



ManTech
International Corporation®

Leading the Convergence of National Security and TechnologySM

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

ManTech Project Manager

John Stiffler, Security Consultant

ManTech Mission, Cyber, and Intelligence Solutions Group

John.Stiffler@mantech.com

(814)244-1732

- 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



- 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



- 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

- 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.



- 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



- 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 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

- 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 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

- 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

- 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

- 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

- 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



- 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



- 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

- **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.



- 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.

- 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.

