

---

# MISI Municipal Information Systems, Inc.

---

2665 Scott Ave., Suite C  
St. Louis, Missouri 63103 ♦ (314) 533-2320

## **Special Report:**

### Penetration Testing

Performed February 6, 2004

By: TechGuard Security, Chesterfield, MO

Purpose: This report contains a detailed security analysis and penetration test of the Municipal Information Systems, Inc. (MISI) Citrix environment.

Systems examined in report:

[server names removed by MASW to preserve MISI security]

Network Scan Results:

“A full TCP port scan was performed for each of the IP addresses listed. Each IP address listed was found to have port 1494/tcp open. This port is traditionally used for the Citrix Metaframe service.”

Server Analysis:

“A logon was attempted utilizing the Administrator built-in Windows account, the Guest built-in Windows account, and several other common accounts. Account logon with these user names and some of the most common weak passwords was not possible.”

Executive Summary of Findings:

“All four systems examined in the report appear to be behind a firewall running some version of the Sun Solaris operating system. Citrix encryption is in use, however, the encryption level could not be determined. It was determined that the “Guest” account is disabled and the Administrator account password is set to something that is not easily guessable. UDP port 1604 is not enabled at the firewall, which prevents several different attacks against Citrix, including brute-force published applications.”