



network defense through collaboration

Vulnerability Assessment Report

ACME CORPORATION

July 5, 2003

CONFIDENTIAL DOCUMENT

1. EXECUTIVE SUMMARY

1.1. Security Rating

7.4

1.2. Network Range

172.16.174.49-54

172.16.172.8

172.16.172.10

172.16.172.17

1.3. Network Changes:

2.1.1. Devices added

172.16.174.50

- o TCP 53 DNS OPEN
- o UDP 53 DNS OPEN

172.16.174.51

- o TCP 25 SMTP OPEN
- o TCP 53 DNS OPEN
- o UDP 53 DNS OPEN
- o TCP 80 HTTP OPEN

2.1.2. Devices removed

172.16.172.8

2.1.3. Devices changed

172.16.174.52

- o TCP 22 SSH OPEN
- o TCP 80 HTTP CLOSED



2. OUTSTANDING SECURITY ISSUES

2.1. DNS Server Spoofable.

172.16.174.50
172.16.174.51

2.2. DNS server allows unauthenticated zone transfers.

172.16.174.50

2.3. SMTP server allows mail relaying.

172.16.174.51

2.4. FrontPage Extensions Present.

172.16.174.51

2.5. Telnet is Externally Accessible.

172.16.172.10
172.16.172.17

2.6. WebDAV/PROPFIND Method Found on Server.

172.16.174.51

2.7. Server Allows Unlimited SSH Login Attempts.

172.16.174.52

2.8. Host Responds to ICMP Timestamp Request.

172.16.172.10
172.16.172.17
172.16.174.50
172.16.174.51
172.16.174.52
172.16.174.56

3. REPORT EXPLANATION

This report is the result of the weekly external assessment of your network, systems, and software. This assessment is not as comprehensive as a full external evaluation but is intended to keep you apprised of the current security level of your network and systems configuration. The results of the weekly assessment are compared against those of the previous week. This is done to provide you with a gauge on how your network changes from week to week and, most importantly, what the security ramifications of those changes are. You may find that your security rating changes from week to week without changes to your systems. This is the result of the ever-changing state of vulnerabilities and exploitation of the systems and software utilized in your network.

This report is designed to be concise so that you may quickly assess the matters of importance to your particular organization. The intent is not to list every possible security issue, but rather, those that might lead to a compromise of security at your organization. If you have any questions regarding the contents of this report please contact the Asperios Security Engineer assigned to your organization. The Security Engineer and contact information were supplied to your firm upon the commencement of services by Asperios. Alternatively, you may also contact the Asperios Security Operations Center 24/7/365 by email at security@aperios.net.

The weekly report contains the following three sections:

3.1. Security Rating

In order to quantify the level of security achieved by your particular organization, we use a rating scale ranging between 0 and 10. The purpose of the rating system is to weigh the relative significance of various vulnerabilities in order to achieve an overall valuation of the effectiveness of security measures. Different settings and vulnerabilities carry positive and negative score impacts weighted on their significance specific to the environment at your organization. The specific ratings equate to the following overall descriptions of security effectiveness:

- 0.0 – 2.0.....Trivial Security**
- 2.1 – 4.0.....Low Security**
- 4.1 – 6.0.....Moderate Security**
- 6.1 – 8.0.....Good Security**
- 8.1 – 10.0.....Strong Security**

3.2. Changes Detected

This section lists the changes that were detected in your network and systems from the previous week's report.

- Devices Added** – Systems not present the previous week sorted by IP address.
- Devices Removed** – Systems that were present previously which are no longer detected.
- Devices Changed** – All other system changes appear here. Examples include new ports open, ports closed, new vulnerabilities detected, and software version changes detected.

3.3. Outstanding Security Issues

This section lists both new and outstanding security issues detected. Outstanding security issues are ones that were detected in earlier scans and have not yet been mitigated. For purposes of brevity, only the issues are listed in the report. Explanations of vulnerabilities, their severity, and their possible remediations can be found in the Asperios Ongoing Security Issues Manual. Should you need another copy of the manual, please contact Asperios as mentioned above