ManTech
International Corporation

Leading the Convergence of National Security and Technology℠

2013 North Dakota Information Technology Security Audit
Vulnerability Assessment and Penetration Testing Summary Report

14 March 2014

Submitted to:

Donald Lafleur
IS Audit Manager
ND State Auditor’s Office
Phone: 701.328.4744
E-mail: dlafleur@nd.gov

ManTech Point of Contact:

ManTech Mission, Cyber and Intelligence Solutions
Mark E. Shaw
Senior Executive Director, Cyber Security Solutions
1951 Kidwell Dr, Suite 500
Vienna, VA 22182
Phone: 703.388.2126
E-mail: mark.shaw@mantech.com

DOCUMENT REVISION HISTORY

Version	Date	Change Description
1.0	19 February 2014	Initial Draft
1.1	24 February 2014	Updated Draft
2.0	14 March 2014	Final Report

TABLE OF CONTENTS

1. INTRODUCTION

No organization is immune to network intrusions. In this age of increased communication, the rate of electronic activity has grown exponentially as consumers and organizations find more opportunities to engage in transactions that involve the use of both the Internet and computer networks. As a result, organizations have become targets of individuals and groups seeking to gain “unauthorized access” for which they are unprepared and vulnerable. Not only are organizational network security breaches increasing in number and scope, they are causing more damage than ever before. Millions of dollars are lost each year and proprietary data and personally identifiable information is stolen as a result of network intrusions.

Network Vulnerability Assessments give organizations an opportunity to thoroughly and realistically evaluate the security posture of their IT infrastructure. Vulnerability testing also allows the organization to assign relative risks to each vulnerability that is discovered. This allows for a quantitative risk analysis of vulnerabilities, and provides a basis for prioritization of fixes and countermeasures. Combining the technical vulnerability information with the organization’s overall threat environment and risk tolerance, results in a clear risk picture that can be used to create a comprehensive mitigation plan.

Penetration Testing is intended to provide an organization a snapshot of the overall security and risk picture of its network. Penetration testing focuses on gaining access to systems under an organization’s control. Often a single system can provide a foothold into an organization’s network and allow further access to external and/or internal systems.

During the months of November and December 2013, ManTech performed an external/internal vulnerability assessment of the State of North Dakota’s statewide computer network, an application security assessment of two State web applications, and reviewed the network and physical security of six State agencies. In December 2013 and January 2014, ManTech performed multiple penetration testing scenarios against the State's internal network.

2. ASSESSMENT SCOPE

The assessment of the North Dakota state network included an external vulnerability assessment, an internal vulnerability assessment, and a penetration test.

2.1 External Vulnerability Assessment

ManTech evaluated the state network by performing an analysis of publicly available information about the state network, using tools to scan the network, assessing the behavior of security devices and screening routers and firewalls, and analyzing potential target hosts identified by reviewing software, bugs, patches, and configuration. Vulnerabilities were identified, verified and the implications assessed. Recommendations are provided to improve the security of the state network from external threats.

2.2 Internal Vulnerability Assessment

ManTech evaluated the state network by using tools to scan the network, assessed the behavior of security devices and screening routers and firewalls, and analyzed potential target hosts identified. Scanning was done with administrator privileges to fully assess each host for vulnerabilities. Vulnerabilities were identified, verified and the implications assessed. Recommendations are provided to improve the security of the state network from internal threats.

2.3 Application Vulnerability Assessment

ManTech assessed two applications, the State Portal and Criminal Justice Information System for web-based application vulnerabilities. This evaluation was meant to compliment the vulnerability scanning process implemented by the Information Technology Department (ITD). ManTech personnel worked with ITD security administrators while onsite to offer recommendations for improving ITD's process of scanning applications for vulnerabilities.

2.4 Security Assessment of Non-consolidated IT Services

ManTech evaluated the physical and logical security of electronic mail, file, and printer server administration, database administration, and application server services that were not consolidated within the Information Technology Department. Vulnerabilities were identified, verified and the implications assessed. ManTech offered recommendations to improve the security of these services. Agencies assessed were the Office of the Attorney General, Department of Mineral Resources Oil and Gas Division, Public Service Commission, Water Commission, Housing and Finance Agency, and Department of Emergency Services.

2.5 Penetration Testing

ManTech used the information gathered in the assessments performed, in compliance with NDCC § 54-10-29 subsection 3, and developed penetration testing scenarios which targeted hosts and applications in an attempt to access protected information or demonstrate that such information could be accessed by unauthorized individuals. All scenarios were fully coordinated with the State prior to execution to limit operational impact to production systems.

3. ASSESSMENT APPROACH

3.1 External Vulnerability Assessment Approach

3.1.1 Background

The Internet is an integral part of an organization's day-to-day business and operations. Due to its open nature, the Internet is also a tool that is often used by attackers to disrupt an organization's ability to perform normal business activities. These attacks can lead to a loss of sensitive data, data integrity, productivity, and time, and be costly to correct.

An External Vulnerability Assessment is intended to provide an organization a snapshot of the overall security and risk picture of the network from an external (Internet) point-of-view. External assessment procedures focus on performing Internet research, discovering systems connected to the Internet, and selectively probing these systems to discover misconfigurations and vulnerabilities. Additionally, external assessments provide a means to capture the responsiveness of an organization's security devices and personnel. The assessment approach presented here consists of passive mapping, active mapping and vulnerability analysis which are described in more detail in the following sections.

3.1.2 Passive Mapping

This step emulates an outside threat (the average hacker) with limited knowledge of the network and involves enumerating the network and critical systems through open source techniques such as:

- Network and domain registrations
- Network administrator profiles (resumes, newsgroup postings, etc.)
- Web and news group postings
- Internet Research

This type of information gathering technique is frequently used by attackers to identify targets and obtain valuable information about a target. Passive mapping is an extremely effective data collection technique because the target is unaware intelligence is being collected.

3.1.3 Active Mapping

Once the passive mapping step is complete, active network probing begins with small stealthy probes and escalates to the use of very "loud" commercial tools to identify externally-facing systems on an organization's networks. Enumeration tools are used to identify critical resources that touch the Internet. Methods in this step include the following:

- DNS Zone transfers
- Single packet probes to specific targets

- Operating system identification scans
- Identifying server loads through custom packet probes
- Service and application scanning
- Using "bulk vulnerability" commercial scanning engines

If enough data regarding an organization's network is obtainable through misconfigurations and security holes on externally-facing systems, the Test Team will attempt to glean some preliminary data regarding an organization's internal network architecture. This phase only looks at vulnerabilities that are exploitable from the Internet.

Examples of such assets include limited reviews of the following if they are accessible:

- Databases
- Critical Servers
- Sensitive Data
- Access Credentials
- Network Nodes

Once the various devices that are accessible from the Internet have been identified and information about those devices cataloged, the process of identifying potential vulnerabilities can occur. The Team uses the data collected combined with the predefined goals to determine a course of action that will achieve the objectives defined for the assessment. It should be noted this is often a very fluid process. In some cases, misconfigurations can cause key data to be found during the mapping phase that allows for instant collection of data or access to systems directly from the Internet.

After all information is correlated, the Test Team attempts to confirm that any identified vulnerabilities are valid and do not represent false positives or are mitigated through other defenses.

3.2 Internal Vulnerability Assessment Approach

3.2.1 Background

An Internal Vulnerability Assessment is intended to provide an organization with a snapshot of the overall security and risk picture of the systems and network under assessment. Internal assessment procedures focus on examining networked systems for known vulnerabilities, misconfigurations, and implementation flaws that may expose the system to additional risk and is comprised mostly of automated testing complimented by manual inspection.

3.2.2 Internal Vulnerability Assessment Methodology

ManTech began the internal assessment with a review of open ports, protocols, and shared resources on each system. This phase of the internal assessment emulated the insider threat as both a person with limited access and knowledge and also as the trusted – curious, malicious, or unwitting insider. Sources of these types of threats range from cleared cleaning crews, maintenance workers, temporary employees, and other individuals (who can gain some type of

access to the facility and/or network but have no privileges on the system) to typical system users that use the network daily to fulfill their job duties.

After obtaining internal network access, we conducted a thorough vulnerability assessment, similar in nature, but much more comprehensive in scope than the external security assessment. The goal of the internal assessment was to identify potential vulnerabilities in the systems, as well as potential risks to critical data and systems, and recommend solutions to mitigate those risks. We tailored the assessment to each target set with the overall objective being to emulate the given threat as closely as possible to provide an accurate risk assessment of the system and the data it contains.

Once the various devices that were accessible have been identified and information about those devices cataloged, the process of identifying potential vulnerabilities occurred. The Team used the data collected combined with the predefined goals to determine a course of action that achieved the objectives defined for the assessment. It should be noted this is often a very fluid process. In some cases, misconfigurations caused key data to be found during the mapping phase that allowed for instant collection of data or access to systems.

After all information was correlated, the Test Team attempted to confirm that any identified vulnerabilities were valid and did not represent false positives or were mitigated through other defenses.

3.3 Application Vulnerability Assessment Approach

3.3.1 Background

Web-based applications are used extensively by many organizations to provide Internet users access to a variety of types of information. These applications are increasingly complex with numerous components such as databases which may contain sensitive data. Often custom developed applications focus on the functionality of the application and not the security of the application. An organization might have a secure web server, but if the web-based application that is hosted on the server can be compromised, then those protections are not effective.

3.3.2 Application Assessment Methodology

ManTech uses automated and manual methods to test the security of the selected application. We use a two-tiered approach to application security testing. We begin by using automated tools to capture a high-level security snapshot of the application. We then take testing one step further by providing expert analysis of these results and probing further into the application with manual techniques and custom written tools that can help find more elusive and less well known security flaws.

Advanced tools and techniques are use to find flaws in the following categories:

- Un-validated input
- Non-functioning access controls
- Authentication and session management issues
- Cross-site scripting flaws
- Buffer overflows
- Injection flaws
- Improper error handling
- Insecure data storage
- Denial of service (DoS)

Based on the business logic of the application, the application may also be tested using various roles. These roles correspond to differing levels of access to the system and the data it contains. This testing ensures that an account with one role (e.g. user) cannot access other portions of the application restricted to a different role (e.g. administrator functions). These tests are repeated for each role within the system, ensuring that access controls function properly at all levels.

3.4 Security Assessment of Non-consolidated IT Services Approach

3.4.1 Background

Physical, network, and system security assessment reviews were used in a baseline analysis of the agency's environment to include current security architecture and configurations. These reviews included a series of side-by-side tabletop reviews and discussions with key personnel focused on the technical implementation of specific security mechanisms within the agency's environment. Agencies assessed were the Office of the Attorney General, Department of Mineral Resources Oil and Gas Division, Public Service Commission, Water Commission, Housing and Finance Agency, and Department of Emergency Services.

3.4.2 Review Methodology

Side-by-side tabletop assessments are an extremely valuable and interactive approach to enhancing security while ensuring the agency's unique needs and environment are thoroughly addressed. The ManTech Test Team covered the following areas during the tabletop assessments:

- Physical Security
- Network Configuration and Architecture
- Network Access Controls
- Auditing
- Malware Protection/Antivirus
- Recovery and Back-Up Procedures
- Vulnerability Scanning
- Security Patch Updates

3.5 Penetration Testing Approach

3.5.1 Background

A penetration test is intended to provide an organization with a snapshot of the overall security and risk picture of its network from an external (Internet) or an internal point-of-view. Penetration testing focuses on gaining access to systems under an organization's control. Often a single system can provide a foothold into an organization's network and allow further access to external and/or internal systems. A penetration test requires extensive research, identification of an organization's systems and selectively probing these systems to discover misconfigurations and vulnerabilities. Additionally, penetration testing provides a means to capture the responsiveness of an organization's security devices and personnel. The penetration test performed by ManTech was conducted after an external and internal assessment of the State's network.

3.5.2 Penetration Testing Methodology

Penetration testing seeks to gain unauthorized access to systems, passing data that should be rejected/dropped by the network security controls, or disrupting communications to or between systems. Access includes user or administrator level privileges on systems, the ability to read/write/modify/delete data on protected systems, or the ability to adversely affect system operation. It is important to note that during penetration testing, exploit and privilege escalation tools and techniques were run by test team personnel, but no physically destructive attacks were performed.

The objectives of the network penetration test were to ascertain:

1. If security controls are properly implemented and functioning
2. Attack vectors that can cause harm to systems
3. The means to use said attack vectors to gain access to systems and data
4. Unauthorized use of technologies within that can put systems at risk
5. Security training and compliance with security policies
6. Personnel activities in response to threats and intrusions

The penetration test had three goals:

1. To emulate a realistic technical threat to the State computer networks
2. To discover and exploit any vulnerability or combination of vulnerabilities found on the system in order to meet the stated objective of the penetration test.
3. To test the extent the State's security incident response capability was alerted and to gauge the response to such suspicious activity.

Vulnerabilities can include unpatched services, misconfigurations, and poor security practices. Exploiting vulnerabilities is dependent on several factors:

- **Impact** – Some exploits can cause services to crash. ManTech tests all exploits within the safety of a closed test bed in order to minimize impact to State systems. Exploits that have the potential of causing long-term impact to the State's business processes were not used against production systems.
- **Availability** – Due to time constraints, the Test Team leverages existing public exploits (with modifications as needed), but the lack of a public exploit does not mitigate the risk of a particular vulnerability.
- **Time** – Vulnerabilities can be time dependent. A good example would be password cracking. Generally any password can be broken given enough time and computing power. The Test Team had a set time frame for the penetration test, but an attacker would not be hindered by time constraints or test controls.

4. VULNERABILITY ANALYSIS METHODOLOGY

Vulnerabilities are assigned a risk identifier that is relative to the network under test. These identifiers are intended as a notional representation of the severity of the vulnerability. They are provided as a reference to the overall probability of a loss and the consequences of that loss due to a particular vulnerability. These risk levels do not constitute a risk assessment or complete risk picture. Three risk levels are defined below:

High Risk – A high likelihood of compromise of system level access exists. If exploited this vulnerability may allow total control of the system.

Medium Risk – A vulnerability exists that may provide access to critical data and/or user level access to a system. This vulnerability may lead to further exploitation.

Low Risk – A vulnerability exists that may disclose information but does not directly lead to the exploitation of a system.

5. EXTERNAL VULNERABILITY ASSESSMENT RESULTS

Multiple tools were used to perform both automated and manual vulnerability scans against specific external systems as requested by the State. There were 3 high risk vulnerability findings, 7 medium risk vulnerability findings, and 1 low risk vulnerability finding. These vulnerability findings could generally be classified into two categories; misconfigured systems or applications, and operating systems or software applications that were missing critical security patches. Full technical details of these vulnerability findings can be found in the Vulnerability Assessment and Penetration Testing Technical Report provided to the State.

6. INTERNAL VULNERABILITY ASSESSMENT RESULTS

Multiple tools were used to perform both automated and manual vulnerability scans against specific internal network systems as requested by the State. There were 24 high risk vulnerability findings, and 3 medium risk vulnerability findings. These vulnerability findings could generally be classified into two categories; misconfigured systems or applications, and operating systems or software applications that were missing critical security patches. Full technical details of these vulnerability findings can be found in the Vulnerability Assessment and Penetration Testing Technical Report provided to the State.

7. APPLICATION VULNERABILITY ASSESSMENT RESULTS

The State requested two applications, the NDGOV State Portal and CJIS application, be assessed that had recently undergone an application assessment using the State's application assessment toolset. The purpose of this assessment was to help the State assess the effectiveness of their toolset in adequately performing application security reviews. The ManTech Test team used both automated scanners and manual testing techniques in the execution of this phase of testing. The NDGOV State Portal was found to have 1 medium risk vulnerability finding and the CJIS application was found to have 2 medium risk vulnerability findings. Full technical details of these vulnerability findings can be found in the Vulnerability Assessment and Penetration Testing Technical Report provided to the State.

8. SECURITY ASSESSMENT OF NON-CONSOLIDATED IT SERVICES RESULTS

Physical, network, and system security assessment reviews were conducted at each of the 6 identified state agencies. In addition, limited internal vulnerability assessment scanning and application security scanning were conducted if requested by the agency. Full technical details of these assessments are included in the State Agency reports provided to the State Auditor and individual State agencies. Specific vulnerability information was included in these reports so the individual agencies could take appropriate mitigation and remediation actions to correct the vulnerabilities. Physical security measures varied greatly between the agencies depending on the specific mission of the agency assessed. In most cases, the physical security of the agencies was adequate to very good.

It is recommended the State agencies with non-consolidated IT Services institute regular vulnerability scanning of all systems on a quarterly or bi-monthly basis to ensure to measure compliance with system patching requirements. Systems with vulnerabilities should be documented, evaluated and a determination made as to the validity of the vulnerability. For vulnerabilities determined to be valid, corrective action should be required and implemented (e.g. apply patch or other mitigation). Scans should be run with administrative privileges to ensure all vulnerabilities with locally installed software can be discovered and documented.

9. PENETRATION TESTING RESULTS

The Test Team proposed 11 penetration testing scenarios for further exploration based on the findings of the internal vulnerability assessment. Of these scenarios, 9 scenarios were approved for execution and testing was completed in December 2013 and January 2014. The Test Team achieved either user or system level access during five of the nine executed scenarios. The Test Team did not succeed in achieving system access on the remaining four scenarios. Full technical details of the penetration testing scenarios can be found in the Vulnerability Assessment and Penetration Testing Technical Report provided to the State.

10. GENERAL RECOMMENDATIONS

The following general recommendations are provided with respect to the overall network architecture and observed security practices:

Continue to Mature Structured Patch Management Program

Multiple systems were found to be missing critical operating system and application security patches. A baseline should be established to document deployed operating systems and application software installed on each system in the environment. Application software that is not mission critical should be removed. Regular reviews should then be completed to ensure all operating system and application security patches are deployed in a timely manner. Additional priority should be placed on the timelines for deploying patches to systems and applications that are publically accessible from the Internet.

Consideration should be given to implementing application white listing to enforce the State's application baseline. In addition, consideration should be given to implementing a continuous monitoring approach to provide real-time visibility to the State's patch status.

Internal Segregation of Critical Servers and Development Systems

Critical servers appear to be fully accessible from the internal network. It is recommended the State segregate servers deemed to be hosting critical data or services from the internal network by hosting these servers on a separate subnet strictly controlled by access-lists on an IP-to-IP and port-to-port basis. Lack of access control to these systems increases network exposure and risk from malicious users, worm and virus outbreaks. Additionally, development servers are currently hosted on the State’s production network. Development systems are typically default, unpatched installs which can pose a serious security risk to the rest of the network. It is recommended development systems be completely isolated on a separate subnet with no access to other State resources (e.g. email).

Require use of Encrypted Protocols for Remote Management

Large numbers of systems on the State’s external and internal network were noted using unencrypted protocols for remote access and management of systems. These protocols included FTP, Telnet, and VNC systems.

Security best practices recommend the use of encrypted protocols for remote access and management. In some cases, these systems may not be capable of using encrypted protocols. However, it is recommended critical systems utilize only secure protocols and where possible implement IP-based access restrictions.

Restrict Access to Protocols for Remote Management from the Internet

Multiple systems were running services such as Secure Shell, which are typically used for remote access and administration, available from the Internet. IP-based access controls should be put in place to restrict access to known and trusted IP addresses that have a legitimate need to connect to these services.

Develop a Formal Vulnerability Scanning Program- Non-consolidated IT Services

It is recommended the State agencies with non-consolidated IT Services institute regular vulnerability scanning of all systems on a quarterly or bi-monthly basis to ensure to measure compliance with system patching requirements. Systems with vulnerabilities should be documented, evaluated and a determination made as to the validity of the vulnerability. For vulnerabilities determined to be valid, corrective action should be required and implemented (e.g. apply patch or other mitigation). Scans should be run with administrative privileges to ensure all vulnerabilities with locally installed software can be discovered and documented.

11. SUMMARY

The findings presented in this report are typical of organizations with an enterprise the size of the State of North Dakota. Organizations with large numbers of systems face the challenge of maintaining a variety of operating systems, network devices, applications, and databases. Overall, there were 27 unique high risk findings found on multiple systems, 13 unique medium risk findings found on multiple systems, and 1 unique low risk finding found on multiple systems. These vulnerability findings could generally be classified into two categories; misconfigured systems or applications, and operating systems or software applications that were missing critical security patches.

Of greatest concern, multiple systems were found to be missing critical operating system and application security patches. A baseline should be established to document deployed operating systems and application software installed on each system in the environment. Application software that is not mission critical should be removed. Regular reviews should then be completed to ensure all operating system and application security patches are deployed in a timely manner. Additional priority should be placed on the timelines for deploying patches to systems and applications that are publically accessible from the Internet. Wrapping these initiatives into a robust Enterprise Patch Management capability should be a top priority moving forward.

Due to the shared nature of the State's internal network (as with the external), the security posture of each agency directly impacts the security of the other agencies. Poorly maintained and patched systems in one agency could lead to compromise of these systems and inevitably the use of these systems for attacks against other State systems across the internal network. While the State seems to be doing an excellent job ensuring Operating System patches are deployed, a fundamental weakness continues to exist in ensuring applications installed on these systems are patched as well.

The results of the penetration testing also illustrate that attackers often only need to gain access to one system to provide a firm foothold from which to expand the exploitation of an organization. This testing enforces the importance of keeping systems patched in a timely manner, validating that patches have been successfully applied, periodically testing the organization's systems for security vulnerabilities and weaknesses, and the importance of actively monitoring network and system activity for suspicious events from both external and internal sources.