Table of Contents

Results of Evaluation

The purpose of this evaluation was to answer the question:

> Is the ARC network's perimeter defense effective?

Yes. The ARC network’s perimeter defense is effective.

A penetration test is an attempt to breach a network and gain unauthorized access to its resources. On July 1, 2013, we conducted a penetration test of the ARC network using public information. Our search for public information on the ARC network servers identified one potential targets, and the office of CIO provided its network range of 16 IP addresses to limit the scope of the scan so it did not impact non-ARC equipment. We used software to detect servers and their listening service ports, and then we scanned these servers for vulnerabilities.

The ARC’s computer network, the ARC network, has over 100 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 ARC 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 100 systems to present 2,000 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 by detecting and blocking scans meant to identify open ports.

Several effective characteristics of the ARC network’s perimeter defense include the following:

- The ARC network’s firewalls effectively limit the exposure of internal systems to the Internet. Inside the ARC network, 5,000 or more service ports might be actively listening and responding to requests. From the Internet, only 8 systems and 17 ports were discovered in our scan of the ARC network.
- We were unable to exploit the systems found to gain unauthorized access to the ARC network.
- One system allowed registration for access. When we attempted to create a user account, the system denied this request because the details didn’t match some

requirement. The preregistration process deployed by ARC effectively helps prevent unauthorized access.

In summary, the ARC 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 ARC network's current perimeter defense is currently effective, continuous attention and improvement are required to ensure that it remains effective in the future.

Our penetration testing did reveal several potential areas for improvement: the agency should implement ongoing scanning to detect vulnerabilities, and it should remediate current potential risks 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 mitigating 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 ARC 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.

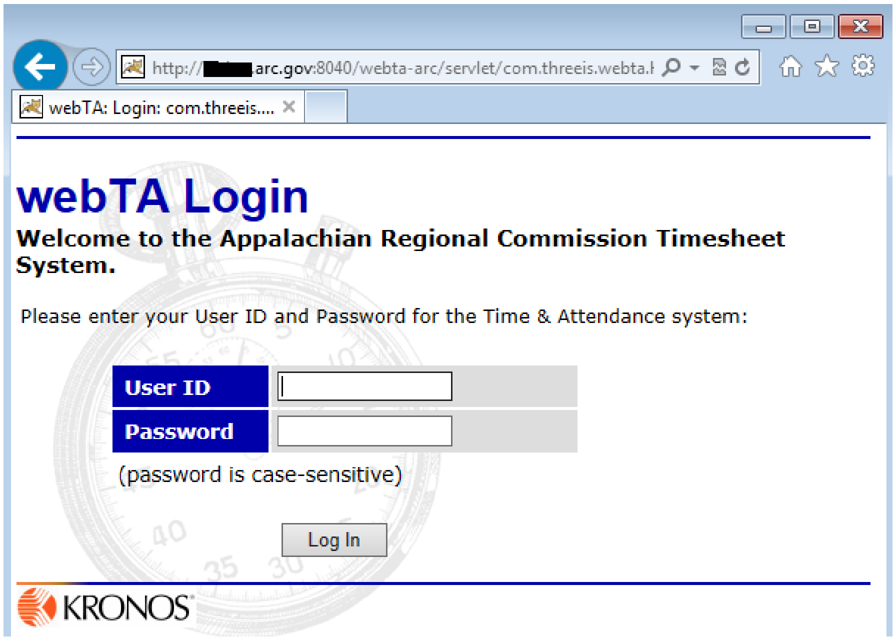
Recommendation 1: Perform scheduled, routine scanning of the perimeter on at least a monthly basis.

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

Area for Improvement 2:
The agency should remediate current potential risks.

The penetration test we performed identified several potential risks 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 ARC's systems or its users.

The Commission's web time and attendance system allows users to enter their username and passwords in clear text, instead of requiring encryption, as seen below:



http://[redacted]arc.gov:8040/webta-arc/servlet/com.threeis.webta.I
webTA: Login: com.threeis.... ×

webTA Login

Welcome to the Appalachian Regional Commission Timesheet System.

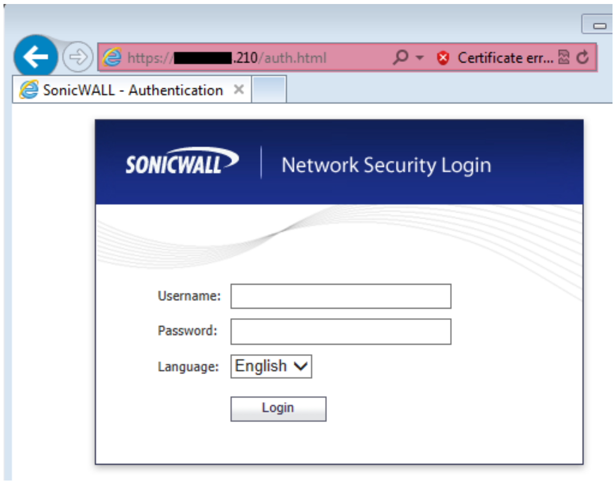
Please enter your User ID and Password for the Time & Attendance system:

User ID	
Password	

(password is case-sensitive)

This makes it possible for someone to intercept these credentials, and acquire usernames, passwords, and unauthorized access to the system. The Commission should encrypt the submission of passwords on its websites to eliminate this risk to its users and systems.

In our scan of the network perimeter, we identified several ports responding to the Internet that were not necessary for business communications. These ports were found on the Commission's on the previously mentioned web time and attendance system and its firewall product:



https://[redacted].210/auth.html

Certificate err...

SonicWALL - Authentication

SONICWALL | Network Security Login

Username:

Password:

Language: English

Responding ports provide potential entry-points to the network for authorized and unauthorized users alike. The Commission should limit responding ports to those necessary for business communications, and block access to those not needed for that purpose.

The ARC 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 devices to remediate the issues found in the perimeter scan.

Recommendation 3: Implement SSL to encrypt access to the web time and attendance webserver.

Recommendation 4: Block access to ports not necessary for business communications.

Management Comments and Our Analysis

On July 26th, 2013, management provided comments on the draft evaluation report. They concurred with our assessment that the perimeter network defense was effective, and that the defense could be further improved through ongoing vulnerability scanning and the remediation of current potential risks. They subsequently provided management decisions that would address each of the four recommendations.

At the time of the final report, the Commission was arranging for a vendor to conduct periodic scans of its Internet-facing network. It was also continuing to attempt to encrypt the Time and Attendance website.

Objective, Scope and Methodology

Objective:

Is the ARC network's perimeter defense effective?

Scope:

This evaluation included all externally available wired nodes on The ARC network. The device list included 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 ARC 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/Kali tool suite.
2. Reviewed and analyzed protocol encryption types, as applicable.
3. Performed automated and manual login attacks.