



August 20, 2002

OIG Report 02-28

MEMORANDUM FOR The Federal Co-Chairman
ARC Executive Director

SUBJECT: Audit Report--Appalachian Regional Commission
Computer Network and Systems' Security

PURPOSE

The purpose of this audit was to conduct a vulnerability assessment of the Appalachian Regional Commission's (ARC) network and computer systems to detect system vulnerabilities that may compromise ARC's network and systems, leaving them open to misuse and attack.

SCOPE

The Office of Information Technology Audits, Department of the Treasury Office of Inspector General, conducted this audit at my request. The detailed audit scope can be found in Appendix 1 of the report (attachment 1).

RESULTS

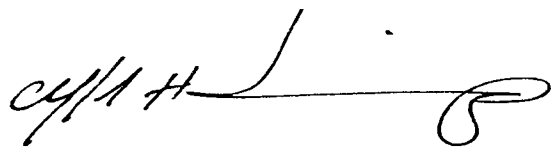
A high number of security vulnerabilities were detected that may expose ARC's network and systems to unauthorized access and exploitation. The inadequate or improper configurations of ARC's systems that lead to a high number of vulnerabilities could provide an attacker with unauthorized access, administration, and reconfiguration capabilities. The details of the vulnerabilities can be found in attachment 1. Some specific remedies to address individual vulnerabilities are documented in attachment 2, which will be kept in my office and made available to you or your staff at any time.

RECOMMENDATION

Immediate steps should be taken to prioritize and address the vulnerabilities detected to mitigate risks and threats to ARC assets, infrastructure, and information.

As this is an open recommendation, I am requesting a written description of actions taken and planned and target dates for any incomplete corrective actions, within 30 days of the date of this memorandum.

I would like to make note of the extremely cooperative assistance provided to the Treasury auditors by ARC staff as well as to thank the Treasury Office of Inspector General for its generous contribution of expertise and time to perform this audit.

A handwritten signature in black ink, appearing to read 'C/H Jennings', with a long horizontal flourish extending to the right.

Clifford H. Jennings
Inspector General

Attachments (2)

August 16, 2002

MEMORANDUM FOR CLIFFORD H. JENNINGS, INSPECTOR GENERAL
Appalachian Regional Commission

FROM: Edward G. Coleman
Director, Information Technology Audits

SUBJECT: Audit Report - Security Vulnerabilities Pose
Risks to the Appalachian Regional Commission's
Network and Systems

The attached report presents the results of our audit of security controls over the Appalachian Regional Commission's (ARC) network and systems. We used Internet Security Systems' (ISS) Internet Scanner and System Scanner programs to detect the vulnerabilities that exist in ARC's network and computer systems. The vulnerability assessment results from the ISS scans are summarized in this report.

During our review, we identified that a high number of vulnerabilities could expose ARC's network and systems to compromises and exploitation. In addition, we have highlighted a number of security vulnerabilities that are on the System Administration, Networking and Security Institute/Federal Bureau of Investigation list of the Twenty Most Critical Internet Security Vulnerabilities. We will send the detailed ISS reports under separate cover in order to provide ARC with the technical information needed to address the identified vulnerabilities.

We appreciate the courtesies and cooperation provided to our staff during the audit. If you wish to discuss this report, you may contact me at (202) 927-5007, or Barbara Bartuska, Audit Manager, at (202) 927-5083.

Attachment

**INFORMATION TECHNOLOGY:
Security Vulnerabilities Pose Risks to the
Appalachian Regional Commission's
Network and Systems**

OIG-02-110

August 16, 2002



Office of Inspector General

The Department of the Treasury

Contents

| | |
|---|---|
| Audit Report | 3 |
| Executive Summary | 4 |
| Background | 6 |
| Results and Recommendation | 8 |
| Security Vulnerabilities Could Compromise Network and Systems | 8 |

Appendices

| | |
|---|----|
| Appendix 1: Objective, Scope, and Methodology | 13 |
| Appendix 2: Major Contributors to This Report | 14 |
| Appendix 3: Internet Scanner Report | 15 |
| Appendix 4: System Scanner Report | 16 |

Contents

Abbreviations

| | |
|----------|--|
| ARC | Appalachian Regional Commission |
| FBI | Federal Bureau of Investigation |
| ISS | Internet Security Systems |
| NT | New Technology |
| OIG | Office of Inspector General |
| OWA | Outlook Web Access |
| SANS | System Administration, Networking and Security Institute |
| Treasury | Department of the Treasury |

*The Department of the Treasury
Office of Inspector General*

Clifford H. Jennings, Inspector General
Appalachian Regional Commission

Treasury OIG recently completed the vulnerability assessment of the Appalachian Regional Commission's (ARC) network and computer systems. The overall objective of this review was to detect security vulnerabilities that may compromise ARC's network and systems, leaving them open to misuse and attacks.

To complete our objective, we used two commercial off-the-shelf products to check for, but were not limited to, vulnerabilities such as bugs in the operating systems, missing operating system patches, compromised system services, insecure default configurations, inadequate password requirements, unauthorized changes to system configurations, improper sharing of directories, failure to run virus scanning software, and the use of modems to dial-in past firewalls. A detailed description of our objective, scope, and methodology is provided in Appendix 1.

Our report highlights the security vulnerabilities detected and the impact of potential compromises or exploitation. The security vulnerabilities are ranked by risk levels: high, medium, and low. A high-risk vulnerability allows an attacker immediate access to a system, to gain superuser or administrator access, or to bypass a firewall. A medium-risk vulnerability provides system information, degrades performance, or has a high potential of giving system access to an intruder. A low-risk vulnerability provides system information that could potentially lead to a compromise, for example, exposing a list of usernames.

Executive Summary

We identified that a high number of security vulnerabilities detected by Internet Security Systems' (ISS) tool scans may expose ARC's network and systems to unauthorized access and exploitation. The inadequate or improper configurations of ARC's systems, that lead to a high number of vulnerabilities, could provide an attacker with unauthorized access, administration, and reconfiguration capabilities. In addition, a number of vulnerabilities in ARC's systems are also listed on the System, Administration and Network Security Institute/Federal Bureau of Investigation (SANS/FBI) list of Twenty Most Critical Internet Security Vulnerabilities. The majority of successful attacks on computer systems via the Internet can be traced to exploitation of these vulnerabilities.

Our report provides highlights of vulnerabilities at each risk level. Examples of high-risk vulnerabilities include the following:

- User accounts have no passwords or weak passwords.
- Systems and applications do not have the latest patches.
- System audit configurations are ineffective.
- File and registry access controls are inadequate.
- System administrative privileges are inappropriately assigned.

We also identified certain medium and low-risk vulnerabilities that are on the SANS/FBI list of critical security vulnerabilities. These vulnerabilities also pose numerous opportunities for hackers to obtain information and exploit the network and systems.

Internet Scanner was used to scan 11 Windows NT/2000 servers, 60 Windows NT/2000 desktop computers, 3 Unix servers, and the firewall. Though Internet Scanner detected no vulnerabilities in the firewall, the scan summary shows a significant number of vulnerabilities in servers and desktops, as listed below:

Table 1: Internet Scanner Results

| TYPE OF DEVICES | HIGH | MEDIUM | LOW | TOTAL |
|------------------|------------|------------|------------|-------------|
| NT/2000 Servers | 84 | 276 | 737 | 1097 |
| NT/2000 Desktops | 83 | 39 | 2 | 124 |
| Unix Servers | 11 | 0 | 5 | 16 |
| TOTAL | 178 | 315 | 744 | 1237 |

System Scanner was used to scan 6 of ARC's Windows NT/2000 servers. The number of vulnerabilities detected is documented below:

Table 2: System Scanner Results

| | SERVER NAME | HIGH | MEDIUM | LOW | TOTAL |
|---|--------------|------------|---------------|-------------|---------------|
| 1 | ARC-WEB | 22 | 580 | 307 | 909 |
| 2 | ARC-LS | 74 | 27103 | 246 | 27423 |
| 3 | ARC-VW | 17 | 69 | 228 | 314 |
| 4 | ARC-FS | 141 | 159241 | 1250 | 160632 |
| 5 | ARC-APPS | 143 | 40601 | 1152 | 41896 |
| 6 | ARC-BKUP | 56 | 5811 | 243 | 6110 |
| | TOTAL | 453 | 233405 | 3426 | 237284 |

The Internet Scanner and System Scanner Reports are provided in Appendices 3 and 4.

Proper configurations are essential for network and system management. The ARC's network and systems are integral parts of its mission support structure. Information maintained by the network and systems play a vital role in ARC's economic, human, development, and highway programs for the Appalachian Region. Because ARC's network and systems are highly interconnected with each other and the Internet, it is extremely important that network connections are secured and only authorized users are granted access.

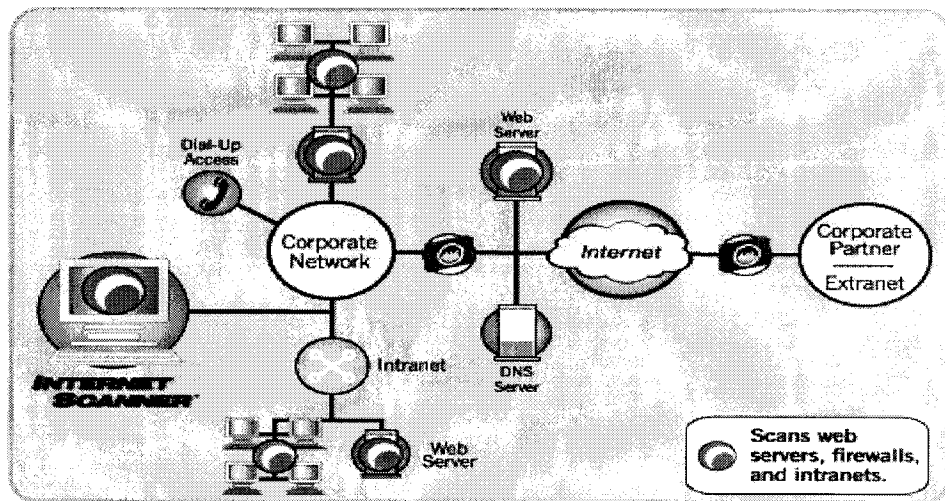
Due to the high number of vulnerabilities detected, we recommend that ARC analyze, prioritize, and address these vulnerabilities, especially high-risk vulnerabilities, to strengthen its security posture. By strengthening its information security posture, ARC will be in a better position to deter hacker attacks and protect its network and systems from other types of compromises. The detailed ISS reports with proposed remedies will be provided under separate cover.

Background

In an effort to upgrade and enhance information security, ARC's Inspector General requested assistance in performing an automated scan and vulnerability assessment of ARC's network and computer systems. In response to this request, we conducted the audit, using the ISS Internet Scanner and System Scanner tools to identify vulnerabilities in ARC's network and systems.

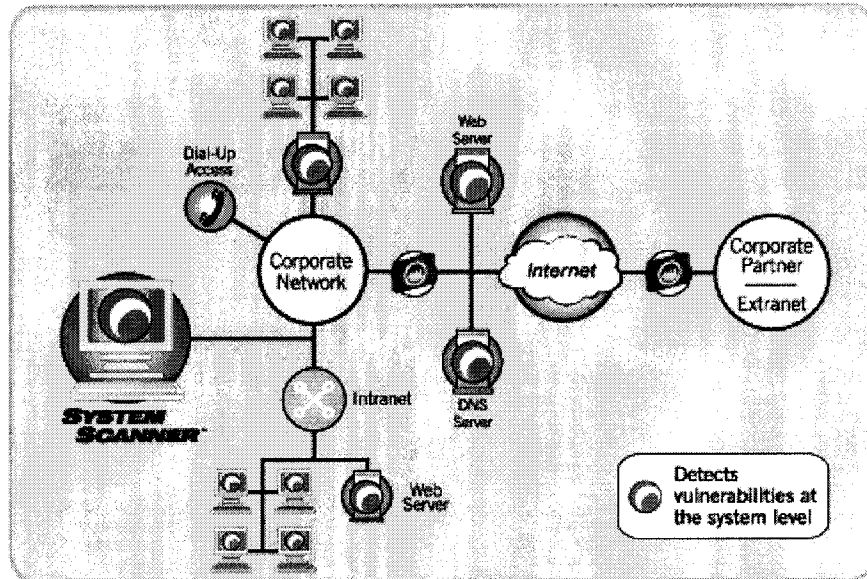
Internet Scanner provides an automated, network-based security assessment for systems and telecommunication devices on an enterprise-wide network. Specifically, Internet Scanner checks for vulnerabilities on routers, Web servers, Unix servers, Windows NT servers, desktop systems, and firewalls. The configuration of Internet Scanner on a network is illustrated below:

Figure 1: Internet Scanner Configuration



System Scanner provides a host-based vulnerability assessment of an individual system by identifying vulnerabilities inherent in software and hardware, configuration elements that make a system vulnerable to attacks. It also detects vulnerabilities in domain administration, audit configuration, frozen files, home files, logon failure auditing, mount points, registry access, security files, system files, and others. The configuration of System Scanner on a network is illustrated below:

Figure 2: System Scanner Configuration



Results and Recommendation

Results **Security Vulnerabilities Could Compromise Network And Computers**

The ARC's network and systems are integral parts of its mission support structure. The ineffective configuration and inefficient management of ARC's systems can result in a growing number of vulnerabilities, thus weakening its network security posture. The results of the ISS scans show a high number of security vulnerabilities in ARC's network and systems. These security vulnerabilities may lead to unauthorized accesses, computer viruses, the deletion and modification of data, Denial of Service attacks, and system exploitation. Furthermore, access through unsecured, interconnected systems leaves ARC's network and systems vulnerable to attacks that can corrupt data.

High-Risk Vulnerabilities

The ISS scans detected a significant number of high-risk vulnerabilities in ARC's network and systems. These vulnerabilities allow immediate access as privileged users, such as root or administrator, using widely known hacker programs that could directly compromise a system. High-risk vulnerabilities detected in ARC's systems also appear on the SANS/FBI list of Twenty Most Critical Internet Security Vulnerabilities. These areas of risks relate to password settings, system and application patches, audit configuration, user access, and administrative rights.

User Accounts Have No Password or Weak Passwords

The ISS scans discovered that a number of user and administrator accounts were assigned a null password. In addition, the scans detected user and Administrator accounts with the passwords set to user ids. Because some vendors ship Windows NT pre-installed with a null password for the Administrator and other user accounts, these accounts can easily be accessed if a password is not assigned. Furthermore, if the account is "Administrator," an attacker could gain unlimited access and take control of the host or domain.

Systems and Applications Do Not Have the Latest Patches

The ISS scans identified that a number of systems do not have appropriate patches installed, which could “open” a system to a remote attacker. For example, without the required patch, Microsoft Exchange 5.5 Outlook Web Access (OWA) service could allow malicious scripts to be executed in a user’s mailbox when Internet Explorer is used to access email using OWA. A similar vulnerability was found in computers with Internet Explorer versions 5.5 and 6.0 installed. Without this patch for Internet Explorer, a system could allow an attacker to add, delete or modify files; communicate with other remote systems; or reformat the hard drive. ISS scans also discovered that some Windows 2000 servers do not have a patch to prevent errors in the catalog file. These errors could cause the removal of a valid hotfix, causing the system to revert to the previous software version that contains problems or deficiencies.

System Audit Configurations Are Ineffective

System Scanner detected that auditing capabilities are disabled on a number of ARC’s servers and in other instances the logs are being overwritten. If auditing capabilities are disabled, audit trails cannot be generated; therefore, it is impossible to log either authorized or unauthorized activities on the system. Additionally, when log events are overwritten, vital audit information is lost.

File and Registry Access Controls Are Inadequate

The ISS scans found that the “Anonymous” user account, which does not require a password, has access to system and application log files. If the “Anonymous” user account has the privileges to remotely view the “System” or “Application” log, a hacker can log on using this account to gain access to sensitive information.

The ISS scans also detected a vulnerability related to registry access in ARC’s servers. For example, the “Everyone” group has permissions other than “Read” to some specific registry keys. These permissions allow users to change registry values and redefine system startup or shutdown.

System Administrative Privileges Are Inappropriately Assigned

The ISS reports listed a number of users and groups assigned with inappropriate system privileges such as “act as part of the operating system,” “replace a process level token,” or “restore files and directories.” These rights are not normally granted to an end user. They can be used to run parts of the operating system that are secured and trusted, modify the security of the access token, or replace any file or registry key.

Medium-Risk Vulnerabilities

The medium-risk vulnerabilities identified provide information that has a high potential of giving system access to an intruder. The System Scanner detected a noticeably high number of medium-risk vulnerabilities in ARC’s Windows NT/2000 servers. Below are examples of medium-risk vulnerabilities reported from the scans, which are also included in SANS/FBI list of Twenty Most Critical Internet Security Vulnerabilities:

- A password history file is not retained, permitting the frequent reuse of a password.
- Shared objects are inadequately protected, allowing users other than administrators to redefine system-wide resource attributes.
- The Remote Procedure Call server service is enabled, potentially allowing message spoofing and the breaking of encryption.
- The Windows NT 4.0 Network Basic Input/Output System enables open Internet Protocol ports, which allows an intruder to install an unprivileged program and listen on these ports to gain information.

Low-Risk Vulnerabilities

Low-risk vulnerabilities are weaknesses resulting from ineffective configurations, which provide system information that could potentially lead to compromises. Many low-risk vulnerabilities were found in ARC’s systems; examples are listed below:

- Anti-virus software is not installed.
- A minimum password age is not required.
- A password cannot be changed.
- A user password never expires.

-
- Dormant accounts (i.e., accounts that users have not logged into for 30 days) are not disabled or removed.
 - A default “Administrator” account exists.

Recommendation

The ARC’s management should take corrective actions to prioritize and address the vulnerabilities detected to mitigate risks and threats to ARC’s assets, infrastructure, and information. The specific remedies to address individual vulnerabilities will be provided under separate cover.

* * * * *

Treasury OIG would like to extend its appreciation to ARC for the cooperation and courtesies extended to its staff during the review.

If you have any questions, please contact me at (202) 927-5007, or Barbara Bartuska, Audit Manager, Office of Information Technology Audits, at (202) 927-5083. Major contributors to this report are listed in Appendix 3.

Edward G. Coleman
Director, Office of Information Technology Audits

The overall objective of this audit was to identify security vulnerabilities that may compromise ARC's network and systems, leaving them open to misuse and attacks. In conducting our review, we used two commercial off-the-shelf products from ISS, Internet Scanner and System Scanner, to scan systems and telecommunications devices on ARC's network.

The Internet Scanner performed scheduled or interactive scans of network communication services, operating systems, routers, email, web servers, firewalls, and applications to identify weaknesses that could be exploited by intruders who gain access to the network. The scan configurations were customized in accordance with ARC's information security policies. Different levels of scans were selected based on ARC's system architecture and characteristics.

The System Scanner performed scheduled or interactive scans of selected systems to identify vulnerabilities inherent in software and hardware, configuration elements that make a system vulnerable to attacks. The default settings were selected to scan ARC's systems.

Fieldwork was performed at ARC in Washington, DC between June 2002 and July 2002. This audit focused on detecting the vulnerabilities in ARC's network and computer systems. We did not prioritize or rank the security vulnerabilities detected by ISS products, nor did we evaluate the remedies that should be taken to address the vulnerabilities identified. Additionally, we did not evaluate the logical controls or system policies in place at ARC. Our review did not cover any other security issues related to ARC's assets, infrastructure, information, or mission.

We conducted our audit in accordance with generally accepted government auditing standards.

Office of Information Technology Audits

Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Patrick Nadon, Audit Manager
Tram J. Do, Computer Specialist

Internet Scanner Report

System Scanner Report