Real-Time Auditing for SANS Consensus Audit Guidelines

Leveraging Asset-Based Configuration and Vulnerability Analysis with Real-Time Event Management

January 14, 2010
(Revision 3)

Ron Gula
Chief Technology Officer

Carole Fennelly
Director, Content & Documentation

Table of Contents

Introduction

Tenable Network Security, Inc. was founded on the belief that it is crucial to monitor for compliance in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for compliance violations to occur undetected. Tenable's solutions can be customized for a particular organization's requirements and then automatically provide a unified view of the security status through a single management interface that is continually updated with the latest information.

This paper describes how Tenable's solutions can be leveraged to achieve compliance with the SANS Consensus Audit Guidelines (CAG) by ensuring that key assets are properly configured and monitored for security compliance. The SANS-CAG initiative provides a unified list of 20 critical controls that have been identified through a consensus of federal and private industry security professionals as the most critical security issues seen in the industry. The SANS-CAG team includes officials from the Department of Defense (DOD), Department of Homeland Security (DHS), National Security Agency (NSA), SANS Institute, General Accounting Office (GAO) and the Department of Energy (DOE). According to SANS, fifteen of these controls can be evaluated through automated network scanning and five require manual effort. The SANS controls do not introduce any new security requirements, but organize the requirements into a simplified list to aid in determining compliance and ensure that the most important areas of concern are addressed.

For more information on SANS-CAG, please refer to "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines" at: http://www.sans.org/cag/guidelines.php.

ICE Act of 2009 and SANS-CAG

The National Institute of Standards and Technology (NIST) is responsible for publishing a variety of guides for implementing security controls, performing audits and certifying systems. Some of these guides are very specific, such as recommended settings to harden Windows servers, and others are very generic, such as how to audit change management procedures. Many of these NIST standards have been adopted by auditors as the model for network management. In the U.S. Government, many FISMA audits specifically reference NIST guidelines.

The ICE Act of 2009 calls for a restructuring of federal computer security practices to unify security efforts under a federal "cyber office" that reports directly to the President of the United States. Quoting from the OpenCongress website, the ICE Act is:

> *"A bill to amend chapter 35 of title 44, United States Code, to recognize the interconnected nature of the Internet and agency networks, improve situational awareness of Government cyberspace, enhance information security of the Federal Government, unify policies, procedures, and guidelines for securing information systems and national security systems, establish security standards for Government purchased products and services, and for other purposes."*

This new legislation also calls for revising the FISMA Act of 2002. Currently, there are multiple agencies with a substantial number of specific security control requirements, making compliance extremely difficult and expensive. The SANS-CAG initiative is designed to help the Federal Government prioritize resources and consolidate efforts to reduce costs and ensure that the critical security issues are addressed. The three guiding principles of the SANS-CAG initiative, as listed on their website, are as follows:

- Defenses should focus on addressing the most common and damaging attack activities occurring today, and those anticipated in the near future.
- Defenses should be automated where possible, and periodically or continuously measured using automated measurement techniques where feasible.
- To address current attacks occurring on a frequent basis against numerous organizations, a variety of specific technical activities should be undertaken to produce a more consistent defense.

The twenty critical controls that comprise the SANS-CAG are as follows:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

How Tenable Can Help

Tenable’s Unified Security Monitoring (USM) approach provides a unification of real-time vulnerability monitoring (24x7 discovery through remediation), critical log/event monitoring and custom compliance monitoring capabilities in a single, role-based interface for IT and security users to evaluate, communicate and report the results for effective decision making. The Security Center enables customers to easily measure vulnerabilities and discover security problems, asset by asset. In some cases, the Security Center also helps manage asset discovery. The Security Center correlates all of the information gathered from active and passive scanning with enterprise-wide log data to provide a comprehensive view of system and network activity across the enterprise. A seemingly insignificant event on one system can gain significance when correlated with an event from another source. The Security Center provides a defense-in-depth methodology for security event management.

Tenable solutions map to the SANS-CAG guiding principles in the following manner:

- Active and passive vulnerability scanning using thousands of plugins with new updates on a daily basis.
- Automated scanning and log correlation not only identify vulnerabilities and anomalies, but also new hosts that can be automatically classified into asset lists as they appear on the network.
- The combination of automated active and passive network scanning, credentialed scanning and log correlation provide a variety of technical measures that produce a consistent defense.

Tenable ships the Security Center with several configuration audit policies based on various publications from NIST, FDCC, SCAP, NSA and DISA-STIG. These **`.audit`** files are a generic baseline that can be modified for the organization's specific requirements. In some cases, Tenable has helped customers convert their corporate-wide configuration guides into repeatable audits that can be scheduled to automatically run with the Security Center.

"Appendix A" provides a matrix that lists each SANS-CAG control point, an interpretative summary of the control point and a brief description of how Tenable's solutions apply to the control point.

Standards and Configuration Guides

NIST has also developed reference configuration settings for Windows servers. These have been distributed to the public as Microsoft "**`.inf`**" files that can be used to configure a server more securely.

The Security Center and Nessus have the ability to securely log into Windows and Unix hosts to perform patch and configuration audits. Nessus can be configured to take advantage of the underlying protection mechanisms in SSH and Windows authentication protocols to ensure credentials used in these scans are protected from interception. Tenable has produced audit policies that test specific system profiles, such as:

- Windows 2000, XP, 2003, Vista, 2008 and 7
- Red Hat, Solaris, AIX, HP-UX, Debian, SuSE and FreeBSD
- Oracle, MySQL, MS SQL, DB2, PostgreSQL
- Applications such as IIS, Apache, Nessus and more

Tenable also provides audit files that test against a number of configuration audit policies including but not limited to:

- FDCC and SCAP audits
- DISA STIG audits
- CIS audits for Unix and Windows
- Microsoft vendor recommendations
- PCI configuration settings

Tenable's Solutions

Tenable offers a variety of methods to detect vulnerabilities and security events across the network. Tenable's core technology is also extremely powerful for conducting network compliance audits and communicating the results to many different types of end users.

Core Solution Description

Tenable offers four basic solutions:

- **Security Center** – Tenable’s Security Center provides continuous, asset-based security and compliance monitoring. It unifies the process of asset discovery, vulnerability detection, log analysis, passive network discovery, data leakage detection, event management and configuration auditing for small and large enterprises.

- **Nessus Vulnerability Scanner –** Tenable’s Nessus vulnerability scanner is the world-leader in active scanners, featuring high-speed discovery, asset profiling and vulnerability analysis of the organization’s security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs and across physically separate networks. Nessus is currently rated among the top products of its type throughout the security industry and is endorsed by professional security organizations such as the SANS Institute. Nessus is supported by a world-renowned research team and has an extensive vulnerability knowledge base, making it suitable for even the most complex environments.

- **Log Correlation Engine** – Tenable’s Log Correlation Engine (LCE) is a software module that aggregates, normalizes, correlates and analyzes event log data from the myriad of devices within your infrastructure. The Log Correlation Engine can be used to gather, compress and search logs from any application, network device, system log or other sources. This makes it an excellent tool for forensic log analysis, IT troubleshooting and compliance monitoring. The LCE can work with syslog data, or data collected by dedicated clients for Windows events, Netflow, direct network monitoring and many other technologies.

- **Passive Vulnerability Scanner** – Tenable’s Passive Vulnerability Scanner (PVS) is a network discovery and vulnerability analysis software solution, delivering real-time network profiling and monitoring for continuous assessment of an organization’s security posture in a non-intrusive manner. The Passive Vulnerability Scanner monitors network traffic at the packet layer to determine topology, services and vulnerabilities. Where an active scanner takes a snapshot of the network in time, the PVS behaves like a security motion detector on the network.

In addition, Tenable provides Security Center customers with the **3D Tool** that is designed to facilitate presentations and security analysis of different types of information acquired from the Security Center.

The key features of Tenable’s products as they relate to compliance auditing are as follows:

Asset Centric Analysis

The Security Center can organize network assets into categories through a combination of network scanning, passive network monitoring and integration with existing asset and network management data tools. This enables an auditor to review all components of a particular application.

Typically, an auditor reviews a long list of IP addresses that may have vulnerabilities of various severities associated with them. However, the correlation of interdependencies of an application's components is usually missing. The Security Center provides a complete asset list of applications and ensures that the weakest link in the chain is recognized and taken into account.

For example, consider a typical PeopleSoft deployment for a human resources group. The actual PeopleSoft application may run on one or more Windows servers that interact with several databases. It may be connected over some network switches and possibly have front-end web servers for load-balancing. The entire group of servers comprises the "PeopleSoft" asset. A critical security problem in a supporting switch or database can lead to a compromise just as easily as one in the actual PeopleSoft program. It is very efficient for an auditor to be able to work with all of the security issues for one asset type at a time.

Data Leakage Monitoring

Both Nessus and the Passive Vulnerability Scanner (PVS) can identify sensitive data that may be subject to compliance requirements.

The Nessus scanner can be easily configured to look for common data formats such as credit card numbers and Social Security numbers. It can also be configured to search for documents with unique corporate identifiers such as employee names, project topics and sensitive keywords. Nessus can perform these searches without an agent and only requires credentials to scan a remote computer.

The PVS can monitor network traffic to identify sensitive traffic in motion over email, web and chat activity. It can also identify servers that host office documents on web servers.

The Security Center correlates the information about sensitive data gained from Nessus and the PVS that can be useful in several ways:

- Identifying which assets have sensitive data on them can help determine if data is being hosted on unauthorized systems.
- Classifying assets based on the sensitivity of the data they are hosting can simplify configuration and vulnerability auditing by focusing on those hosts and not the entire network.
- Responding to security incidents or access control violations can be facilitated by knowing the type of information on the target system that helps identify if a system compromise also involves potential theft or modification of data.

Configuration Audits

A configuration audit is one where the auditors verify that servers and devices are configured according to an established standard and maintained with an appropriate procedure. The Security Center can perform configuration audits on key assets through the use of Nessus' local checks that can log directly onto a Unix or Windows server without an agent.

The Security Center ships with several audit standards. Some of these come from best practice centers like the National Institute of Standards and Technology (NIST) and National Security Agency (NSA). Some of these are based on Tenable's interpretation of audit requirements to comply with specific industry standards such as PCI, or legislation such as Sarbanes-Oxley.

In addition to the base audits, it is easy to create customized audits for the particular requirements of any organization. These customized audits can be loaded into the Security Center and made available to anyone performing configuration audits within an organization.

Once the audit policies have been configured in the Security Center, they can be repeatedly used with little effort. The Security Center can also perform audits intended for specific assets. Through the use of audit policies and assets, an auditor can quickly determine the compliance posture for any specified asset.

Security Event Audits

The Security Center and Log Correlation Engine (LCE) can perform the following forms of security event management:

- Secure log aggregation and storage
- Normalization of logs to facilitate analysis
- Correlation of intrusion detection events with known vulnerabilities to identify high-priority attacks
- Sophisticated anomaly and event correlation to look for successful attacks, reconnaissance activity and theft of information

Tenable ships the LCE with logic that can map any number of normalized events to a "compliance" event to support real-time compliance monitoring. For example, a login failure may be benign, but when it occurs on a financial asset, it must be logged at a higher priority. The Security Center and LCE allow any organization to implement their compliance monitoring policy in real-time. These events are also available for reporting and historical records.

The LCE also allows for many forms of best practice and Human Resources (HR) monitoring. For example, unauthorized changes can be detected many different ways through network monitoring. Another useful application of the LCE is to determine if users recently separated from the organization are still accessing the system. All activity can be correlated against user names so that it becomes very easy to see who is doing what on the inside the network.

Web Application Scanning

Tenable's Nessus scanner has a number of plugins that can aid in web application scanning. This functionality is useful to get an overall picture of the organization's posture before engaging in an exhaustive (and expensive) analysis of the web applications in the environment. Nessus plugins test for common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion and command execution.

Another useful Nessus option is the ability to enable or disable testing of embedded web servers that may be adversely affected when scanned. Many embedded web servers are static and cannot be configured with custom CGI applications. Nessus provides the ability to test these separately to save time and avoid loss of availability of embedded servers.

Nessus provides the ability for the user to adjust how Nessus tests each CGI script and determine the duration of the tests. For example, tests can be configured to stop as soon as a flaw is found or to look for all flaws. This helps to quickly determine if the site will fail compliance without performing the more exhaustive and time-consuming Nessus tests. This “low hanging fruit” approach helps organizations to quickly determine if they have issues that must be addressed before the more intensive tests are run.

Nessus also provides special features for web mirroring, allowing the user to specify which part of the web site will be crawled or excluded. The duration of the crawl process can be limited as well.

Appendix A: Tenable and SANS-CAG Controls

The following table provides a summary interpretation of the SANS-CAG control and a brief description of how Tenable's solutions address this area. Each interpretation is also mapped to the corresponding NIST SP 800-53 Revision 3 Priority 1 Controls as provided by SANS.

The following acronyms are used:

- SC – Security Center
- LCE – Log Correlation Engine
- PVS – Passive Vulnerability Scanner

Critical Controls Subject to Automated Collection, Measurement and Validation:

1. Inventory of Authorized and Unauthorized Devices	
Interpretation	Many security vulnerabilities are introduced by new devices gaining access to the network. It is important to have an accurate inventory of all devices on the network to ensure that they are patched and hardened in compliance with the organization's policy. **NIST SP 800-53 Rev 3 Priority 1 Controls:** CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6
Tenable Solution	The SC's asset discovery capabilities leverage both active and passive detection via Nessus and the PVS to help maintain an up-to-date network list. This includes the ability to determine when new devices have been added to the network, what their operating system or device type is, the topology of the network and what types of services these devices are running. For Linux and Windows operating systems, Nessus can leverage information about running processes, known vulnerabilities, configuration information, WMI data, system BIOS data and more to classify systems into one or more different asset groups. The SC can also be used to determine authorized or unauthorized devices in several different ways: • Any type of detected change can be audited. New hosts, new services and software can all be identified through the SC. The SC allows inspection of any vulnerability, service or node for when it was first seen or last seen. The PVS allows for real-time alerting of new hosts and finally, for any scan controlled by SC, an automatic list of "new" hosts is automatically discovered. • The SC has a sophisticated method for classifying hosts. For example, corporations that leverage DNS names for authorized devices can use the SC to identify nodes that do not have an official DNS record. The SC can use

	combinations of the output of any active or passive scan to classify hosts in accordance with various types of "authorized" and "unauthorized" device lists. • The SC can also leverage automatic classification of hosts based on complex rules that reflect deviations from policy. For example, you could identify all Linux computers in a "Windows Only" type of environment. Another example would be to identify hosts in a DMZ that have open ports against a known policy. These types of policy violations are often related to "unauthorized" devices.
2. Inventory of Authorized and Unauthorized Software	
Interpretation	New vulnerabilities in applications and operating systems are discovered on a daily basis. It is important to determine what software versions are running on the network to ensure that any reported vulnerabilities are addressed promptly. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7
Tenable Solution	Software can be discovered multiple ways: • Direct network scanning of running services such as the identification of a web server running IIS 4.0. • Credentialed auditing of Windows and Unix hosts to enumerate software installed in the operating system and user directories as well as modified operating system software such as manually compiled Unix daemons. • Log analysis of process accounting on Unix and process auditing on Windows can identify all executables run by specific users. • The PVS can passively observe network traffic to identify the majority of client software used to communicate on the network as well as the ability to infer the presence of installed software such as VMware or iTunes by monitoring "self update" traffic. The combination of these techniques allows for a flexible and comprehensive method to enumerate all of the software in use on your network by specific asset groups or by particular users. This information can assist in developing lists of "black listed" software to be monitored for, as well as "white listed" software that is approved.
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	
Interpretation	Configuration standards for desktops, laptops and servers must be established to provide consistency throughout the organization. For example, the Center for Internet Security (CIS) has benchmarks that provide consensus guidelines for securing a number of applications

	and OS platforms. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
Tenable Solution	Tenable's products can help detect and measure violations to an established desktop and server configuration management policy. The SC can be used to assess specific asset classes of servers or desktops with specific configuration audits. Audits are available to be performed against: • Windows 2000, XP, 2003, Vista, 2008 and 7 • Red Hat, Solaris, AIX, HP-UX, Debian, SuSE and FreeBSD • Oracle, MySQL, MS SQL, DB2, PostgreSQL • Applications such as IIS, Apache, Nessus and more Tenable's list of pre-configured configuration audit policies include but are not limited to: • FDCC and SCAP audits • DISA STIG audits • CIS audits for Unix and Windows • Microsoft vendor recommendations • PCI configuration settings Real-time network analysis as well as repetitive active scanning can discover new hosts that need to be audited. Audits are performed entirely with credentials and do not require the use of an agent.
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	
Interpretation	Configuration standards for network devices must be established to provide consistency throughout the organization. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AC-4 (7, 10, 11, 16), CM-1, CM-2 (1), CM-3 (2), CM-5 (1, 2, 5), CM-6 (4), CM-7 (1, 3), IA-2 (1, 6), IA-5, IA-8, RA-5, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18), SC-9
Tenable Solution	Tenable's products can help detect and measure violations to an established network device and firewall configuration management policy. Specifically, Tenable solutions can be used to: • Scan networks or specific assets for a list of open ports. This can be used to test against a known access control policy. • Scan for excessive trust relationships. Multiple Nessus

	scanners can be placed throughout the network to perform scans from different vantage points. For example, this can test how much access a DMZ has to a developer network or vice verse. • Passively and continuously monitor both services and client activity. When managed by the SC, it is very easy to analyze which ports are being served or browsed from which asset groups or hosts. This can highlight issues such as which servers in the DMZ communicate on IRC, or even connect to the Internet outbound at all. • Through log analysis, any type of change indicated in a router, firewall or switch log can be normalized. This can easily be reported on and filtered by time, asset group or user. With full log search, any type of audit trail generated by any network device can also be gathered, searched and analyzed.
5. Boundary Defense	
Interpretation	Log and monitor all traffic that traverses between the internal network and the Internet to detect signs of external attacks or unauthorized data flows. Implement filtering to ensure that IP traffic is legitimate. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AC-17 (1), AC-20, CA-3, IA-2 (1, 2), IA-8, RA-5, SC-7 (1, 2, 3, 8, 10, 11, 14), SC-18, SI-4 (c, 1, 4, 5, 11), PM-7
Tenable Solution	Tenable's LCE has two different agents that can log all network traffic thought direct "sniffing" or receive NetFlow information from one or more devices. Logs from network sessions include start and stop time, the IPs and ports involved and the amount of client or server bandwidth collected. This information collected by the LCE is further analyzed with the following methods: • All network connections are labeled by duration and bandwidth. This makes it very easy to look for long TCP sessions as well as sessions that transfer large amounts of data. • Each host on the network is statistically profiled such that if there is a change in "normal" traffic, the deviation is noted. For example, if a server had an increase in inbound network connections, a log stating this would be noted. With the SC, it is very easy to sort, view and analyze this information to decide if this sort of anomaly is worth investigating. • Each flow is fed into a variety of correlation scripts that look for worm behavior, network scanning, and correlate attacks detected by a NIDS and with known "blacklisted" IP addresses and a variety of other threat monitoring rules. The LCE also can use firewall, web proxy and router ACL logs to understand when network communications occur.

6. Maintenance, Monitoring, and Analysis of Security Audit Logs	
Interpretation	Systems, applications and network devices must be configured to log relevant activity that includes source, destination, user name (if applicable) and validated time/date stamp. Multiple log sources must be available to corroborate information that may have been altered at the source. Logs must be stored on a central server that is separate from the system that is originally generating the logs. Log data must be maintained in a manner to protect it from intentional or unintentional loss or alteration. Logs from multiple systems must be aggregated and correlated for analysis with network scanning results. Storage allocation for log data must be monitored for resource exhaustion. A mechanism must be in place to determine the status of logging activity. Log data must be protected from unauthorized access. Log data must be maintained in an archive for a specified time period in accordance with the organization's policy. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)
Tenable Solution	Tenable's LCE provides the ability to normalize multiple log types from a variety of devices, including NetFlow data, firewall logs, operating system logs, process accounting, user maintenance and even honeypot logs. This can help build a better picture of what has occurred during an event where some logs could be forged at the source. The LCE can store, compress and search any type of ASCII log that is sent to it for correlated events of interest or to detect anomalies. The LCE has the ability to import syslog data from multiple sources in order to analyze data from past change-control events and can also accept logs from Tripwire and correlate these events with suspicious events and IDS attacks. Tenable also ships a wide variety of configuration audit policies that can be used to ensure that the sources of log data are correctly configured to send their logs. Audits currently available include: • Detection of all Windows GPO and local policy settings that refer to event logging such as audit of process creation. • Support for all types of Unix platforms to ensure that syslog is enabled and logging correctly. • The ability to audit the LCE client that is installed at the host that is generating logs. The LCE can be configured to log access control changes on specific servers and can monitor file MD5 checksums in real-time to detect modifications made during a change-control process. All events arriving at the LCE are uniquely time-stamped. The LCE retains the entire log record and provides a number of filters and analysis tools to simplify log analysis and generate concise reports. Searches can be made with Boolean logic and limited to specific date ranges. There are an infinite number of searches that can be performed, such as

	searching DNS query records or tracking down known Ethernet (MAC) addresses in switches, DHCP and other types of logs. The full log search capability in the SC and LCE provides the ability to quickly summarize events across the entire enterprise. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. Previous searches can also be re-launched against the latest log data. The LCE can be configured to alert administrators when a hard disk is nearing capacity. Agents used by the LCE also report CPU, memory and disk utilization. The SC also maintains a real-time status of all LCE servers and their clients.
7. Application Software Security	
Interpretation	Application software that is developed in-house must be developed in a manner to limit the possibility of vulnerabilities created from programming errors that have been identified as common causes of security exposures. Third party libraries or other software that are used in the development process must be scanned to ensure they do not contain known vulnerabilities. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10
Tenable Solution	Tenable's ability to audit custom web applications is built on several key functions: • Nessus can be used to audit the underlying operating system for any vulnerability in the OS, application or database. • Nessus can be used to audit the configuration of the operating system, application and database. • Nessus can perform a variety of web application audits to test for common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion and command execution. • Nessus has the ability to send POST requests in addition to GET requests, which enables testing of HTML forms for vulnerabilities. • Nessus has the ability to enable or disable testing of embedded web servers that may be adversely affected when scanned. • Nessus scans can be configured to stop as soon as a flaw is found or to look for all flaws. This helps to quickly determine if issues need to be addressed before running exhaustive scans. • Nessus provides special features for web mirroring, allowing the user to specify which part of the web site will be crawled or excluded. • On a production system, the PVS can monitor network traffic to look for evidence of SQL injection issues and other types of

	web application errors. • The LCE can make use of web and database logs to look for web application probes and testing. Nessus also has the ability to audit the content of specific files. If an issue with a customer web application system is discovered, it can easily be scanned without the need to program a new check in Nessus. For non-web based applications, Nessus already performs a wide variety of third party library audits for vulnerabilities. Libraries tested include .Net, Java, PHP and Adobe AIR.
8. Controlled Use of Administrative Privileges	
Interpretation	Administrative privileges are necessary to support the IT infrastructure but it is important to ensure that such privileges are protected from unauthorized use, limited in scope and that activities are logged and can be traced to a particular user. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)
Tenable Solution	Tenable’s LCE normalizes all logins and login failures from a wide variety of devices. Through normalization, the LCE has the ability to understand many different ways an enterprise can experience a login failure from regular operating systems like Linux and Windows as well as network devices such as a Checkpoint Firewall. The ability to see all logins and login failures in one report makes it very easy to understand and audit what types of access have been granted and which users are accessing which resources. In addition to logins and login failures, the LCE can be configured to automatically learn which users use which IP addresses. For many different types of login and authentication events, the username and source IP address is known. The LCE can associate this information such that other logs that do not have a username in them can still be associated with a user. This means that an LCE can associate NetFlow, NIDS, firewall and many other types of logs with a user. This also facilitates reporting on a user’s activities across the entire range of logs gathered. Finally, Nessus can be used to audit the configuration of Unix and Windows systems to make sure that they have been locked down to prevent non-administrators from being able to access data and settings for which they do not have authorization. Tenable’s audit policies for FDCC, CIS, PCI and DISA include a variety of user account auditing settings for both administrators and end users that ensure access is limited.
9. Controlled Access Based on Need to Know	

Interpretation	Data must be classified in a manner to identify the sensitivity of the data, such as public information, internal use only, client confidential data or personal information (including patient health information, credit card data and Social Security numbers). Once data has been classified it must be stored in a manner in accordance with the sensitivity of the data. For example, highly sensitive data such as patient health information may not be stored on systems in the DMZ. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6, MP-3, RA-2 (a)
Tenable Solution	Tenable's solutions enable testing of servers to ensure they are configured with the proper level of access control, including separation of duties for default and new accounts and configurations of servers to ensure they have been locked down to a least level of privilege. For example, a running daemon or service on a server can be tested to see which user level it is operating against. Tenable's PVS passively monitors network data flows and can be configured to monitor for a number of specific data types (e.g., credit card data, patient health information, etc.) across specified network segments. Nessus and the PVS can be used to identify a wide variety of applications that offer data without requiring a unique user login. For example, Nessus can identify which systems are publishing PDF files over web pages that do not require a login. Similarly, the PVS can identify anonymous FTP servers hosting content.
10.Continuous Vulnerability Assessment and Remediation	
Interpretation	It is important to monitor systems for vulnerabilities in as close to real-time as possible. Penetration tests can discover vulnerabilities in the IT infrastructure, but they are only a snapshot in time. A system that is scanned one day and found to be free of vulnerabilities may be completely exploitable the next day. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)
Tenable Solution	Tenable was founded on the belief that it is crucial to monitor systems in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for vulnerabilities to be undetected. To achieve this goal, Tenable offers several technologies that can be leveraged: • Nessus can perform rapid network scans. A typical vulnerability scan can take just a few minutes. With the SC, multiple Nessus scanners can be combined to perform load balanced network scans. • Nessus credential scans can be leveraged to perform highly

	accurate and rapid configuration and vulnerability audits. Credentialed scans also enumerate all UDP and TCP ports in just a few seconds. • The PVS monitors all network traffic in real-time to find new hosts, new vulnerabilities and new applications. It scans for the same vulnerabilities detected by the Nessus scanner.
11.Account Monitoring and Control	
Interpretation	It is common for attackers to exploit inactive or default accounts on systems to gain access to the network. Organizations must have a process to monitor systems for inactive, suspended, terminated or default accounts and ensure access is blocked for these accounts. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AC-2 (e, f, g, h, j, 2, 3, 4, 5), AC-3
Tenable Solution	Tenable’s solutions can audit the access control policies in use for any type of system, application or network access control and test for the presence of inactive, suspended, terminated or default accounts to determine if they have been disabled. The presence of the account through network and/or log analysis can also be detected. Tenable’s products can also detect changes to network access control policies through the use of repeated network scans, passive network monitoring and log analysis. For organizations that do not have a very good understanding of which user accounts are valid or invalid, the LCE will automatically learn which user accounts are active on each system. This information can then be used to further refine Nessus configuration audits to look for invalid or inactive user accounts.
12.Malware Defenses	
Interpretation	Appropriate measures must be in place to ensure that systems are protected from malware such as viruses and Trojan software. Anti-virus solutions must be deployed and automatically updated on all systems that are vulnerable to virus attacks. Systems must be configured to automatically scan downloaded software for viruses before opening it. Systems must be scanned for configuration and patch level compliance before being granted access to the network. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)
Tenable Solution	Tenable has several technologies to audit your organization’s anti-malware defenses. These include the ability to: • Audit your desktop and server configurations to make sure basic hardening has been put in place to limit the chance of a virus compromise.

	• Detect systems that have no anti-virus software installed. • Detect systems that have anti-virus software installed, but their signatures are out of date or the service is not running. • Detect systems that do not have an authorized enterprise anti-virus configuration. Tenable offers configuration auditing policies for many anti-virus solutions including CA, Symantec, Trend Micro, McAfee, Sophos and more. Tenable can also help monitor your network for malware activity. This includes the ability to: • Aggregate logs from anti-virus products with email filtering, network IDS and SPAM filtering products. By aggregating these logs together, analysts can visibly observe spikes in email SPAM/malware activity followed by smaller spikes in actual detected viruses at the host. • Detect and analyze virus outbreaks through the LCE's ability to correlate NetFlow, NIDS events, blacklisted IP address activity and other types of anomaly detection. • Use Nessus to scan for specific types of known viruses such as Conficker, listening services that were unknown to the operating system as well as generic "backdoor" fingerprints such as executables being served on any port.
13.Limitation and Control of Network Ports, Protocols, and Services	
Interpretation	The best defense against an exploit is for the targeted service or application to not be running. This is not always practical, but it is important to ensure that the only services that are running are those that are required for the particular system and that all others are turned off. The CIS benchmarks provide hardening guides for a wide variety of operating systems and applications to help determine which services can be safely disabled. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)
Tenable Solution	Tenable's products can help detect and measure violations to an established configuration management policy. This can include specification of running network services as well as specific configuration settings for an operating system or application. The SC can be used to assess specific asset classes of servers or network devices with specific audits. Similarly, real-time network analysis can discover new hosts as well as hosts operating outside of configuration guidelines. SC and Nessus are certified to perform FDCC and Center for Internet Security (CIS) audits. The SC makes it easy to detect any host within an asset class that is not configured correctly. This could indicate an open port, an

	incorrect registry setting, missing patches and so on. Additionally, when using data from the PVS and LCE, an analyst can determine if a server has a port open, but has no traffic actually going to it. This is an excellent way to look for services that are enabled, but are not actually being used.
14.Wireless Device Control	
Interpretation	Wireless networking provides a great convenience for users but also introduces a wide range of security issues. Organizations must ensure that wireless networks are authorized and configured in accordance with the site’s security standards. Systems that are not intended to connect to a wireless network must have the ability disabled. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)
Tenable Solution	Tenable’s solutions can detect all wireless devices that are connected to the network. • Nessus can identify a great deal of wireless access point devices. • The PVS can identify devices that perform network address translation (NAT) services. • The LCE can identify wireless devices though log analysis. For example, if any Ethernet addresses are logged from a sniffer, switch, firewall or NIDS, the LCE will automatically generate an alert if this is a new address and also indicate the manufacturer of the wireless device. In addition, Nessus can perform a variety of audits through credentialed scanning: • Nessus can report the wireless SSID that can be used for auditing if one or more wireless networks are indeed active. • Nessus can audit end nodes for the presence of authorized and unauthorized wireless network interfaces. • Nessus can review system configurations to ensure that wireless capability is disabled on systems that are not intended to be used on a wireless network.
15.Data Loss Prevention	
Interpretation	The public exposure of sensitive information, as can be seen on the DataLossDB site (http://datalossdb.org/), has caused Data Loss Prevention (DLP) to be a growing concern in IT. It is critical to ensure that data is classified and handled in a manner appropriate for the sensitivity of the data. Highly sensitive data, such as patient health information, credit card data and Social Security numbers must be protected.

	Associated NIST SP 800-53 Rev 3 Priority 1 Controls: AC-4, MP-2 (2), MP-4 (1), SC-7 (6, 10), SC-9, SC-13, SC-28 (1), SI-4 (4, 11), PM-7
Tenable Solution	Tenable's solutions assist in the mitigation of data loss in several strategic areas: • During an actual incident, the situational awareness delivered by Tenable's solutions allows for quick determination of the scope. This can assist an organization to quickly determine what has been and has not been compromised. Knowing this type of information can help an organization to more accurately report what has been compromised. • Prior to an incident, Tenable's solutions help monitor as much of the network as possible against a known policy to minimize the chance of an incident occurring. Specifically, Tenable also offers some tactical technologies that can help lock down data in motion and data at rest for any organization: • Nessus can list all devices that have had a USB device connected to them and also identify what the devices are. • The LCE can monitor multiple Windows servers for real-time USB device usage. • Both Nessus and the PVS can monitor a network and identify which servers and services share documents such as spreadsheets or PDFs. • Nessus has the ability to audit SQL databases to ensure they have been hardened to prevent attacks (such as SQL injection) from obtaining data from ad hoc queries. • The LCE's ability to track user activity can be used to quickly audit many different types of access to servers that house sensitive data. • Both Nessus and the PVS can be used to audit documents at rest and in motion that contain specific patterns such as credit card numbers, Social Security numbers and other types of sensitive data.

Additional Critical Controls (not directly supported by automated measurement and validation):

16.Secure Network Engineering	
Interpretation	A secure network design is critical to ensure that attackers cannot exploit superfluous network connections, weak filtering and poor network segregation. DHCP lease information needs to be standardized and logged. The network must be designed in a manner to compartmentalize attacks to limit penetration. Only authorized DNS servers may be deployed and must be configured to protect against DNS spoofing attacks.

Associated NIST SP 800-53 Rev 3 Priority 1 Controls:
IR-4 (2), SA-8, SC-7 (1, 13), SC-20, SC-21, SC-22, PM-7

Tenable Solution

Multiple Nessus scans can test to see if certain parts of the network have excessive trust relationships with other parts. This allows Nessus scanners associated with one department, physical location or data center to scan the network of another group. At a minimum, Nessus scanners placed outside a network can get an "outsiders" view of what is being exposed, even if this is still within the corporate network.

Nessus, the LCE and the PVS can also be used to look for network issues such as:

- Unauthorized DHCP servers
- End user systems sending SMTP messages directly to the Internet
- Protocols that can tunnel connections such as Tor, Teredo and other types of proxies
- Identification of nodes that are running on a virtual environment such as VMware
- Security issues with DNS and BGP
- Unauthorized (or unknown) router, firewall or switch deployment
- Unauthorized use of network scanners or penetration tools

17.Penetration Tests and Red Team Exercises

Interpretation

Penetration tests simulate the actions of an attacker by analyzing information gathered about the network to determine potential weaknesses that may be unique to that particular network. Penetration tests are intended to bring human insight into vulnerability analysis in order to detect potential problems that an automated scan may not detect.

Associated NIST SP 800-53 Rev 3 Priority 1 Controls:
CA-2 (1, 2), CA-7 (1, 2), RA-3, RA-5 (4, 9), SA-12 (7)

Tenable Solution

Penetration tests help identify vulnerabilities and also test the response system of the security team.

To facilitate a penetration test, Tenable solutions can help identify a wide variety of data that can be used to further refine a penetration test. This includes:

- A list of all externally facing servers or targets that can be used as a target for a penetration test. This could also include a list of vulnerabilities or missing patches.
- The PVS can also provide a list of all computers that communicate with certain servers. This can help a penetration testing team select targets that are of high value.

- Both the PVS and Nessus can be used to indicate which servers have sensitive data or run SQL databases.

During the test, if the penetration testing team recovers credentials such as password, NTLM hashes or SSH keys, they can use Nessus to perform a configuration audit, patch audit and full vulnerability scan. This can make your penetration test more insightful as it can point out deficiencies in following corporate patching and configuration guidelines.

Finally, regardless of the type of penetration test (e.g., malicious insider, web application test, etc.), Tenable's unified approach to combining log analysis, anomaly detection and system analysis can help detect any type of breach. If a breach does occur, it will likely point out log and monitoring sources that are not currently being collected. For example, an organization may have NetFlow, NIDS and firewall logs protecting a DMZ, but these logs would have no indication of a successful web application attack. However, if those logs were sent to the LCE, a wide variety of web application attacks could be detected.

18.Incident Response Capability

Interpretation

A documented and tested incident response plan is necessary to ensure the prompt detection, identification, mitigation and analysis of all security incidents.

Associated NIST SP 800-53 Rev 3 Priority 1 Controls:
IR-1, IR-2 (1), IR-4, IR-5, IR-6 (a), IR-8

Tenable Solution

Tenable's solutions provide tools that can aid in the incident response process in two strategic areas. These are:

- Detecting the incident
- Responding quickly to an incident

The ability to detect an incident efficiently and in an automated manner is often overlooked. Most automation for detecting incidents generates many false positives that make it unreliable. Tenable's approach is to correlate many types of data along with known system configuration and vulnerabilities.

When an incident is reported externally (e.g., through a help desk phone call), having all network activity, system logs, configuration data and firewall logs at an analyst's fingertips can help them quickly categorize the type of incident they are dealing with. When an analyst detects a potential compromise, abuse or other type of anomaly with Tenable's products, they also have enough information to make a determination to start an incident response exercise.

The ability to respond to an incident correctly and quickly is key to limiting and remediating any exposure from an incident.

19.Data Recovery Capability	
Interpretation	Very often organizations that have had a security breach restore systems only to be subjected to repeat attacks. It is common practice for an attacker to install malware such as backdoors, Trojans and spyware to provide alternative access if the initial vulnerability is closed. It is important to ensure that a data backup program is in place that backs up all data on a weekly basis, encrypts backup data and stores backups in a physically secure location. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** CP-9 (a, b, d, 1, 3), CP-10 (6)
Tenable Solution	Nessus credentialed scans can be used to ensure that systems are configured to backup data on a weekly basis. The SC can be used to identify systems that do not have certain backup software installed or configured correctly. The actual backup process can also be monitored with the LCE through the use of program audits or even traffic analysis.
20.Security Skills Assessment and Appropriate Training to Fill Gaps	
Interpretation	Security awareness programs help educate end users, developers, administrators and managers of security issues particular to their job function. Periodic assessment quizzes help determine the effectiveness of the program. **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:** AT-1, AT-2 (1), AT-3 (1)
Tenable Solution	The SC includes trending and reporting tools that can help demonstrate the types of security deficiencies that can be fed back into the security awareness program. For example, if an organization was struggling with the requirement to apply patches within 30 days of release, then more training could be conducted about the importance of this, the risk to the organization and why the corporate policy addresses this issue. A different organization might be patching systems efficiently, but could also have a higher frequency of virus outbreaks that could indicate that more user training is in order. Tenable also offers a variety of training and certification programs for Nessus and all of our enterprise products. These certification programs can be used to ensure that your security team has the right set of training and skills to operate the Tenable products. Finally, Tenable produces a wide variety of content for our customers to help drive any type of security awareness and training program. These include: • An active corporate blog with more than 300 technical and

	strategic posts that focus on scanning, security auditing, log analysis, insider threat detection and more. • A user discussion portal that allows Tenable’s customers to exchange ideas, tools, strategies and questions with each other. • A support portal that includes many knowledgebase articles on achieving certain types of capabilities with Tenable’s products. • A wide variety of recorded webinars about specific product features and high level security concepts such as compliance auditing and log analysis.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenablesecurity.com/.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenablesecurity.com/