Vulnerability Management

Enhancing Security for Servers & Applications

The Evolution of Vulnerability Management

December 2016 – December 2018

The State of Tennessee
Department of Finance and Administration
Division of Strategic Technology Solutions

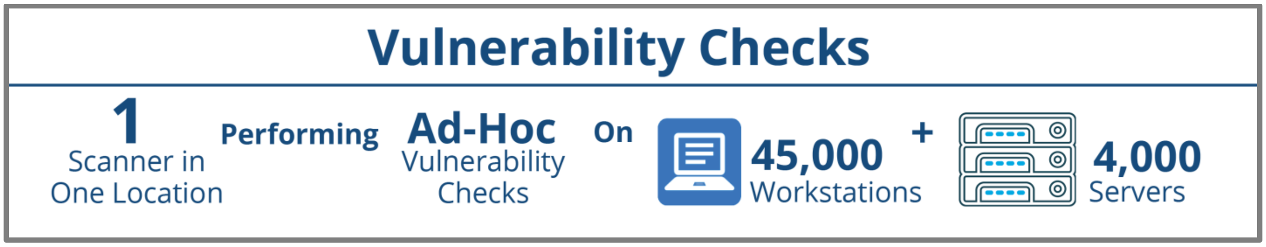
NASCIO Award Category: Cybersecurity
Contacts: Addy Newsom, Project Coordinator CIO Office
Curtis Clan, Chief Information Security Officer

TN Department of Finance & Administration | Strategic Technology Solutions

Executive Summary

Given the Information Technology (IT) centric world we operate in, risk of a breach is high and the consequences are potentially dire. Every effort made to secure our 4,000 servers, our 45,000 workstations and our IT network provides critical protection not only within Tennessee State Government but for all Tennessee citizens, as well.

The State of Tennessee Security Vulnerability Management Program is a patch scanning program designed to expose weaknesses on all servers in real-time. Prior to this implementation the state had only one scanner, in one location where vulnerability checks could only be performed ad-hoc, leaving the state susceptible to attack.



Vulnerability Checks

1 Scanner in One Location **Performing** **Ad-Hoc** Vulnerability Checks **On** **45,000** Workstations **+** **4,000** Servers

The team faced significant hurdles throughout the process such as application limitations, budgetary shortfalls, and no way to map vulnerabilities to responsible parties. The Vulnerability Management (VM) team was able to utilize their exceptional skills to reconfigure the Archer application to allow for an integration process that even the manufacturer failed to implement. The budgetary issues were addressed by keeping the project timeline fluid until all necessary purchases were secured.

This project is a win that helped improve the State of Tennessee's security posture. The project team's disposition in working with customers on security issues has helped to improve the reputation of security overall and to reduce friction with those affected by challenging findings.

Concept

The State of Tennessee’s central IT organization, Strategic Technology Solutions (STS), is responsible for the administration of 4,000 servers, 45,000 workstations, and the statewide network. STS performs all operating system patches and updates. Prior to the establishment of the STS Security Vulnerability Management (VM) Program, the number and degree of vulnerabilities across all servers was unknown.

The VM program, a standalone project, was largely created from a vulnerable position. There was a single Nessus scanner in a downtown Nashville office building with no application testing capability. Vulnerability scans were performed on an ad-hoc basis.

The initial goals were to scan all servers in the data center and to work with a third party security vendor to test hand-picked, high-priority web applications. This mission eventually grew to testing all servers on a regular and frequent schedule, to expand the number of applications being tested, and to develop application testing capability at STS to augment testing done by the security vendor.

Project Mission

1. **Consistency** Testing all servers on a regular and frequent schedule
2. **Expansion** Expand the number of applications being tested
3. **Development** Develop application testing capability at STS to augment testing done by the security vendor

To this end, simultaneously testing in-house and vendor developed applications for vulnerabilities became a priority. The STS VM team was tasked with developing a methodology to effectively test a large number of disparate web applications for common security flaws.

Given the experience with Tenable Nessus, the decision was made to upgrade to the enterprise version of Nessus, SecurityCenter (now known as Tenable.sc). The VM team attempted to leverage Core Impact and HP Webinspect for application testing, but ultimately found that the much lighter weight tool, Burp Suite Professional, was more effective for finding programming flaws. This allowed the team to drop the larger, more expensive applications entirely.

Implementation was not without its challenges. Firewalls and VLANs presented major roadblocks. Scanning can be done through firewalls, but scans can degrade firewall performance and firewalls can affect scan results. The solution to these problems was to create global firewall rules for scanners and to create virtual machine scanners placed strategically throughout the network to allow access to all VLANs and physical locations.

Integrating SecurityCenter and Archer was even more challenging. STS was promised “out of the box integration” between these two systems. In fact this did not exist at all and had to be created by the VM team using Application Programming Interface (APIs), Extensible Markup Language (XML) transforms, PowerShell scripting, and extensive Archer customization.

The methodology utilized for this implementation was gradual and methodical. The number of Nessus scanners was increased over the course of two years to eventually reach servers everywhere on the network, regardless of firewalls and VLANs. This approach was chosen out of necessity as the VM team expanded equipment and software licensing only as funding became available.

The VM team identified highest impact areas by assigning all findings, whether server or application, a severity level. Vulnerabilities can also be grouped into exploitable and non-exploitable categories. Vulnerabilities have ages which indicate the number of days since first detected. The approach to identifying the highest impact areas is to concentrate on the most critical, oldest, most publicly accessible vulnerabilities. As these are remediated, lower risk, less severe findings can be addressed.

Early on, the risks were single points of failure, lack of expertise, and lack of funding. The VM team learned the technology, additional servers were deployed, and funding continues to be a challenge.

The implementation timeline was not formal until it was clear the VM team had the tools and abilities to accomplish the scanning and application testing goals. Once the tools were available, the desired timeline was approximately 1.5 years to scan all servers and have the results automatically fed into the Archer GRC tool.

The costs associated with this project include three full time employees of the VM team who put in over 2,000 hours through the two year process. Additional software licenses were purchased gradually, over the two years of the project, totaling $ 150,000.

Cost of the Project

3 Full Time Employees	2,000 Hours	2 Year Process	$150,000 Software Licenses

Project oversight fell under the auspices of the State Cyber Information Security Officer (CISO). The STS VM team consisted of a systems architect, an auditor, and a software developer. Executive management asked the VM team to expand to more and more systems and applications, and to increase depth of scans and application tests. They fought for funding and helped with direction and selection of software. They provided the freedom the team required in the form of time to learn how to use the tools, and to configure and integrate different systems.

Senior management's approach to this project was and is a strong factor in our success. They practice a largely hands-off approach with the STS VM team, allowing the team the time and flexibility to solve problems without excessive guidance and bureaucracy. There was pressure to get the job done, but timelines were reasonable and attainable.

The initiative will be assessed by its consistency and in the State's ability to successfully scan servers and applications for vulnerability across state government. The program is going well and there is no expectation that this would change.

Accessibility and Information Security

The vulnerability management program is subject to much scrutiny. Each agency has access to Archer with dashboards and reports that show at a glance the current state of vulnerability within their systems and applications. They have a reasonable expectation that vulnerability counts and severities will trend downward. STS Domain Information Security Officers also study the information and are quick to make the VM team aware of accumulating issues. Metrics are provided to the CISO and Executive Leadership on a monthly basis. The entire security program, including vulnerability management undergoes annual State and third party audits. The state is responsible for 100% of the oversight of this initiative and outcomes.

The VM team took a simple approach toward creating awareness and training for the project by providing workshops and user guides with step by step instructions for the use of Archer across agencies.

Significance

The scope of this project is to scan all servers and all applications for vulnerabilities on a regular basis. The beneficiaries and stakeholders would be the state agencies and the citizens they serve.

A challenge that brought about enormous internal innovation with, and distinction for, this project was centered in integrating the SecurityCenter and Archer systems. STS was promised "out of the box integration" between these two systems, but this was not the case. The team created the integration from scratch, including an extensive in-house customization completing the partially implemented vendor solution. The successful implementation of this project provides the ability to scan all systems regularly and repeatedly. It is the ability to have all results fed into the Governance, Risk Management and Compliance software (GRC) tool, which brings about decreased vulnerability with the state's IT network, and makes evident, immediately any vulnerabilities that do arise. Additionally, it brings us into 98% compliance with STS guidelines.

In terms of the larger, policy picture, this project fits under:

STS strategic priorities

Maturing the STS Risk Management Program is one of STS strategic priorities. - Increase Departmental involvement in disaster recovery and patch management for business applications, and look at areas to further reduce cybersecurity risks within the State.

The State of Tennessee recognizes that it has a vital role in identifying, protecting its citizens from, and responding to cyber threats that may have significant impact to our individual and collective security and privacy.

State Policy: Patch Management (4.5.1.1)

All applications and processing devices that are attached to the State's enterprise technology infrastructure will have critical application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable date can be agreed upon by all affected parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

Impact

From Blissful Ignorance to Excellence

When the VM team first presented detailed scan results for just hundreds (of the thousands) of servers to system administrators and their management, they were completely overwhelmed with the magnitude of the work that needed to be done. There were simply not enough resources to do the work, and it was difficult to coordinate with the agencies. This condition persisted for some months until senior management provided direction to get the systems patched and updated on a quarterly basis, starting within a 90 day time frame.

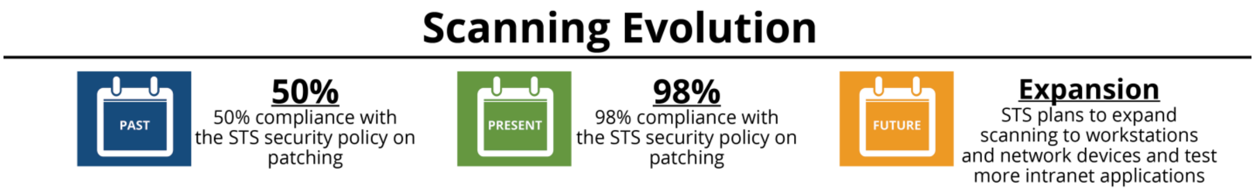
When the first set of full data center scans were tracked, it included approximately 2,000 servers; only 50% of them met our own security patching policy, and the VM team had a hard time determining who was responsible for each server, as well as who was responsible for each finding.

Now STS VM scans approximately 4,000 devices and knows which agency is responsible for each server. STS also knows whether the patch is operating system or application level, and in many cases, which major application resides on these servers in order to know exactly which administrators should be notified of findings. In addition, they are at 98% compliance with the STS security policy on patching.

Delivery/Results Summarized

It took years to perfect network vulnerability scanning with SecurityCenter. Firewalls and network segmentation greatly complicated network scans. Scans also needed administrative privileges. Today the STS VM team oversees fully automated, weekly, credentialed scans of all servers in two data centers plus agency server rooms. Per enterprise security policy, all applications must be tested for security vulnerabilities before they may be given a public IP address. The STS VM team performs most of these assessments at no additional cost to the agencies; consequently the service has been widely adopted.

Network scanning and application testing continually provides opportunities to raise awareness about security among system administrators, software developers and management. As "critical severity" findings diminish in number, administrators and developers will be able to address merely "high severity" issues and even security best practices. In the future, STS plans to expand to scanning workstations and network devices and to test more intranet applications.



Scanning Evolution

50%
50% compliance with the STS security policy on patching

98%
98% compliance with the STS security policy on patching

Expansion
STS plans to expand scanning to workstations and network devices and test more intranet applications

The STS vulnerability management program is a high visibility "win" for security. It has gone a long way toward reducing the "us versus them" mentality that often exists between IT and end users, between security and developers, and between security and operations. The VM team's approach to working with customers on security issues has helped to improve the reputation of security overall and to reduce friction with those affected by findings.

The Return on Investment, or value, of the program is provided in the form of measurably increased security. The cost involved in a data breach is incalculable, including the loss of reputation, and worse yet the compromising of our citizens' personal data. State servers and applications are now much more secure, and far less likely to be compromised.