INSPECTOR GENERAL

IG-U-042

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, D.C. 20436

September 25, 1997

**MEMORANDUM**

TO: Director, Office of Information Services

FROM: Inspector General Jane E. Altenhofen

SUBJECT: Inspection Report No. 04-97: Vulnerability Assessment of the Commission's Automated Information Systems

We initiated this inspection in August 1997 as a follow-up to the findings and recommendations made in Audit Report No. IG-01-96, Audit of the USITC Local Area Network Operations. That report identified weaknesses in the adequacy of the Commission's Local Area Network (LAN) security.

Our objective was to assess the potential vulnerability of Commission automated information systems to unauthorized access from external sites. We found that, within the limited parameters of this assessment, we were unable to obtain unauthorized access to the Commission's internal network through either the publicly accessible Internet gateway or telephone connections. However, certain vulnerabilities were identified that could potentially be exploited to obtain such access. The results of our inspection are summarized below and presented in entirety in the vulnerability assessment transmitted with this memorandum.

**Background and Scope**

Since 1988, the Commission has invested substantial resources to automate agency functions and implement a LAN. As of September 1997, the Commission's LAN consisted of 11 file servers running Banyan Vines 5.5; several special application servers, such as for facsimile messages; and approximately 400 personal computers as work stations. The LAN supports a variety of office automation functions, including word processing, electronic mail, spreadsheets and end-user database applications. The system contains unclassified as well as sensitive information, such as confidential business information.

The Office of Inspector General (OIG) contracted with the Computer Sciences Corporation (CSC) to conduct a limited vulnerability assessment of the Commission's LAN. The fieldwork was done from August 29 through September 2, 1997. CSC assessed the vulnerability of the Commission firewall and surrounding computer components. CSC also performed a "wardialing" exercise against the Commission's telephone system to identify weaknesses in access to the system through modems. These tasks were performed from the CSC Commercial Laboratory site in Maryland using CSC proprietary and freeware tools. The OIG provided CSC with the Commission's Internet Protocol addresses, the make of it's firewall, and the range of telephone numbers assigned to the Commission. This information was obtainable by CSC through other means, but for the sake of economy was provided by the OIG.

**Summary of Results**

CSC's scan of the Commission's network identified seven hosts that linked the Commission's automated systems with the Internet. A host is any machine with an Internet address; hosts that are linked to a system provide a potential entry point. The seven hosts identified were outside the firewall. CSC was unable to penetrate into the Commission's internal network through the firewall. However, CSC did identify six potential vulnerabilities surrounding the host machines.

The vulnerabilities provide no direct access route to the Commission's internal system, although given the present state of the hosts and with a sufficient amount of time, an intruder could probably obtain some form of unauthorized access, which is undoubtedly true of any computer systems. According to OIS, the most serious threat would be mutilation of the Commission's external Internet website and possible denial of access to the Internet for Commission staff.

In the second phase of the vulnerability assessment, CSC attempted to access Commission automated information systems through modems attached to various servers. CSC identified 65 modems within the range of numbers we provided; 51 of these were later found to be numbers no longer belonging to the Commission. The 14 lines belonged to OIS or other offices, indicating that staff appear to be complying with Commission policy prohibiting individual dial-in connections.

All of the modems were called back, and five of the fourteen Commission modems offered a connection to login prompts. All five of these connections were to OIS-managed devices which were specifically provided to allow staff dial-in access to Commission resources. CSC made a very limited attempt to log on to the system by trying carriage returns and some commonly used passwords, but was unsuccessful. A more serious effort to gain access via the modems may have been successful.

**Suggestions**

We suggest that the Director of Information Services implement the recommendations made on pages 4 and 5 of the vulnerability assessment report in order to more fully secure the Commission's automated information systems.

The Director of OIS agreed to implement the recommendations in the report even though the vulnerabilities do not constitute a significant threat. We agree with OIS that the quality of the systems put in place to secure agency resources is such that implementing the recommendations will improve security, but not substantially.

The above procedures constitute an inspection made in accordance with the President's Council on Integrity and Efficiency Standards for Inspections.

If you have any questions, please contact me on 205-2210.

cc: Commission

# International Trade Commission Vulnerability Assessment Report

September 8, 1997

Computer Sciences Corporation
Systems Engineering Division
Technology Focus Center
7459 Candlewood Road
Hanover, MD 21076

# Table of Contents

# 1 OVERVIEW

This document describes the vulnerability assessment conducted by Computer Sciences Corporation (CSC) for the International Trade Commission (ITC), involving the ITC's firewall and surrounding computer components. CSC also performed a "wardialing" assessment against the ITC telephone system. The task was performed from the CSC Commercial Laboratory in Hanover, MD, using CSC proprietary and freeware tools.

# 2 TOOLS

## 2.1 Hydra

Hydra is a CSC proprietary software tool that is made up of several different programs, each of which performs a particular scanning or penetration task. The core programs are listed below:

- Subscan - scans a range of IP address, and reports all existing devices, including hosts, routers, printers, and terminal servers.
- Probe – checks devices discovered by Subscan for network vulnerabilities that lead to unauthorized access on the device.
- Analysis - generates detailed vulnerability reports, using databases created by Subscan and Probe.

## 2.2 Strobe

This tool scans a host for all active TCP ports from 1 to 65535. It can provide information about what services are being offered by the host.

## 2.3 Whois

This is an information service available on the Internet that provides information about companies and domains that exist on the Internet. This information usually provides a list of DNS servers that the particular company or domain is served by.

## 2.4 Traceroute

Traceroute is used to discover the network path from one host to another. It does this be having each host in the path return information back to the originating host, which gathers the information and displays it in a table showing IP addresses, host names, and response times.

### 2.5 NSLookup

NSLookup is a standard Unix tool used to send host name queries to arbitrary Domain Name Service (DNS) servers. Provided that a server is not restricting access to information, NSLookup can gather a list of all host names and their corresponding IP addresses within a particular DNS domain.

### 2.6 Samba

Samba is a set of tools allowing access to Microsoft Network share resources. This tool can be used to read from or write to shared Windows NT file directories from a Unix platform.

### 2.7 Netscape

Netscape is a World Wide Web (WWW) browsing client, and is used to examine WWW servers for vulnerabilities, including exploitable CGI scripts.

### 2.8 Toneloc

Toneloc is a wardialer used to dial a large quantity of phone numbers in an attempt to discover modems.. The wardialing process involves the use of Toneloc, an automated software tool which uses the phone range parameters to dial all numbers in the designated range in a random pattern to identify modems within that range.

## 3 METHODOLOGY

CSC used Hydra to scan the Demilitarized Zone (DMZ) of the ITC Internet presence. This DMZ includes the premise router (that connects ITC to the Internet Service Provider), the firewall protecting ITC internal networks, and all hosts located on the LAN segment between. This LAN segment uses the 205.197.120 Class C IP subnet.

CSC used Whois, Traceroute, and NSLookup to gather information about the ITC network connectivity to the Internet. This information can usually provide a starting point for attack and penetration efforts. For example, the Whois utility will provide the name of the DNS server for the ITC. NSLookup can then be used to gather a list of publicly known ITC machines from the DNS server, and Traceroute can be used to discover the network path to the ITC firewall.

Samba was used to attempt connections to any machines that were sharing out resources via SMB (Microsoft Network). It was used to test account availability on NT machines, and to gather NT Domain information about the machines. Strobe was used to gather a list of all active TCP ports on the firewall.

Toneloc was used for the "wardialing" analysis to dial all of the ITC phone numbers. The range of numbers are within the 202-205-xxxx range, and include 1800-2253, 2300-2399, 2501-2599, 2602-2699, 2701-2799, 3101-3399, and 3402-3499

# 4 RESULTS

## 4.1 Network Scan Summary

The Hydra scan of the 205.197.120 subnet identified seven hosts. The one host that it did not identify, however, was the firewall. Though Hydra was able to see that the firewall was present, it was not able to run its normal scans against it. CSC used the Strobe tool to probe the firewall for active TCP ports. These ports were tested using a variety of adhoc methods, but any attempts at exploiting the firewall's services were unsuccessful. The table below indicates the potential vulnerabilities discovered on the other seven hosts, followed by descriptions of those vulnerabilities. Vulnerabilities within DMZ hosts can often lead to unauthorized access through a firewall, usually due to trust relationships between the firewall and the DMZ hosts.

| Host Description | Vulnerabilities |
|---|---|
| 205.197.120.1, probable Cisco router | Telnet and Finger services are accessible from the Internet, and NetBIOS connections are allowed from the Internet. |
| 205.197.120.3<br>(net1.usitc.gov)<br>OS = unknown<br>(seems to also go by net2.usitc.gov) | The SMTP service supports the VRFY command. |
| 205.197.120.5 (**Error! Reference source not found.**)<br>OS = Windows NT 3.51<br>Windows name = ITC-WEB<br>Windows domain = WEBSERVER | The "guest" account seems to be enabled with a NULL password, allowing the two shared resources "columbia" and "heaven" to be mapped remotely. The Event Log and Diagnostics may also be viewed remotely as well. |
| 205.197.120.17<br>OS = Windows NT 4.0<br>Windows name = ITCDB<br>Windows domain = WORKGROUP | No vulnerabilities found. |
| 205.197.120.37<br>(beardog.usitc.gov)<br>OS = SunOS 4.1.x<br>(running NCSA v1.5.1 WWW Server) | A number of CGI scripts, available through the WWW server application, have vulnerabilities allowing remote browsing of the file system (but not the content of actual files). The SMTP service supports the VRFY command, and Finger services are available. |

| | |
|---|---|
| 205.197.120.86<br>(news.usitc.gov)<br>OS = Windows NT 4.0<br>Windows name = NEWS<br>Windows domain = WORKGROUP<br>(running Netscape Mail Server v2.0) | The SMTP service supports the VRFY command. The News services allow connections and transactions from the Internet. |
| 205.197.120.222<br>OS = Windows NT 3.51<br>Windows name = FIRSTSERVER<br>Windows domain = OIS | No vulnerabilities found. |

## 4.2 Network Scan Vulnerability Descriptions and Recommendations

### *4.2.1 Services Accessible from the Internet*

A majority of the machines within the DMZ are directly accessible from the Internet. The router between the DMZ and the Internet Service Provider does no filtering of incoming connections.

It is typically a good idea to have a premise router filter any unwanted connections before they reach the DMZ. If there is no need to allow incoming NetBIOS connections, that service should be disallowed at the router. Any other services not needing to be accessed from the Internet should be blocked as well (such as Finger and News).

### *4.2.2 VRFY Command Allowed*

The SMTP VRFY command allows remote users to query a mail host for valid mail account names. This can often be used to confirm or gather a list of potential target accounts on a machine.

If the SMTP server software permits, the VRFY command should be disabled.

### *4.2.3 NT Guest Account Enabled with NULL Password*

Since the "guest" account is a default account created during the initial installation of NT, it is often a target account for attacks. Some implementations of NT, however, require the "guest" account to exist and be enabled in order for certain services (such as WWW and FTP) to work properly. However, the "guest" account can be used through the NetBIOS protocol to gather information about the server, such as being able to browse through the Event Logs or the Diagnostics output.

Whenever possible, the "guest" account should be disabled, or given a password. In cases where the account can't be disabled, the premise router should block NetBIOS connections to the particular server that has the "guest" account.

### *4.2.4 Vulnerable CGI Scripts*

A number of the sample CGI programs distributed with the NCSA 1.5.1 WWW Server application contain vulnerabilities that allow attackers to obtain directory listings of any directory within the server's file system. These CGI programs include "test-cgi" and "nph-test-cgi".

Any CGI programs not needed should be deleted, and patches applied to those that are needed.

### *4.2.5 Finger Services*

Finger is a service that allows remote users to gather information about accounts on a system. Information about the account, such as the home directory, default shell, owner, and last login time and origin may be obtained. This information can be used to gather information about the accounts on a system, and provide starting information for an attack.

The Finger service should be disabled from all DMZ machines.

### *4.2.6 Publicly Accessible News Server*

The News server in the DMZ allows remote (non ITC) clients to connect and download (and possibly upload) articles from the server. Any ITC information on the server would be available to the Internet.

The server should be configured to only allow connections from designated Internet hosts. Typically, only the main news feed site is allowed access from the Internet.

## 4.3 Wardialing

The following table indicates the wardialing statistics gathered during the dialing vulnerability assessment.

| | Total | Percent of Total |
|---|---|---|
| Numbers Dialed | 1247 | N/A |
| Busy | 66 | 5.29% |
| Voice | 485 | 38.89% |
| RingOut (max rings = 7) | 383 | 30.71% |
| Timeout (wait time 60 sec) | 248 | 19.89% |
| Carriers Detected | 65 | 5.21% |

All of the carriers found were called back, with the intent to exploit the remote answering host. During the dial backs, CSC was unable to exploit any of the carriers, but there was very little time available to work this potential area.. A number of the carriers found appeared to be Point-to-Point dial-up servers, and NT Remote Access Servers (RAS).

# 5 SUMMARY

CSC was unable to penetrate into the ITC internal network through the firewall. Though a number of the hosts within the DMZ had vulnerabilities that CSC could exploit, none of those exploits resulted in privileged control of the machines. Given the present state of the hosts on the DMZ, and with a sufficient amount of time, it is probable that some form of access could be achieved. With that access, and intruder would be able to set up a remote network packet sniffing program to gather information being passed between the ITC internal network and the Internet. It is therefore important that the DMZ hosts be secured.

CSC's wardialing effort turned up a number of modems attached to various servers that could potentially be exploited. A handful of carriers offered connection to login prompts. However, CSC was unable to guess any of the passwords or account named that would give access to the remote host.