U.S. International Trade Commission

Audit of Perimeter Network Security

June 24, 2013

Office of Inspector General

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency that provides trade expertise to both the legislative and executive branches of government, determines the impact of imports on U.S. industries, and directs actions against certain unfair trade practices, such as patent, trademark, and copyright infringement. USITC analysts and economists investigate and publish reports on U.S. industries and the global trends that affect them. The agency also maintains and publishes the Harmonized Tariff Schedule of the United States.

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

June 24, 2013 IG-LL-008

Chairman Williamson:

This memorandum transmits the Office of Inspector General's final report, *Audit of Perimeter Network Security*, OIG-AR-13-09. This audit focused on whether the Commission's perimeter defense was effective. In finalizing this report, we analyzed management's comments to our draft report and have included those comments in their entirety as Appendix A.

This audit found that the Commission's perimeter defense was effective, and it identified two areas for improvement. This report presents seven recommendations to further secure the Commission's perimeter.

Thank you for the courtesies extended to the auditors during this review.

Philip M. Heneghan
Inspector General

Table of Contents

Results of Audit

The purpose of this audit was to answer the question:

Is ITCNet's perimeter defense effective?

Yes. ITCNet's perimeter defense is effective.

We assessed the Commission's perimeter defense and were unable to gain unauthorized access to the Commission's systems. The Commission's perimeter defense continues to be effective.

A penetration test is an attempt to breach a network and gain unauthorized access to its resources. In July, 2012, we conducted a penetration test of the ITC network using public information. Our search for public information on the ITC network servers identified a network range of 64 IP addresses known to host ITC services. We used software to detect servers and their responding ports, and then we scanned these servers for vulnerabilities.

The ITC's computer network has over 500 systems, consisting of servers, desktops, laptops, printers, phones, and network infrastructure devices. Every computer is connected to the network with a unique IP (Internet Protocol) address. For example, a desktop PC on the ITC network might have an address like 192.168.50.40. A typical Windows PC could have more than 20 listening ports. Each port serves a specific function: port 80 is used to request web pages from a webserver; and port 25 is used to transfer email. It would be normal for a network of 500 systems to present 10,000 responding ports, all potential targets for attack.

The Commission's effective perimeter defense exhibits the following traits:

- The Commission's intrusion detection system effectively prevents port scanning.
- It was not possible to gain unauthorized access to identified services within the scope of the audit.
- The majority of listening services we identified all seemed to be functions necessary for the ITC to conduct business.

In summary, the ITC network's perimeter defense effectively prevented our intrusion attempts.

An effective perimeter defense is a significant component of a complete network security program. An attacker can exploit a network in a number of ways. In general, she can attack the network perimeter as we did, or she can bypass the perimeter by tricking a user into letting her in. Means of accomplishing this could be as simple as having a user open a malicious email or visit an infected website, or by leaving an infected USB drive to be found by an employee near the front door of the building. While the ITC network's

current perimeter defense is effective, continuous attention and improvement are required to ensure that it remains effective in the future.

Our penetration testing did reveal two potential areas for improvement: the agency should implement ongoing scanning to detect vulnerabilities, and it should remediate current webserver vulnerabilities. These areas for improvement are detailed below.

Areas for Improvement

Area for Improvement 1:
The Commission should implement ongoing scanning to detect vulnerabilities.

Networks and their systems evolve over time, either deliberately or by chance. Secure systems installed today will become insecure over time due to newly discovered vulnerabilities in their underlying operating system or application software. Furthermore, any time changes are made to the existing environment, vulnerabilities can be inadvertently introduced. The best means of mediating this risk is through vulnerability scanning, on both a periodic basis and on-demand any time a change is made to the environment.

Even though it is licensed to use software that can perform vulnerability scanning of its perimeter, the ITC was not performing this function. The penetration test we performed as part of this audit found several potential vulnerabilities. Because previous tests were not performed, it was not known how long these systems had been vulnerable. The longer systems remain vulnerable, the more likely it is that they will be exploited. Regular testing would have identified these vulnerabilities and enabled timely remediation.

In order to execute the mission of the agency, senior management must remain informed of risks to their underlying systems. Regular perimeter scans are a critical source of information describing risks to an agency's information systems.

Recommendation 1: Perform scheduled, routine scanning of the perimeter on at least a monthly basis.

Recommendation 2: Perform perimeter scans after new hardware or software is introduced to the ITC perimeter network.

Area for Improvement 2:
The Commission should remediate current webserver vulnerabilities.

The penetration test we performed identified several potential vulnerabilities in the agency's webservers. We were unable to exploit them using the tools and methods within our scope of testing, but a determined attacker could use these vulnerabilities to exploit the ITC's systems.

We identified three types of potential vulnerabilities affecting four of the agency's internet-facing servers. One was specific to the type and configuration of vendor software, which was an obsolete and vulnerable version of Apache software. An upgrade to a newer version of Apache would resolve the first issue.

The remaining two types of vulnerabilities are specific to the custom software applications providing website services. These affect two systems, and are known as "Cross-Site Scripting" and "SQL Injection" vulnerabilities.

Cross-Site Scripting (XSS) vulnerabilities can be used to redirect users of a website to a different website without their knowledge or permission. A recent higher-profile example includes the exploit in November, 2012 of the Yahoo email service, which resulted in account breaches and the proliferation of spam.

The SQL Injection vulnerabilities found indicates that it may be possible for an external attacker to change the behavior of the application to directly access or possibly modify the internal ITC database supporting the application. This type of vulnerability is frequently used to modify a once-legitimate website to sell male enhancement drugs, embarrassing the owners of the website. Firms that store private data such as passwords or credit card numbers are at significant financial risk from these types of attacks.

The ITC has a responsibility to control access to its data, and to protect users of its public websites from malicious activity. It is possible to improve security by reconfiguring the existing webservers to remediate the issues found in the perimeter scan.

Recommendation 3: Upgrade vulnerable software to current, secure versions.

Recommendation 4: Upgrade encrypted websites to current standards.

Recommendation 5: Remediate known Cross-Site Scripting vulnerabilities.

Recommendation 6: Remediate known SQL Injection vulnerabilities.

Recommendation 7: Perform routine maintenance to identify and remediate vulnerabilities affecting public websites.

Objective, Scope and Methodology

Objective:

Is the ITC network's perimeter defense effective?

Scope:

This audit included all externally available wired nodes on the USITC network. The device list includes but was not limited to all servers, workstations, routers, email gateways and firewalls. The access types attempted included login attempts for the purposes of information gathering, privilege escalation, and establishment of jumping points to other areas of the USITC network infrastructure.

Methodology:

1. From an unfiltered IP address, performed unauthenticated network and device discovery using a toolset to include but not limited to Nessus, Wireshark, and other applications within the BackTrack tool suite.
2. Reviewed and analyzed protocol encryption types, as applicable.
3. Performed automated and manual login attacks using Hydra and/or other tools.
4. Attempted to gain shell access using BackTrack tools.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A: Management Comments on Draft Report

Chairman

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

CO81-LL-008

May 30, 2013

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Irving A. Williamson, Chairman

SUBJECT: Management Response to the Inspector General's "Audit of Perimeter Network Security"

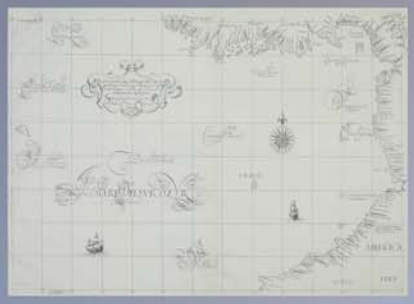
Thank you for your recent transmittal of the "Audit of Perimeter Network Security" draft report, dated May 6, 2013, and for the opportunity to review it.

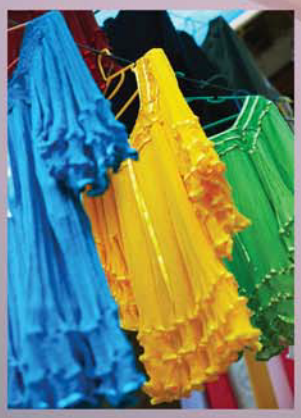
The audit's central determination was that the Commission's ITCNet online perimeter defense system was effective. While the report stated that the Commission's system demonstrated a capacity to prevent online intrusion, it also recommended that two specific functions be improved. The first relates to the Commission's vulnerability detection scanning procedures, which the report recommended be continuous. The second relates to the Commission's webserver vulnerabilities, which the report recommended be remediated.

We agree with the findings and are in the process of instituting management decisions that will address the recommendations put forth in this report. Thank you, once again, for your thoughtful review and we look forward to working together to address this situation in a timely manner.

"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to quickly perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission





U.S. International Trade Commission
Office of Inspector General
500 E Street, SW
Washington, DC 20436

Office: 202-205-6542
Fax: 202-205-1859
Hotline: 202-205-6542
OIGHotline@USITC.gov