Compliance Scanning

THE MISSING PIECE OF VULNERABILITY MANAGEMENT

DARRIN MORAN — Director of Services

THE MISSING PIECE OF VULNERABILITY MANAGEMENT:

Compliance Scanning

INTRODUCTION

Designing and deploying a vulnerability management program is essential for businesses in today's highly-interconnected world — but many of these programs are still missing a crucial piece of the puzzle.

When most people think of the scanning functionality within such a vulnerability management program, they visualize an application that scans for and detects exploitable vulnerabilities within systems. For the most part, this vision is correct. However, one vital aspect of vulnerability scanning is considerably more important in today's business climate and often overlooked: compliance scanning.

If you are in healthcare, then you already know the importance of being compliant with regulations like HIPAA and HITRUST. You likely trust your vulnerability management program to ensure that you are adhering to these compliance requirements. But are you getting compliance information with your vulnerability scans? Are you certain that compliance scans are being performed within your infrastructure? Are you sure that any risk to being compliant is identified and known? Do you understand the difference between a vulnerability and compliance scan? If you answered no or "I don't know" to any of these questions, here is your guide to understanding and implementing compliance scanning.

WHY IS COMPLIANCE SCANNING OFTEN OVERLOOKED?

The widespread unfamiliarity with compliance scanning is rooted in two issues regarding vulnerability scanning.

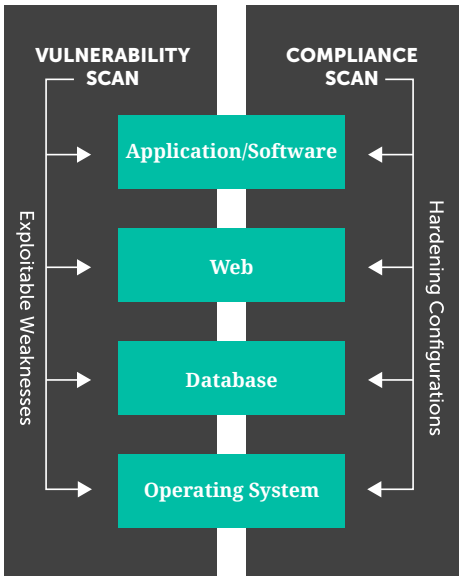
First, many people associate vulnerability scanning with the issues found when scanning a system for weaknesses, which can be exploited by others (i.e. hackers) to circumvent the security of that system. This thinking no doubt stems from the abundance of malware that targets these weaknesses and has plagued the security of computer systems and users for years. While this association is reasonable, it doesn't capture the entire scope of the problem since the definition of vulnerability management encompasses more than the detection of exploitable holes in systems.

Second, security professionals have a tendency to lump all vulnerabilities under one umbrella term (vulnerability) without specifying the type of vulnerability (such as software, personnel, organizational, or compliance). Because of this, many people revert back to the classic definition of vulnerabilities and vulnerability scanning described above. In doing so, their focus on vulnerability scanning becomes extremely narrow and allows for other types of vulnerabilities to slip through the cracks.

Ultimately, these issues affect the overall health of your vulnerability management program. If your program is entirely focused on vulnerability scanning, then a large amount of your security posture information is not being identified or reported. Compliance scanning can help discover and identify this information.

WHAT IS COMPLIANCE SCANNING?

Compliance scanning focuses on the configuration settings (or security hardening) being applied to a system. In short, compliance scans assess adherence to a specific compliance framework.



Hardening consists of applying security guidance from the various compliance frameworks applicable to your company. For example, if your company must comply with HIPAA and/or HITRUST regulations, then your computing systems must be configured (or hardened) to satisfy these regulations. Once applied, the hardening for each system can be verified and/or confirmed via a compliance scan.

When a compliance scan is performed against a single computing system, it produces a report that defines how well the system is hardened against the selected compliance framework. These results contribute to the system's overall security posture. Combining the compliance scan reports/results of all systems helps define the overall security posture of your system and/or infrastructure.

WHAT IS ASSESSED DURING A COMPLIANCE SCAN?

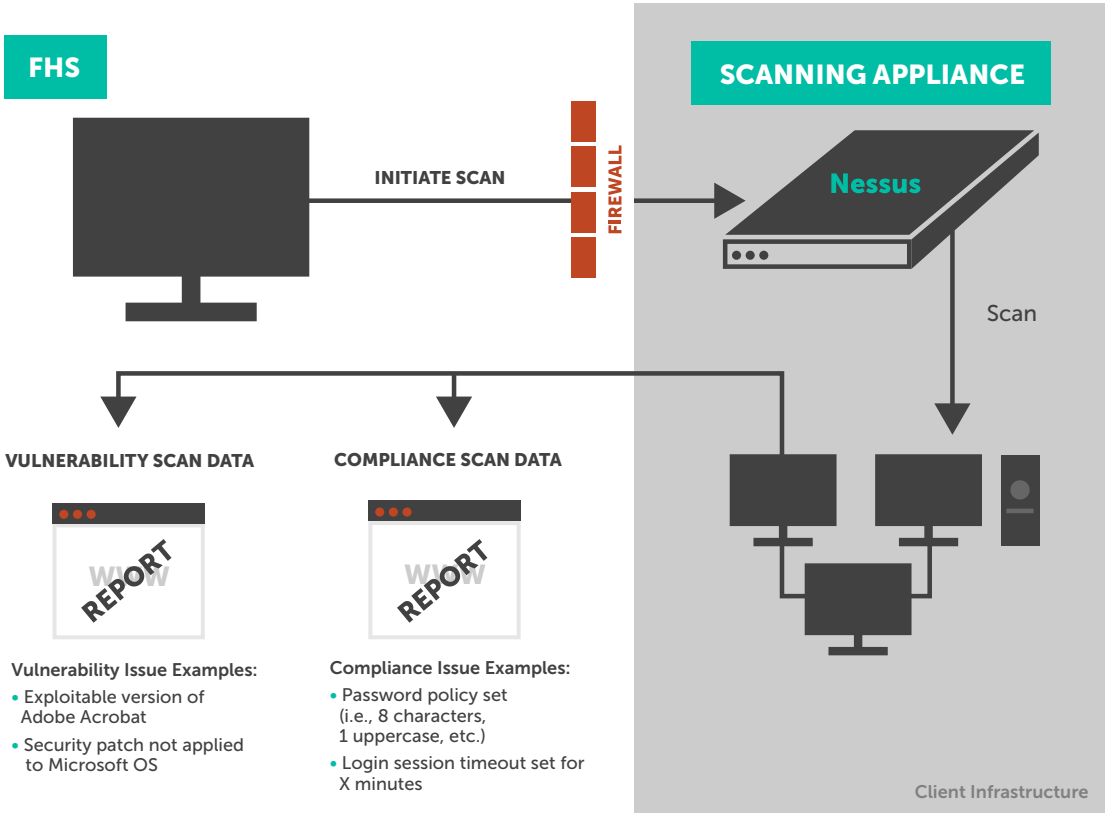
Unlike vulnerability scans, compliance scans are not designed to locate vulnerabilities in software applications or operating systems. Instead, compliance scans are built to locate and assess vulnerabilities in system hardening configurations. Some examples may include:

- Has a password policy has been set (i.e. at least 8 chars, maximum age of 90 days, etc.) on each system?
- Are computing sessions set to automatically lockout (screen lock) after a specified amount of time (i.e. 15 minutes)?
- Have RDP communications been configured for secure communications?
- Is an Apache server configured for SSL?
- Are Oracle default passwords still present in a database?
- Has Internet Explorer been configured to prevent users from adjusting security settings?

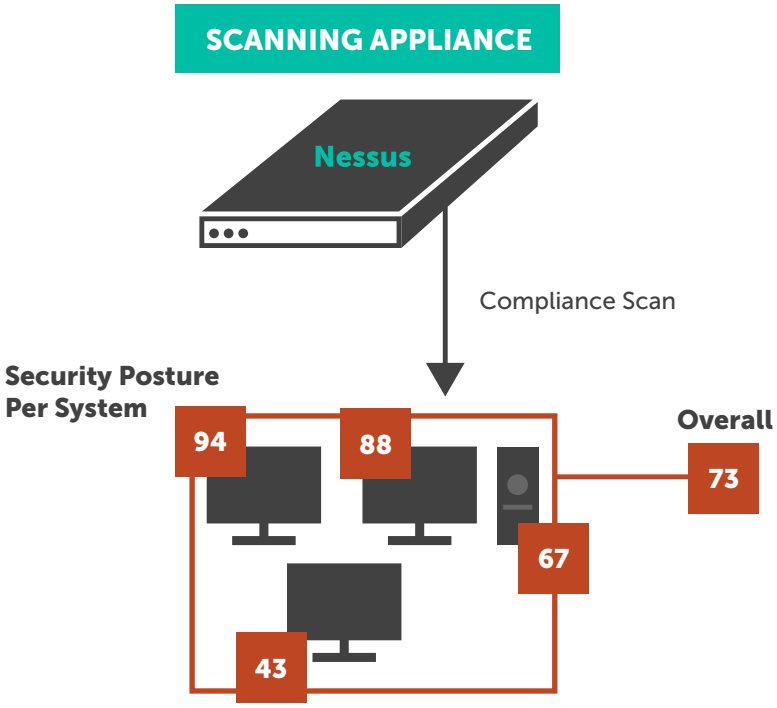
Obviously, these examples represent only a small portion of security hardening guidance from compliance frameworks. A compliance scan will thoroughly assess the complete set of hardening configurations as required by the relevant compliance framework.

HOW CAN FORTIFIED HEALTH SECURITY HELP?

Compliance scanning can be included within the Fortified Health Security's Vulnerability Threat Management (VTM) service. Based upon the compliance needs for your company, Fortified Health Security can supply the input files needed for compliance scanning within the VTM service. Once provided, these files instruct our VTM service to perform a compliance scan of your systems and/or infrastructure.



Upon completion of the compliance scan, a report will be generated for each system scanned. The report will confirm each system's adherence to the selected compliance framework via a percentage (measured against 100% adherence). Combining and averaging the scores of all scan results provides a percentage of compliance adherence for your entire system/infrastructure.



In addition to reporting general adherence to a compliance framework, compliance scanning:

- Provides assurance that compliance regulations are being satisfied
- Identifies gaps in current compliance posture
- Augments internal and/or third-party audits by providing compliance evidence
- Reduces risk of potential fines and/or lawsuits
- Reduces risk to covered entities
- Increases brand recognition and trust among customers and potential covered entities/ business associates

CONCLUSION

Compliance scanning is very different from vulnerability scanning and provides unique and vitally important results. In today's world, compliance with HIPAA and HITRUST is mission critical for any healthcare company because of the valuable information that you are ultimately charged with protecting and the risks associated with being non-compliant. Therefore, in addition to vulnerability scans, business leaders in healthcare would be best served to include compliance scanning as an additional method for determining overall security postures.

CONTACT US TO START ON THE PATH FROM COMPLIANCE TO CONFIDENCE.

For more information, visit our website at:

fortifiedhealthsecurity.com

INQUIRIES

1 (615) 600-4002

sales@fortifiedhealthsecurity.com

OFFICE

2555 Meridian Blvd., Suite 250
Franklin, TN 37067

ABOUT THE AUTHOR

Darrin Moran serves as the Director of Services at Fortified Health Security where his primary focus is delivering and enhancing the world-class managed services Fortified is known for. Drawing on 20 years of security and IT experience in both government and healthcare industries, his background and education as a Virtual Information Security Officer, coupled with deep technical insights, provide Darrin with the unique capability of being able to effectively translate security issues into business solutions.

Prior to joining Fortified, Darrin has served at the Director level for various IT and Security organizations within government and healthcare sectors that comply with such frameworks as FISMA, NIST, ISO, HIPAA, HITRUST and PCI. His work in these areas has provided a wealth of experience, knowledge and business acumen that he applies regularly to increase the security posture of our clients.

Darrin currently holds a Master's Degree in Secure Information Systems from George Mason University, a Bachelor's Degree in Computing Engineering from The Ohio State University, is a Certified Information System Security Professional (CISSP) and HealthCare Information Security and Privacy Practitioner (HCISPP).

ABOUT FORTIFIED HEALTH SECURITY

Fortified Health Security is a leader in information security, compliance and managed services, focused exclusively on helping healthcare professionals overcome operational and regulatory challenges every day in regards to HIPAA, HITECH, and Meaningful Use. Founded in 2009, Fortified has established a heritage of excellence, compliance and innovation. Today, Fortified partners with healthcare organizations across the continuum, serving health systems, single hospital entities, physician practices, post-acute providers, payors and business associates.