Payment Card Industry Data Security Standard (PCI-DSS) & Vulnerability Scanning

Justin David Pineda
August 1, 2015
Asia Pacific College

Agenda

1. What is PCI-DSS and why is it necessary?
2. What is vulnerability scanning why do we need to conduct it regularly?
3. Vulnerability scan demonstration

1. What is PCI-DSS and why is it necessary?

1 of 3

What is PCI-DSS?

- Developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.
- Provides a baseline of technical and operational requirements designed to protect cardholder data.

(PCI Requirements & Procedures, 2010, p.5)

What are the PCI Requirements?

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

(PCI Requirements & Procedures, 2010, p.5)

What are the steps?

- **Assess** - Take an inventory of IT assets and business processes and analyze for vulnerabilities that could expose cardholder data.
- **Remediate** - Process of fixing those vulnerabilities.
- **Report** - Validate remediation records required by PCI and submit reports to the bank and payment brands you do business with.

The vulnerability management req't…

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

2. What is vulnerability scanning why do we need to conduct it regularly?

2 of 3

Vulnerability Scan

- Checks for the weaknesses in a network, system and application.
- Helps the organization discover their weaknesses to fix before the actual intruder exploits it.

Top 6 Free Network Vulnerability Scanners

- OpenVAS
- Retina CS Community
- Microsoft Baseline Security Analyzer
- Nexpose Community Edition
- SecureCheq
- Qualys Free Scan

From: http://www.networkworld.com/article/2176429/security/6-free-network-vulnerability-scanners.html

14 Best Open Source Web Application Vulnerability Scanners

Grabber	RatProxy
Vega	SQL Map
Zed Attack Proxy	Wfuzz
Wapiti	Grendel-Scan
W3af	Watcher
Web Scarab	X5S
SkipFish	Arachni

From: http://resources.infosecinstitute.com/14-popular-web-application-vulnerability-scanners/

Vulnerability Scan vs. Penetration Testing

- Vulnerability scan – finding weaknesses
- Penetration testing – actively exploiting the weaknesses found

- **Caution: In both scenarios, you need permission first before initiating tests.**

Vulnerability Scanning in PCI

- Organizations must look for a third-party Authorized Scanning Vendor (ASV)
- To pass the test, applications and servers must have no high or medium severity issues.
- ASV attests to the results of the scan.
- The scan is done quarterly.

3. Vulnerability Scan demonstration

3 of 3

Vulnerability Scanner: Acunetix

Tasks:

- Download trial version here- https://www.acunetix.com/vulnerability-scanner/download/
- Run a scan in its test site: http://testhtml5.vulnweb.com/
- Verify a vulnerability by exploiting it.