TENABLE Network Security®

Application Note: FDCC Compliance

Measure, Monitor and Report FDCC Compliance

Tenable's Security Center is a NIST SCAP Validated Tool for Windows XP and Windows Vista

Introduction

Realizing that regulatory and policy compliance is an ongoing process, IT organizations should focus their efforts on finding the right risk management program that provides the standards and best practices to make the process repeatable. Companies need to focus on managing and implementing controls to meet and manage regulations and risk management programs.

Federal Desktop Core Configuration Initiative (FDCC)

The U.S. Office of Management and Budget has required, in the July 31st, 2007 memorandum to Federal CIOs, that "Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations."

Security Content Automation Protocol (SCAP) Validation Program

SCAP validation focuses on evaluating specific versions of vendor products based on the platforms they support. Validations are awarded on a platform-by-platform basis for the version of the product that was validated. Currently, US government SCAP content is primarily focused on Windows operating systems.

XCCDF security benchmark automation

TENABLE and FDCC

The Federal Desktop Core Configuration (FDCC) mandate requires all U.S. government agencies and their contractors to meet or exceed FDCC standards for desktops and laptops running Microsoft Windows XP or Windows Vista. The FDCC standard makes use of the NIST XCCDF standard to specify required system configurations settings.

Tenable's Security Center and Nessus Vulnerability Scanner are recognized by NIST as Security Content Automation Protocol (SCAP) compliant tools. The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement and policy compliance evaluation (e.g., FISMA compliance). Federal departments and agencies can use Tenable's Security Center and Nessus to verify configurations before deployment and then to monitor compliance with FDCC mandated configurations on an ongoing basis.

Tenable Specific SCAP Validations:

FDCC Scanner: Tenable's Security Center has the ability to audit and asses a target system in order to determine its compliance with the Federal Desktop Core Configuration (FDCC) requirements. A typical FDCC audit lasts less than 1 minute and does not require an agent. The Security Center can schedule scans of thousands of desktops and help produce FDCC reports for submission to NIST.

Authenticated Configuration Scanner: Tenable's Security Center has the ability to audit and assess a target system to determine its compliance with a defined set of configuration requirements using target system logon privileges. The FDCC Scanner capability is an expanded use case of this capability. The Security Center can make use of other types of content that has been developed against the XCCDF specification. Content is currently available that tests servers against NSA and DISA best practices.

Authenticated Vulnerability and Patch Scanner: Tenable's Security Center has the ability to scan a target system to locate and identify the presence of known software flaws and evaluate the software patch status to determine compliance with a defined patch policy using target system logon privileges.

Unauthenticated Vulnerability Scanner: Tenable's Security Center has the ability to determine the presence of known software flaws by evaluating the target system over the network.

TENABLE FDCC Case Study

A US government Tenable customer required the ability to monitor the configuration of more than 30,000 Windows operating systems deployed world-wide.

Separate base configurations were developed from NIST's SCAP program to audit settings for Windows XP Pro, Windows 2000 and Windows 2003. More than 20 Nessus scanners were deployed and are managed by the Security Center to conduct vulnerability, patch and configuration audits during one weekly distributed scan.

The results from the scanning are centralized with the Security Center such that each asset, unique vulnerability or unique configuration item can be consumed securely and efficiently by executives, IT managers and auditors.

Tenable's Solutions

From a network security feature set, Tenable offers a variety of ways to detect vulnerabilities and security events. As such, our core technology is also extremely powerful for conducting network compliance audits and communicating the results to many different consumers. Tenable offers four fully integrated components:

Security Center – The Tenable Security Center is a web based management console that unifies the process of asset discovery, vulnerability detection, event management and compliance reporting. The Security Center enables efficient communications of security information to IT, management and audit teams.

Nessus Vulnerability Scanner – The Nessus Vulnerability Scanner is an active scanner that provides a snapshot of network assets, their vulnerability exposure, their compliance with standard configuration policies and determines if they contain sensitive data.

Passive Vulnerability Scanner – The Passive Vulnerability Scanner behaves like a security motion detector on the network. It maps new hosts and services as they appear on the network and monitors for vulnerabilities. File sharing, PII data in motion, encrypted communications, trust relationships and servers sharing content are also identified.

Log Correlation Engine – The Log Correlation Engine correlates and analyzes event log data from raw network traffic, system logs and user activity. The Log Correlation Engine is designed to work in conjunction with the Security Center to provide a central portal for security management.

Broader FISMA Application

The E-Government Act, passed into law in December, 2002, recognized that information security is essential to protect the nation's economic and national security interests. Title III of the E-Government Act, the Federal Information Security Management Act, requires United States government agencies to develop, document, and implement programs to protect the confidentiality, integrity and availability of IT systems.

The consensus among Tenable's customer base is that FISMA audits are primarily about describing methods used to protect data. The Security Center streamlines this process by enabling federal customers to easily measure vulnerabilities and discover security problems, asset by asset.

Specifically, Tenable also ships the Security Center with several configuration audit policies based on various publications from NIST, the NSA and Tenable's interpretation of typical FISMA audit questions. In some cases, Tenable has also helped customers convert their agency-wide configuration guides into repeatable audits that can be scheduled with the Security Center.

TENABLE Network Security, Inc.
7063 Columbia Gateway Dr.
Suite 100
Columbia, MD 21046
TEL: 1-410-872-0555

Tenable's Certification with NIST

Tenable's Security Center is validated by NIST as Security Content Automation Protocol (SCAP) compliant tool. The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement and policy compliance evaluation (e.g., FISMA compliance).

Specific Tenable SCAP Capability validations by NIST:
http://nvd.nist.gov/validation_tenable.cfm
Validation date: April 11, 2008

FDCC Scanner
Authenticated Configuration Scanner
Authenticated Vulnerability and Patch Scanner
Unauthenticated Vulnerability Scanner

Federal departments and agencies can use Tenable's Security Center and Nessus to verify configurations before deployment and then to monitor compliance with FDCC mandated configurations on an ongoing basis.

Benefits of the TENABLE Solution

Scan systems for FDCC compliance at the same time as a vulnerability scan

Get reports on compliance success tests, as well as compliance exceptions

Management reports based on security standards and best practices

Workflow for remediation tracking

Start your evaluation today!

Tenable works in conjunction with industry leading partners to provide Government agencies with a wide array of Federal contracts and vehicles to purchase Tenable products.

Contact our Federal Sales Organization to start your evaluation today by emailing sales@tenablesecurity.com.

Real-Time Compliance Monitoring
101 Pages, November 2008

Tenable has prepared a comprehensive paper outlining how our scanning, configuration monitoring, data leakage, passive network analysis, and log analysis solutions can be used for measuring and demonstrating "compliance".

Request a copy from
sales@tenablesecurity.com