

# State of North Carolina



Office of the State Auditor:

INFORMATION SECURITY VULNERABILITY ASSESSMENT

The State Auditor of North Carolina supervised a penetration test on 22 of the state's network security systems - in 21 cases the test team were able to take control of the target computers using programs that are readily available to hackers and the public.

This article describes the approach to testing taken by the Office of the State Auditor. The full audit report can be downloaded from the State Auditor's web site at...

<http://www.osa.state.nc.us>

## Overview

In a series of projects to evaluate the network and computer security in place within selected areas of state government, contractors employed by the Office of the State Auditor (OSA) attempted to penetrate the network security systems at 22 of the State's computer systems. The outcome was



"Capitol Building, Raleigh"

that security engineers gained control of computers in 21 of the target systems using programs that are readily available to hackers and the public.

To further assist agencies achieve a "best practice" level of information security over their internal systems, data and assets, we performed a comprehensive information security assessment at the Dept of Revenue, Dept of Treasurer, Office of the State Controller, and Dept of Health and Human Services. While our assessments identified well-defined and effective security controls, we also identified several areas that posed extreme security risks and exposed the agency concerned to possible internal or external attack. We classified control weaknesses as *High*, *Medium*, or *Low* in relation to the level of risk, and on this basis concluded that the overall risk that the agency or state network could be compromised was *High*.

## Phase I - preliminary state-wide assessment

Our assessment determined that the State's systems were at high risk for Internet-based attacks. We subjected the twenty two agencies that hosted the critical information systems for the Executive, Legislative, and Judicial branches of state government to an External Network Penetration Test. This was broken down into four separate phases:

**Phase 1 - intelligence gathering:** using common communications protocols and applications, our security engineers determined what information was available to the general public regarding the State's network. This information was then reviewed to determine whether it offered potential intruders an adequate view of the network infrastructure from which they could develop a network blueprint.

## North Carolina Office of the State Auditor

The State Auditor is a member of the Council of State and is elected by the voters of North Carolina every four years. Under the State's Constitution and General Statutes the State Auditor is responsible for conducting and coordinating audits of state agencies and programs supported by state funds. The audits conducted by the Office of the State Auditor include financial and compliance audits on state agencies including community colleges, the Clerks of Superior Court, and the Smart Start partnerships; performance audits to evaluate the effectiveness and efficiency of state agencies and programs; information systems audits on the state's data processing systems; and special reviews to investigate allegations of fraud, waste, or abuse in the state supported agencies or programs.

**Phase 2 - active reconnaissance:** our security engineers used a combination of "hacker" utilities along with the contractor's internally developed audit tools to identify specific hosts and services that were accessible from the Internet. This resulted in a partial list of accessible hosts and a list of possible services offered.

**Phase 3 - attack and toehold:** the object of this phase was to gain user level access to (at least) one host in each agency. Using a combination of "hacker" utilities and internally developed auditing tools our security engineers tested the vulnerability of popular services offered on various hosts to undetected, unauthorized access to the State's network. In cases where automated scanners did not determine the nature of a specific service, the engineers connected directly to the service to verify the security issues.

**Phase 4 - privilege escalation:** our security engineers manually demonstrated their ability to increase their privileges on host sites managed by each Agency in the presence of the Agency Head (or Chief Deputy) and the Information Systems Director. This technique provided a real-time perspective for agency representatives regarding the amount of time required to penetrate their networks and gain

control of proprietary agency information. It also provided an additional buffer for service restoration; should a target machine break down during an attack the responsible individuals could be notified immediately.

Our security engineers succeeded in penetrating 21 of the 22 agencies identified as part of this test. In almost every case they gained full control of an agency computer or device in 30 minutes or less, and in some cases were able to monitor work being carried out while having complete control over the computer. After gaining control they were able to monitor network traffic, capture other user ids and passwords, and launch other attacks that went undetected. However, in one case, due to the vulnerability identified

and exploited being on a device owned by a different agency, our security engineers were unable to complete the attack in the 1 hour and 30 minutes allowed them.

## Conclusion

At the time of our testing the security posture of the State's network offered little protection from hacker attacks via the Internet and was therefore at high risk of compromise. Our testing enabled us to provide each agency and Information Technology Services with detailed reports describing the weaknesses we had identified and our recommendations for corrective action. These security enhancements have been acted on.

This comprehensive information security assessment focused on five key areas:

- **Security Policy Assessment**, which evaluates the implementation of security policies and procedures.
- **Network Architecture Assessment**, which is a detailed review of a network design.
- **Network Vulnerability Assessment**, which provides a thorough understanding of security-related weaknesses and exposures in networks.
- **Host Vulnerability Assessment**, which reviews the current security configuration of mainframes and operating systems.
- **Secure Build Review (one agency only)**, which is a security analysis in a non-production environment for the build procedure for a desktop client computer.

Agency	Security Policy Assessment	Network Architecture Assessment	Network Vulnerability Assessment	Host Vulnerability Assessment	Secure Build Review
Dept of Revenue	X	X	X	X	X
Dept of the State Treasurer	X	X	X	X	
Office of the State Controller	X	X	X	X	
Dept of Health and Human Services			X	X	

Risk Levels	Dept of Revenue	Dept of State Treasurer	Office of the State Controller	Dept of Health and Human Services
High	7	5	4	23
Medium	7	6	2	6
Low	5	2	1	3
Overall	Moderate	High	Moderate	High

## Phase II - comprehensive vulnerability assessment

Following Phase I, four agencies volunteered to be subjected to a more comprehensive assessment of their production networks. Phase II addressed five key areas: Security Policy Assessment, Network Architecture Assessment, Network Vulnerability Assessment, Host Vulnerability Assessment, and Secure Build Review (Dept of Revenue only).

The table shows the tests we carried out at each agency. These can be summarised as follows (further details are set out in the Annex):

**Security Policy Assessment:** our objectives here were to:

- **evaluate current security policies and practices:** this involved

reviewing security policy and associated procedures for completeness, accuracy, and appropriateness. We also reviewed current incident response policies and procedures;

- **provide recommendations** based on best practices and knowledge of the client's business objectives and organisational infrastructure.

**Network Architecture Assessment:** in this stage we focused on the internal network infrastructure, Wide Area Network (WAN) connections to remote locations, and Internet connectivity through the North Carolina Integrated Information Network. We examined the business and technical requirements of the current network infrastructure to ensure a proper balance between functionality, cost, and security.

**Network Vulnerability Assessment:** having gained an understanding of the network architecture, we assessed network vulnerabilities. We examined the configuration of network devices, firewalls, and public web servers to provide a current view of vulnerabilities and threats. Our assessment consisted of a review of devices owned and maintained by each agency and devices owned and maintained by Information Technology Services.

**Host Vulnerability Assessment:** the aim in this stage was to provide a current view of threats and vulnerabilities. Our assessment covered the agency's client services and supporting infrastructure, and consisted of a review of a number of hosts owned and maintained by the agency.

**Secure Build Review (Dept of Revenue Only):** During the Secure Build Review we examined the build process created by the Information Technology group (within the Department of Revenue) for building desktop client computers.

## Findings

Our testing uncovered a number of weaknesses at each of the agencies, some being sufficient to permit unauthorised access, data manipulation, or data destruction. We classified each weakness according to its relative risk using the following definitions:

**High-level Risk:** defined as a vulnerability that could cause grave consequences if not addressed and remedied immediately. This type of vulnerability is evident within the most sensitive portions of the network, as identified by the data owner. This vulnerability could cause network functionality to cease or control of the network to be gained by an intruder;

**Medium-level Risk:** defined as a vulnerability that should be addressed within the near future. There is urgency in correcting this type of vulnerability; however; this may be either a more difficult exploit to perform or of lesser concern to the data owner;

**Low-level Risk:** defined as a vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network to be exploited and/or it is of little consequence to the data owner.

We provided each agency with a detailed report that set out the specific vulnerabilities we had identified together with our recommendations for corrective action. In each of the four agency assessments we also identified vulnerabilities affecting devices controlled by Information Technology Services, and we disclosed these to ITS for corrective action.

The vulnerability assessment performed at the Department of Health and Human Services covered nine of the Department's divisions. Although the results have been consolidated for this article, we evaluated and reported on each division separately.

## Next Steps

The four agencies that volunteered to participate in this vulnerability assessment should be commended for their concern for information systems security. The results of these tests will assist both them and ITS to strengthen network security. However, every state government agency should be subject to a thorough vulnerability assessment, with regular follow-ups.

Our participation in these assessments helped the Office of the State Auditor's Information Systems Audit Division to develop the skills and testing expertise to perform these tests in the future. To be successful in these efforts, OSA must acquire the testing software necessary to analyse networks for vulnerabilities, establish testing facilities, and continue to receive specialised training in the latest advances in networks and the related vulnerabilities.

**North Carolina Office  
of the State Auditor**

## Annex

Further details of our test objectives during "**Phase II - Comprehensive Vulnerability Assessment**" are as follows:

### Network Architecture Assessment

This assessment was divided into the following key areas:

- Network Overview;
- Segmentation Model;
- IP Routing;
- Redundancy;
- Encryption;
- Remote Access;
- Network Management;
- Anti-Virus;
- Intrusion Detection Systems;
- Backups;
- Firewalls.

Our key objectives were to:

- interview business and technical representatives to gain a solid understanding of business objectives and requirements;
- review technical requirements for the network;
- review required data flows;
- assess security zones and access controls;
- review at a high level the host and network management strategy;
- review at a high level the enterprise backup strategy;
- review at a high level the enterprise virus strategy;
- identify applicable industry best practices;
- identify and validate security issues of immediate consequence;
- develop long-term recommendations to enhance security;
- transfer knowledge.

### Network vulnerability assessment

Our key objectives in this stage were to:

- develop a picture of the network, including topology, devices and hosts, and services for correlation against provided information and documentation;
- assess network device configuration for vulnerabilities or insecure configurations;
- use active probing to assess network security features such as firewall configuration, intrusion detection systems (IDS), and virtual private networks for vulnerabilities or insecure configuration;

- analyse the perimeter firewall's rule set;
- assess the configuration and architecture of directory services;
- assess the mainframe environment's security configuration;
- identify and validate vulnerabilities in network components, and overall architecture;
- identify quick fixes for vulnerabilities;
- develop long-term recommendations to enhance security.

### Host vulnerability assessment

The key objectives of this assessment were to:

- assess server configuration (domain controllers, web servers, application servers, database servers) for vulnerabilities or insecure configurations;
- identify and validate vulnerabilities in network and server components, and overall architecture;
- identify quick fixes for vulnerabilities;
- develop long-term recommendations to enhance security.

### Secure Build Review (Department of Revenue Only)

The key objectives of this review were to:

- interview technical and business representatives to gain a solid understanding of the demands placed upon the system and how they impact the host;
- review the intended use of the platform to understand requirements and tailor recommendations;
- establish secure build methodology for evaluating the build;
- examine existing hosts in the production environment for the application of patches and upgrades;
- assess operating system configuration, including: insecure services, permissions, and registry settings as well as unnecessary services and packages;
- identify and validate security issues of immediate consequence;
- develop recommendations to enhance security.