APPENDIX K

ManTech International Corporation®

Leading the Convergence of National Security and Technology℠

North Dakota 2016 IT Security Audit Vulnerability Assessment & Penetration Test Project Briefing

Introduction

ManTech International Corporation

ManTech Project Manager

John Stiffler, Security Consultant
ManTech Mission, Cyber, and Intelligence Solutions Group
John.Stiffler@mantech.com
(814)244-1732

Assessment Overview

ManTech International Corporation

- Assessment conducted January to March 2016
- 6 Major Project Tasks
  - External Vulnerability Assessment
  - Internal Vulnerability Assessment
  - Application Vulnerability Assessment
  - Security Infrastructure Review
  - Incident Response Review
  - Penetration Testing

Vulnerability Assessment Overview

ManTech International Corporation

- A Network Vulnerability Assessment targets an organization's IT infrastructure (network, servers, workstations, etc) with the goal of identifying security weaknesses that could be exploited
- External assessments are conducted from the Internet and mirror the threat of a malicious outsider (ie- hacker)
- Internal assessments are conducted on an internal corporate network and mirror the threat of a malicious insider

Vulnerability Assessment Overview

ManTech International Corporation

- Assessment methodology
  - Commercial vulnerability scanning software used initially to identify all systems connected to the network and the services they are providing (ie- web server, email server, file server, workstation, etc)
  - Scanning software then runs a series of automated checks to identify vulnerabilities in the installed software and system configurations/settings

Vulnerability Assessment Overview

ManTech International Corporation

- Assessment methodology (continued)
  - Once the Test team has completed review, the consolidated findings are be presented in a written technical report which identifies the vulnerabilities found during the assessment along with specific remediation recommendations for how to correct the findings and properly secure the system.

Vulnerability Assessment Scope

ManTech International Corporation

- External Assessment
  - Test Team focused efforts on approximately 57 publically accessible network segments hosting both ITD and State Agency systems
- Internal Assessment
  - Test Team scanned 127 internal network segments hosting both ITD and State Agency systems

Vulnerability Assessment Results

ManTech International Corporation

- All vulnerability findings were rated as critical, high, medium or low risk
  - **Critical Risk:** The risk contains a high likelihood of being exploited, and would cause exceptionally grave damage to the information system if exploited
  - **High Risk:** A malicious user that exploits this level of vulnerability could achieve full control of the system and all data contained on the system
  - **Medium Risk:** A malicious user that exploits this level of vulnerability could achieve limited user level control of the system and/or compromise data contained on the system
  - **Low Risk:** A malicious user that exploits this level of vulnerability could achieve limited access to data contained on the system

Vulnerability Assessment Results

ManTech International Corporation

- Vulnerability findings were present at all levels, critical, high, medium and low
- All findings could be classified into two major areas: patch management and configuration management
  - Continue to refine the current patch management program
  - Enforce a strong configuration management program

Application Vulnerability Assessment Overview

ManTech International Corporation

- Two-tiered approach to application security testing
  - Automated scanning
  - Manual assessment
- Focus on common application vulnerability issues
    - 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)

Application Vulnerability Assessment Scope

ManTech International Corporation

- ManTech assessed one application
  - State Workforce Safety Portal
- This application was assessed due to a breach which occurred in a previous version

Application Vulnerability Assessment Results

ManTech International Corporation

- No critical or high risks were detected at the time of scanning
- However, there were medium and low risk findings detected.

Security Infrastructure Review Overview and Scope

ManTech International Corporation

- Test Team evaluated the policies, practices and tools being used within ITD
- Test Team interviewed key staff
- Items evaluated included:
  - Network Configuration and Architecture
  - Network Access Controls
  - Auditing
  - Malware Protection/Antivirus
  - Recovery and Back-Up Procedures
  - Vulnerability Scanning
  - Security Patch Updates

Incident Response Review Overview and Scope

ManTech International Corporation

- Test Team evaluated the policies, practices and tools being used within ITD
- Test Team participated in an Incident Response Exercise
- Items evaluated included:
    - Existing policies and procedures documentation
    - Notification processes
    - Job responsibilities
    - Actions taken during the exercise
    - Event documentation
    - Chain of custody

Security Infrastructure and Incident Response Review Results

ManTech International Corporation

- No critical findings, but there were high, medium and low findings
- The need to continue to mature and enforce a structured enterprise patch management program
- Finalize and enforce policies and procedures to ensure a common security program across the entire network.
- Ensure employees receive adequate formal training for security related items, such as incident response and intrusion detection
- Documentation must be made a priority during incident response operations

Penetration Testing Overview

ManTech International Corporation

- Purpose is to emulate realistic & current threats in an attempt to gain access to systems and/or information via both technical and non-technical means
- Testing attempts to exploit discovered vulnerabilities and test an organization's mitigation techniques
- Primary Test methods
  - Direct System Exploitation

Penetration Testing Results

ManTech International Corporation

- Direct Exploitation
  - All scenarios assumed access to the internal state network. These scenarios depicted an employee based attack.
    - Test Team explored multiple potential scenarios based on assessment results
    - Of the scenarios tested, all led to direct system access
      - Note: The agreed upon scenarios may have by-passed a level or multiple levels of mitigating controls

General Security Recommendations

ManTech International Corporation

- Continue Maturation of Patch Management Program
  - Baselines need to be established for all operating system and application software used on the network and regular patching processes set up to ensure all systems receive critical patches in a timely fashion
  - Focus on 3rd party applications; consider application white listing
  - Adherence to patch management timelines with compliance monitoring
  - Continuous Monitoring approach for real-time visibility
- Create, Follow and Enforce an Effective Continuous Monitoring Policy and Procedure
  - Although Continuous monitoring is taking place, there are no policies or procedures in place which allow ITD to enforce ramifications for failed compliance.

General Security Recommendations (cont)

ManTech International Corporation

- Provide additional technical security training to staff
  - Incident response training
  - Intrusion detection training
- Update, finalize and enforce policies and procedures
  - Institute periodic review and updating of policies and procedures, this will help ensure a common security stature across the network.
- Review and update all encryption
  - Pre-shared keys should be updated at least annually, and when an IT staff member with access to the pre-shared keys leaves ITD. This ensures the security of the connections from malicious users.

Conclusion

ManTech International Corporation

- Results of this assessment are typical for organizations of a similar size and maturity
- The top recommendation to improve security of the network is to provide ITD with the authority to disconnect non-compliant systems from the network. ITD has identified multiple systems which are misconfigured or out of date, but do not have any control over those system.

Questions

ManTech
International Corporation

ManTech
International Corporation

Leading the Convergence of National Security and Technology℠

2016 North Dakota Information Technology Security Audit
Vulnerability Assessment and Penetration Testing Executive Report

27 July 2016

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
Paul Martin
Senior Executive Director, Cyber Security Solutions
1951 Kidwell Dr, Suite 500
Vienna, VA 22182
Phone: 703.388.2126
E-mail: paul.martin@mantech.com

DOCUMENT REVISION HISTORY

Version	Date	Change Description
1.0	29 June 2016	Initial Draft
1.1	13 July 2016	Minor updates
1.2	27 July 2016	Added ITD responses
2.0		

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 January, February and March 2016, ManTech performed an external/internal vulnerability assessment of the State of North Dakota's statewide computer network and application security assessment of the States Work Force Safety web application. In March 2016, ManTech performed multiple penetration testing scenarios against the State's internal network.

1.1 Assessment Participants

Role	Participant	Organization	Phone
State Audit Lead	Donald Lafleur	ND State Auditor's Office	(701) 328-3744
State ITD Lead	Uriah Burchinal	ND Information Technology Department	(701) 328-2164
Test Team Lead	Paul Martin	ManTech	(703) 388-2126
Test Team Member	John Stiffler	ManTech	(703) 388-2126
Test Team Member	James Daniel	ManTech	(703) 388-2126
Test Team Member	Casey Bourbonnais	ManTech	(703) 388-2126

1.2 Security

All data will remain confidential to the testing parties. All test data and results will only be disclosed to authorize individuals. The tools authorized for use during the testing of State networks are either commercial off-the-shelf (COTS) or open-source. All State related assessment data is maintained on secure systems and will always be encrypted when transmitted electronically.

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 the Work Force Safety web application 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 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

The 2016 assessment scope was much different than past assessments. This assessment was much more in depth and done on a much wider range of networks than past assessments. This assessment included thousands of IP addresses, which included both ITD and ITD customers, internal and external. Compared to past assessments, this assessment dwarfs previous device assessment totals.

Because of the significant difference in the number of devices assessed, it is impossible to compare past assessments to this assessment. Although this assessment reports what seems to be a large number of vulnerabilities, those numbers need to be placed into context compared to the number of devices scanned. Also, to add context to the large number of findings, it must also be understood that many devices scanned and reporting findings are out of ITD's control, which are controlled by ITD's clients.

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 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 if 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 with 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 used 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 Penetration Testing Approach

3.4.1 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.

3.4.2 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, misconfiguration, 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:

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

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. VULNERABILITY ASSESSMENT RESULTS

Multiple tools were used to perform both automated and manual vulnerability scans against specific internal and external systems as requested by the State. The scans were conducted against thousands of IP addresses across multiple subnets, including subnets managed by ITD clients.

External blacklisted scan results found critical, high, medium and low risk vulnerability findings. The critical and high findings are the most concerning, considering these devices are publicly accessible, and should be addressed immediately.

Internal and external white listed scan results also found critical, high, medium and low risk vulnerability findings. The critical and high risk findings is relatively low for a network this size.

Also, Mantech specifically scanned the 911 external website. External blacklist scan results found no critical or low risk vulnerability findings, but did find high and medium risk vulnerability findings. Whitelisted scan results found no critical risk findings, but did find high, medium and low risk findings. As stated above, any critical or high vulnerability discovered during a black listed scan should be addressed immediately.

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.

6. SECURITY INFRASTRUCTURE REVIEW

The State requested an evaluation be done on the information technology policies, practices and tools being used for security. The purpose was to help the State assess the effectiveness of their policies, practices and toolsets for ensuring best security practices. The ManTech team reviewed documentation, drawings and held interviews with key team leads to determine ITD's effectiveness.

Mantech's evaluation of the Security Infrastructure found high, medium and low risk vulnerability findings. The recommendations from this review include enforcing a structured enterprise patch management program, providing fromal training to staff and to finalize and enforce policies and procedures. Further explanations of the recommendations can be found in section 10 of this document.

7. INCIDENT RESPONSE REVIEW

The State requested an evaluation of the Incident Response policies and procedures. The purpose was to help the State assess the effectiveness of their policies and procedures for ensuring best practices. The ManTech team reviewed documentation, and participated in a table top exercise held by the ITD team.

Mantech's evaluation of the Security Infrastructure found no critical or low risks, but did find high and medium risk vulnerability findings. The recommendations from this review is to providing formal incident response training to specialized IR staff and to finalize and enforce policies and procedures. Further explanations of the recommendations can be found in section 10 of this document.

8. APPLICATION VULNERABILITY ASSESSMENT RESULTS

The State requested the North Dakota workforce safety web application be assessed (https://www.workforcesafety.com/wsi). The purpose was to help the State assess the effectiveness of their security reviews. The ManTech Test team used Burpsuite in the execution of this phase of testing.

Mantech's evaluation of the workforce website found no critical or high risks, but did find medium and low risk vulnerability findings. The recommendations from this review is to ensure timely patching of the web server, as well as confirming proper security configuration are applied to all web servers. Further explanations of the recommendations can be found in section 10 of this document.

9. PENETRATION TESTING RESULTS

The Test Team performed multiple penetration test scenarios for further explorations based on the findings of the internal vulnerability assessment. Of these tests performed, the test team was successful in all scenarios. Of the scenarios tested, the test team found critical, high, medium and low risk vulnerability finding.

The tests resulted in recommendations to remove outdated technologies, ensure adequate patching practices, increase network segmentation and to apply increased security controls across the information system. These recommendations are consistent with recommendations created from the internal and external technical scan results. Further explanations of the recommendations can be found in section 10 of this document.

10. GENERAL RECOMMENDATIONS

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

Enforce a Structured Enterprise Patch Management Program

While onsite, discussions with staff made it clear that although ITD does have a patch management program in place and being followed, this program only touches ITD devices. With ITD acting as a service provider to other North Dakota agencies, they are responsible for the security of the client systems. ITD must be able to create and enforce a patch management policy which it should be able to enforce with all of its clients. When a client fails to do updates in a timely fashion, it is increasing the risk of a breech, as well as putting the whole network at risk.

Provide Additional Training to Staff

While conducting the Incident Response interviews, it was determined that ITD has not provided formal training for dealing with incidents, staff instead have relied on their own knowledge or informal training. It would be very beneficial for ITD to have someone on staff with this training. The training should include training for management of an incident, as well as for performing technical analysis of an incident. Training can be obtained by visiting www.sans.org or www.cert.org, as well as many other places.

IT was also determined during the network assessment interviews that no one has any formal IDS training. Using a no trust network design relies heavily on the use of IDS systems. Without proper training and knowledge of the use and monitoring of the IDS systems, attacks can go undetected. Proper training will provide administrators with the knowledge for what to look for in the logs, as well as the ability to tune the IDS to make it more effective.

Update, Finalize and Enforce Policies and Procedures

ITD should continue to update and finalize the documents and disseminate the document to all customers to ensure the customers are meeting the requirements set forth by ITD. The policies should include ramifications for not following the policies.

Review and Update all Encryption

While performing the network assessment interviews it was determined the encryption used for point to point connections is using shared passwords. The passwords are not only a standard, but also have not been changed in many years (no one knew the last time they were changed). Because of this, all encryption used throughout the network should be reviewed and changed as required. All P2P encryption should be updated to use certificates, and no longer a shared password. A policy should also be established to ensure an annual review or encryption being used.

Along with the review of all the encryption, ensure that only suitable versions of SSL/TLS are enable on all external facing websites. Many versions of SSL/TLS are now vulnerable to outsider attack and should be disabled.

Create, Follow and Enforce an Effective Continuous Monitoring Policy and Procedures

While interviewing staff for the network assessment, it was pointed out that some continuous monitoring is performed on the network, but there is no enforcement for non-compliance. In order to have an effective Continuous Monitoring program, a policy and procedures document must be created, a set scanning schedule needs to be set, a Plan of Actions and Milestones (POAM) must

be created and maintained, and ramifications for not following the policy must be set. The POAM will include issues found during the scans, a responsible person for correcting the issues, and a due date.

It was also determined that while monthly scanning is taking place, the scanning is incomplete. Scans need to be set up to scan all equipment, including servers, server and storage hardware, hypervisors, network gear, websites, databases, and any other device that has access on the ITD network.

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, the number of findings were expected within a network this size, with the lack of control over customer networks. 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 were the critical and high finding on multiple systems when doing blacklist scans. A Blacklist scan is equivalent of an attacker scanning the network to find vulnerabilities. These vulnerabilities present a real risk to the network and should be addressed immediately. Regular reviews should then be completed to ensure all operating system and application security settings and 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 ITD seems to be doing an excellent job ensuring patches are deployed to ITD controlled assets, a fundamental weakness continues to exist in ensuring client 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, 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.

12. ITD RESPONSES

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

Enforce a Structured Enterprise Patch Management Program
While onsite, discussions with staff made it clear that although ITD does have a patch management program in place and being followed, this program only touches ITD devices. With ITD acting as a service provider to other North Dakota agencies, they are responsible for the security of the client systems. ITD must be able to create and enforce a patch management policy which it should be able to enforce with all of its clients. When a client fails to do updates in a timely fashion, it is increasing the risk of a breech, as well as putting the whole network at risk.

ITD does indeed have a formal patch management program in place and that program is followed as documented. ITD's patch management program is for all ITD devices and other agency desktops that under ITD support. While ITD does agree that a centrally managed patch management program would be beneficial desktops not required to be supported by ITD are the responsibility of the owning agency.

Provide Additional Training to Staff

While conducting the Incident Response interviews, it was determined that ITD has not provided formal training for dealing with incidents, staff instead have relied on their own knowledge or informal training. It would be very beneficial for ITD to have someone on staff with this training. The training should include training for management of an incident, as well as for performing technical analysis of an incident. Training can be obtained by visiting www.sans.org or www.cert.org, as well as many other places.

IT was also determined during the network assessment interviews that no one has any formal IDS training. Using a no trust network design relies heavily on the use of IDS systems. Without proper training and knowledge of the use and monitoring of the IDS systems, attacks can go undetected. Proper training will provide administrators with the knowledge for what to look for in the logs, as well as the ability to tune the IDS to make it more effective.

Formal incident handling training such as that from SANS and the US-Cert have not currently been part of ITD's training. Such formal training is now in progress. Also to note are part of the updated Security Incident plan training specific to ITD incident handling policies and procedures will be put in place.

The ITD networking staff that is responsible for maintaining the IDS/IPS systems has the knowledge and proper network training to be able to effectively manage such systems.

Update, Finalize and Enforce Policies and Procedures

ITD should continue to update and finalize the documents and disseminate the document to all customers to ensure the customers are meeting the requirements set forth by ITD. The policies should include ramifications for not following the policies.

ITD continues to work on updating and formalizing policy aligned with NIST 800-53. These policies include the enforcement clause as required by NIST.

Review and Update all Encryption

While performing the network assessment interviews it was determined the encryption used for point to point connections is using shared passwords. The passwords are not only a standard, but also have not been changed in many years (no one knew the last time they were changed). Because of this, all encryption used throughout the network should be reviewed and changed as required. All P2P encryption should be updated to use certificates, and no longer a shared password. A policy should also be established to ensure an annual review or encryption being used.

Along with the review of all the encryption, ensure that only suitable versions of SSL/TLS are enable on all external facing websites. Many versions of SSL/TLS are now vulnerable to outsider attack and should be disabled.

ITD agrees with the finding in regards to updating and changing at regular intervals the point to point shared passwords. Updates to the SSL/TLS versions are being updated for external sites as the certificates are renewed.

Create, Follow and Enforce an Effective Continuous Monitoring Policy and Procedures

While interviewing staff for the network assessment, it was pointed out that some continuous monitoring is performed on the network, but there is no enforcement for non-compliance. In order to have an effective Continuous Monitoring program, a policy and procedures document must be created, a set scanning schedule needs to be set, a Plan of Actions and Milestones (POAM) must be created and maintained, and ramifications for not following the policy must be set. The POAM will include issues found during the scans, a responsible person for correcting the issues, and a due date.

It was also determined that while monthly scanning is taking place, the scanning is incomplete. Scans need to be set up to scan all equipment, including servers, server and storage hardware, hypervisors, network gear, websites, databases, and any other device that has access on the ITD network.

ITD does scan for the majority of items listed here. The inclusion of storage, network, and databases is being evaluated at this time as a more comprehensive plan is in development.