report on the security of your network. Organizations with a less fully developed vulnerability database cannot provide any real assurance regarding the security of your corporate information infrastructure.

3.4. The Local Attack Phase

The purpose of the Local Attack Phase is to upgrade the access to your corporate Intranet that was gained in the Remote Attack Phase. If the Engineering team was able to login to a user account on a Unix system, they will attempt to gain root level access on that system. If user level access was gained on a Novell 3.x server, the Engineering team will attempt to gain SUPERVISOR access. If a Windows NT login was compromised, the Engineering team will attempt to gain Administrator access.

3.5. The Local Data Collection Phase

NSAi Engineers examine hosts penetrated in the Remote Data Collection Phase during the Local Data Collection Phase; searching for two types of data:

- Data of Value to Your Organization
- Data of Value to Gain Further Access

Data of value to your organization is collected to demonstrate the losses that may have occurred to your corporation in the past. Your confidential corporate data may not have been as confidential as you thought. This type of data is often useful in gaining the cooperation of department heads, which often believe that security problems simply do not occur in their departments. This part of the Local Data Collection Phase is optional, as certain clients request that their data be examined as little as possible.

Data of value to gain further access is collected in an attempt to gain access to other systems on your corporate Intranet. This data includes:

- The /etc/hosts file (Unix)
- The /etc/hosts.equiv file (Unix)
- Every .rhost file on the system (Unix)
- The /etc/exports file (Unix)
- The UUCP configuration files (Unix)
- The /etc/resolv.conf file (Unix)
- The /etc/passwd file and any accessible shadow password file (Unix)
- Routing table (Unix and Windows NT)
- Network connections (Unix and Windows NT)
- Network shares (Windows NT)
- Network password policies (Windows NT)
- Network view (Windows NT)
- Network groups (Windows NT)

- Network users (Windows NT)
- Remote name cache (Windows NT)
- Session table (Windows NT)
- Show accounting (VMS)
- Show audit (VMS)
- SYSAUF.DAT (VMS)
- Access codes (OS/400)
- Audit journal entries (OS/400)
- Authorized users (OS/400)
- Expiration schedule (OS/400)

At this point, the Engineering team takes any information gained and returns to the Remote Attack Phase. These three phases are then repeated until no further information is gained in a Local Data Collection Phase.

3.6. The Reporting Phase

The Reporting Phase is when everything comes together. This phase always consists of a written report detailing the vulnerabilities discovered in your corporate Intranet. This is often accompanied by a meeting with the Chief Information Officer or with the Chief Information Officer and several of the people responsible for correcting the vulnerabilities discussed in the report.

4. CONCLUSION

A network security assessment should not be an academic exercise. The purpose of a network security assessment is to point out potential problems so that they may be repaired before damage to the organization occurs.

Many organizations choose to contract NSAI to repair the vulnerabilities discovered in the analysis. Organizations that do not have a full-time information security team, or even a full-time information security officer, may choose to contract NSAI to conduct quarterly reviews of their security posture.

In addition, NSAI can provide security policies custom tailored to your organization. These written policies provide guidelines to assist your staff in protecting your corporation's information assets.