U.S. International Trade Commission

Evaluation of NEA Perimeter Security

NEA OIG Report
No. R-13-03

February 15, 2013

Office of Inspector General

Table of Contents

Results of Evaluation

The purpose of this evaluation was to answer the question:

> Is the NEA network's perimeter defense effective?

Yes. The NEA network's perimeter defense is effective.

A penetration test is an attempt to breach a network and gain unauthorized access to its resources. On November 4, 2012, we conducted a penetration test of the NEA network using public information. Our search for public information on the NEA network servers identified one potential targets, and the office of CIO provided its network range of 64 IP addresses to limit the scope of the scan so it did not impact non-NEA equipment. We used software to detect servers and their listening service ports, and then we scanned these servers for vulnerabilities.

The NEA's computer network, the NEA network, has over 200 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 NEA 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 function; for instance, an Internet browser connects to port 80 to request web pages from a server, and email servers use port 25 to transfer messages. It would be normal for a network of 200 systems to present 4,000 listening ports, all potential targets for attack.

The goal of perimeter defense is to minimize the number of exposed ports, known as the "attack surface." A network with no open ports is not a network: open ports are required to communicate. Devices such as firewalls are configured to limit the number of ports exposed to the Internet, and newer technologies such as Intrusion Detection and Protection Systems (IDPS) can provide additional protection.

Several effective characteristics of the NEA network's perimeter defense include the following:

- The NEA network's firewalls effectively limit the exposure of internal systems to the Internet. Inside the NEA network, 5,000 or more service ports might be actively listening and responding to requests. From the Internet, only 7 systems and 8 ports were discovered in our scan of the NEA network.
- The listening services we identified all seemed to be functions necessary for the NEA to conduct business. We did not find any instances of services that should not have been exposed to the Internet.
- We were unable to exploit the systems found to gain unauthorized access to the NEA network.

In summary, the NEA 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 NEA 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 agency 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 NEA is not currently performing this function. The penetration test we performed as part of this evaluation 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 NEA perimeter network.

Area for Improvement 2:
The agency 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 NEA's systems.

We identified four types of vulnerabilities affecting four of the agency's internet-facing servers. Two are specific to the types and configuration of vendor software, which were an obsolete and vulnerable version of Apache software, and weak (easily broken) encryption methods. An upgrade to a newer version of Apache would resolve the first issue, and a relatively simple configuration change would resolve the second.

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 NEA 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 NEA 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.

Exit Conference

An exit conference was held with ITM officials on February 11, 2013. ITM officials concurred with our findings and recommendations.

Objective, Scope and Methodology

Objective:

Is the NEA network's perimeter defense effective?

Scope:

This Evaluation will include all externally available wired nodes on The NEA network. The device list shall include but is not limited to all servers, workstations, routers, email gateways and firewalls. The access types attempted will include login attempts for the purposes of information gathering, privilege escalation, and establishment of jumping points to other areas of The NEA network infrastructure.

Methodology:

1. From an unfiltered IP address, perform 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. Review and analyze protocol encryption types, as applicable.
3. Perform automated and manual login attacks using Hydra and/or other tools.
4. Analyze privilege capabilities if successful login is achieved.

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