ManTech
International Corporation

Leading the Convergence of National Security and Technology℠

2012 North Dakota Information Technology Security Audit
Vulnerability Assessment and Penetration Testing Summary Report

28 September 2012

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 Shaw
Executive Director, Cyber Security Operations
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	20 September 2012	Initial Draft
2.0	28 September 2012	Final Version

TABLE OF CONTENTS

1. Introduction **3**
2. Assessment Scope **4**
2.1 External Vulnerability Assessment 4
2.2 Internal Vulnerability Assessment 4
2.3 Penetration Testing 4
3. Assessment Approach **5**
3.1 External Vulnerability Assessment Approach 5
3.2 Internal Vulnerability Assessment Approach 6
3.3 Penetration Testing Approach 7
4. Assessment Results **10**
4.1 Vulnerability Analysis 10
4.2 External Vulnerability Assessment Results 10
4.3 Internal Vulnerability Assessment Results 10
4.4 Penetration Testing Results 11
5. General Recommendations **13**
8. Summary **15**

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. This type of 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 May through August 2012, ManTech performed an external vulnerability assessment, internal vulnerability assessment, and penetration testing of the State of North Dakota's statewide computer 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.

In addition to automated scanning, ManTech evaluated the current information technology policies, practices and tools used by ITD for virtual machines, implemented firewalls, and IP Phones.

2.3 Penetration Testing

Using the results of the previous external security testing, ManTech attempted to develop penetration testing scenarios which targeted vulnerable hosts from the Internet. All scenarios were fully coordinated with the State prior to execution to limit operational impact to production systems.

ManTech also conducted a social engineering study, in which the test team attempted to gain information on or access to State systems by targeting users of the ConnectND system. This was a remote assessment targeting the users through a phishing email scenario that was pre-approved by the State POC and Trusted Agent prior to execution.

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 identify critical resources that touch the Internet. Methods in this step including 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 Vulnerability Assessment

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 Penetration Testing Approach

3.3.1 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.

3.3.2 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** – Many 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.

Social engineering is part of penetration testing and involves the attempt to gain information or access through means other than through technical vulnerabilities. However, in some cases social engineering leverages technical vulnerabilities and weaknesses. The social engineer uses a combination of knowledge, salesmanship, and trickery to get members of an organization to break security policy by revealing passwords, customer data, or other privileged information.

Social engineering attacks commonly use the Internet to trick people into revealing sensitive information, or get them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting

computer security holes. It is generally agreed upon that "users are the weak link" in security and this principle is what makes social engineering possible.

Social Engineering attacks involving e-mails are often referred to as phishing. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using e-mail or an instant message. Web Based Exploitation commonly follows E-Mail Exploitation in two common forms. In its first form, phishing e-mails attempt to lure users to a fictitious website wherein they are prompted to enter sensitive information. The information users enter on the website is being collected behind the scenes by an attacker who is logging all activity. In its second form, phishing e-mails prompt users to click on a malicious link, modified to carry out exploitation of a user's system or to download and execute a malicious executable. These harvesting techniques are substantially less time consuming than trying to penetrate a system using purely technical resources. The techniques are often exploited as many organizations do not provide awareness training to their employees. In order for e-mails and websites to appear more legitimate, attackers will use the information they gathered through open source Internet research.

4. ASSESSMENT RESULTS

4.1 Vulnerability Analysis

Vulnerabilities were 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.

4.2 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 6 unique high risk vulnerabilities found on multiple systems, 4 unique medium risk vulnerabilities found on multiple systems, and 1 unique low risk vulnerability 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. Full technical details of these vulnerability findings can be found in the Vulnerability Assessment and Penetration Testing Technical Report provided to the State.

4.3 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 22 unique high risk vulnerabilities found on multiple systems, 4 unique medium risk vulnerabilities found on multiple systems, and 2 unique low risk vulnerability 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. Full technical details of these vulnerability findings can be found in the Vulnerability Assessment and Penetration Testing Technical Report provided to the State.

4.4 Penetration Testing Results

4.4.1 Direct Penetration Testing

The ManTech Team proposed five penetration testing scenarios for further explorations based on the findings of the external vulnerability assessment. Upon a detailed review of each system and publically available exploits for the identified vulnerabilities, the Test Team determined none of the proposed scenarios were viable for execution.

4.4.2 Phishing Exercise

Description

The phishing scenario that was executed was based on the recent publicized rollout of the ConnectND PeopleSoft Talent Management Suite. The ManTech Assessment Team sent phishing e-mails to 545 state employees claiming to be from the administrator of the ConnectND system. The email requested the users login in to the ConnectND portal to test new performance features of the Talent Management Suite. The e-mail requested recipients to log onto a Test Team controlled mockup of the ConnectND portal, and enter their standard Peoplesoft credentials to test the new features.

Upon clicking the hyperlink in the e-mail, the user was redirected to a spoofed ConnectND website.. The spoofed website is a modified copy of the official ConnectND main portal and was crafted to be nearly identical to the official website. The ManTech Assessment Team inserted a custom Active Server Page (.asp) script on the modified webpage that captured usernames and passwords that were entered. All login data entered into the site was SSL encrypted.

Once users entered their login credentials, they were directed to another webpage to assess their susceptibility to run unauthorized executables on their system. This webpage informed the users that there was an error processing their login, request they download PeopleSoft Security patch to fix this issue, and provided users step-by-step guidance on how to run the "PeopleSoft Security patch".

In this particular scenario, an attacker could potentially use the harvested usernames and passwords to gain access to State computer network systems and resources. An attacker could have also crafted the "Peoplesoft Security Patch" tool to perform a number other activities. For example, a backdoor could be installed on the system which would allow the attacker full access to the user's system at any time. With access to the system the attacker could capture all sensitive information stored on the system or communicated through the system. The attacker could also use the system as a hopping point in which to conduct attacks on internal network resources or other external targets.

Upon sending the email, the Test team received 33 "Out of Office" messages and 13 delivery failure messages. This reduced the potential target population to 499. The Assessment Team's website collected the first set of user credentials from a State user within five minutes of the initial phishing emails being sent. The first report by a State user of the email to the ITD Service

Desk occurred at approximately 9:14am. ITD simulated a block of the malicious domain at approximately 9:30am and a security advisory was sent to all IT coordinators at 9:55am.

Overall there were 130 submissions of user credentials on the site. After removing duplicate logins from this total, the Test Team collected 63 sets of valid credentials. This represents a success rate of approximately 12.6% of targeted users. Of these users, 44 (8.8%) had entered their credentials prior to the simulated network block being put in place.

Next, there were 36 executions of the "Peoplesoft Security Patch" executable downloaded from the Assessment Team website. After removing duplicate systems from the logs where a user downloaded and executed the tool on the same system more than once, it was found that the tool was executed on 10 unique State systems. This gives a success rate of approximately 2% of targeted users. Of these, 5 systems (1%) downloaded and ran the executable prior to the simulated network block being put in place.

5. GENERAL RECOMMENDATIONS

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

Implement Formal 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.

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 internal network were noted using unencrypted protocols for remote access and management of systems. These protocols included the following:

FTP
Telnet
VNC
R-Services

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 Microsoft Remote Desktop Protocol and 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.

8. 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 28 unique high risk findings found on multiple systems, 5 unique medium risk findings found on multiple systems, and 2 unique low risk findings 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 this testing also illustrate that users continue to be one of the weakest links to an organization's security posture. Attackers often only need to gain access to one system to provide a firm foothold from which to expand the exploitation of an organization. Continuing education and training of users is necessary to minimize the risk to an organization. This testing also enforces the importance of keeping systems patched in a timely manner, validating that patches have been successfully applied, and the importance of monitoring network and system activity for suspicious events from both external and internal sources.