TENABLE Network Security®

Application Note:
Monitoring for PCI

Preparing for a Successful PCI Audit

Introduction

Mandated by Visa USA in June 2001, the Cardholder Information Security Program (CISP) is a set of security standards aimed at protecting credit card information wherever it resides to ensure that members, merchants, and service providers maintain the highest information security standard. In 2004, through a collaboration between Visa and MasterCard, the CISP requirements were incorporated into the Payment Card Industry (PCI) Data Security Standards (DSS) or PCI DSS, to create a common industry standard that is accepted internationally by all major credit card issuers. Currently, Visa maintains the standard and compliance program of PCI DSS.

Implications of non-compliance can be severe. Non-compliant organizations can be fined as much as $500,000 per incident of data theft and this does not include the punitive damages, loss of company reputation, and/or even jail time the corporate officers may face. For third party service providers it can be even worse – non-compliance means they could lose their valuable retail customers. The PCI DSS requires merchants to deal only with third party service providers that adhere to the payment card security standards.

Although it is obvious that PCI is applicable to retailers and e-commerce sites, it affects all organizations that accept credit cards for payment of products or services, such as the physician's office or a university's bursar.

PCI RECOMMENDATION	TENABLE SOLUTION
Firewall Maintenance	Log Correlation Engine
	Passive Vulnerability Scanner
Default Passwords	Nessus Vulnerability Scanner
Protect Data	Log Correlation Engine
Encrypt Transmission	Passive Vulnerability Scanner
Anti-virus Updates	Security Center
	Passive Vulnerability Scanner
Maintain Systems	Nessus Vulnerability Scanner
	Passive Vulnerability Scanner
Need to Know Access	Security Center
Unique ID	Log Correlation Engine
Physical Access	Log Correlation Engine
Regular Testing	Security Center
Policy	Security Center

TENABLE's Role in PCI Security

All merchants fall into one of the four merchant levels determined by transaction volume over a 12-month period. As of July 18, 2006, classifications have been redefined, and the associated requirements defined. The highest classification level requires an annual on-site assessment by a "qualified security assessor or Internal Auditor if signed by the Officer of the company." Using a combination of TENABLE security solutions can provide the Auditor the information required to meet this requirement.

All classification levels require quarterly vulnerability scans to be conducted by an approved scanning vendor. TENABLE does not perform these scans, but TENABLE products are used by approximately 80% of the approved vendors. TENABLE's role in this is to equip our customers with the solutions to manage and report on their network *before* they undergo a costly audit.

Finally, organizations-regardless of classification level-are required to submit a quarterly self-assessment based on various security assessment data that is obtained through the TENABLE solutions.

Vulnerability Scanning and Reporting

According to Master Card, "Network Security Scans are an indispensable tool to be used in conjunction with a vulnerability management program. Scans help identify vulnerabilities and misconfigurations of Web sites or IT infrastructures containing externally facing IP addresses. Scan results provide valuable information that support efficient patch management and other security measures that improve protection against internet hacking.

Network Security Scans apply to all merchants and service providers with external-facing IP addresses. Even if an entity does not offer Web-based transactions, there are other services that make systems Internet accessible. Basic functions such as e-mail and employee Internet access will result in the Internet-accessibility of a company's network. "

Regularly Monitor and Test Networks

VISA Requirement 10 (Track and monitor all access to network resources and cardholder data) states "logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs." Recent qualifications to PCI compliance, require organizations to retain log data for a minimum of 1 year.

PCI Security Scanning

The Nessus™ Vulnerability Scanner, is the world-leader in active scanners, featuring high speed discovery, asset profiling, and vulnerability analysis for PCI compliance. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks. When managed with the Security Center, vulnerability recommendations can be sent to the responsible parties, remediation can be tracked, and security patches can be audited. Additionally, configuration auditing is available.

Passive vulnerability scanning is the process of monitoring network traffic at the packet layer to determine topology, clients, applications, and related security issues. It can not only keep track of the vulnerabilities for more than 25,000 systems at a time, it can also:

- Detect when they are compromised based on application intrusion detection
- Highlight all interactive and encrypted network sessions
- Detect when new hosts are added to a network
- Track exactly which systems communicate with other systems and on which ports
- Detect what ports are served and what ports are browsed by each system

TENABLE's Passive Vulnerability Scanner performs these tasks in real-time, 24x7. A passive scanner has no impact on the systems it is monitoring.

Network Monitoring & Event Management

TENABLE's Log Correlation Engine automatically collects information from system components covered under PCI compliance and provides an intelligent layer of analysis, audit and documentation. When used with the TENABLE Security Center, it creates an automated audit log trail that reconstructs audit trail requirements; provides required access control to audit trail; performs file integrity monitoring; automatically backs up audit logs or retention.

Daily reviews of event and audit logs as prescribed by PCI are near impossible without an automated security event correlation and management component. The TENABLE Log Correlation Engine makes daily review of logs for system components more efficient and provides a holistic view of the PCI components (servers, switches, routers, firewalls, etc.).

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

Benefits of the TENABLE Solution

Using the TENABLE suite of security solutions provides several advantages to enterprises who want a centralized way to conduct active and passive vulnerability scans and network monitoring as prescribed by the Payment Card Industry for protecting confidential information.

- Nessus Vulnerability Scanner and TENABLE Passive Scanner fulfill the requirement in PCI compliance for vulnerability scanning and reporting, whether it be the quarterly or self-assessment activities.
- TENABLE's Security Center provides proactive, asset-based security risk management. It unifies the process of asset discovery, vulnerability detection, event management and compliance reporting.
- TENABLE's Security Center can correlate actual vulnerability data with firewall and IDS events identifying those systems where a threat actually exists.
- As the trend continues for wireless communication for POS networks, scanning for these network points will assure that only authorized WAPs (Wireless Access Points) are enabled.

CONCLUSION

Enterprise risk protection is a key component of security best practices for the enterprise. By using the TENABLE Security Center with the Nessus Vulnerability Scanner, Passive Vulnerability Scanner, and Log Correlation Engine, enterprises can implement a risk protection and threat correlation capability that radically improves security response and increases security effectiveness. The solution requires minimal security experience and can effectively be used to monitor the PCI environment.

For additional information, please visit
http://www.TENABLEsecurity.com

or subscribe to the TENABLE BLOG at
http://blog.TENABLEsecurity.com/

TENABLE Network Security has a detailed White Paper discussing how our technologies map to PCI standards. Please request this by sending an email to sales@TENABLEsecurity.com.