2014

Meet PCI DSS Requirements with FOSS

This document helps you to Identify the Free and Open Source Software which can be used to meet one or more PCI-DSS Requirements

Rajagopalan S
Blog: Http://securityncompliance.wordpress.com
12/07/2014

About this document:

This document is created in order to utilize the Free & Open Source Software which helps us to meet one or more PCI-DSS Requirements. Document was created on my sole interest aimed at helping the PCI-DSS Professionals and entities who are required to be PCI-DSS Compliant. The FOSS is mapped to each PCI-DSS requirement. I have tried my best to search and gather all open source applications which could be used to meet / assess the PCI-DSS Compliance. If you find any useful free and open source software let me know we could add to this list.

This document doesn't recommend any entity to forcefully use only the FOSS to meet its PCI-DSS compliance and also it doesn't replace the interest of any organization buying Commercial Products. Also Read Disclaimer Section of this document.

Targeted Audience:

- PCI-QSA's
- PCI Internal Assessors
- Organization that are required to comply with PCI-DSS Standard
- Compliance Professionals

Abbreviations & Acronyms:

- **PCI DSS – Payment Card Industry Data Security Standards**
- **FOSS – Free and Open Source Software**

Contents

Requirement 1: *Install and maintain a firewall configuration to protect cardholder data*

Requirement 1.1.2:

Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks

Application listed below will help you to create a network diagram at free of cost. If you require all-in-one suite then MS Visio is the best of all, but it cost.

Application to design a Network Diagram:

- **Gliffy Flowchart Software (Create Flow Charts Online)**
  URL: http://www.gliffy.com/uses/flowchart-software/

- **CADE**
  URL: http://www.weresc.com/home.php

- **Diagram Designer**
  URL: http://logicnet.dk/DiagramDesigner/

- **yEd**
  URL: http://www.yworks.com/en/products_yed_about.html

- **Open Office Draw**

Requirement 1.2:

Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

1. **Firewall Auditor**
   Inspect Firewall Configuration to ensure its properly configured
   URL: http://www.firewallauditor.com/Download/

   Supported Firewall:

   Check Point Firewall-1 versions NG™ FP3 and later (including those firewalls that are cluster members), Cisco (PIX versions 6.0 and later, ASA versions 7 and later, FWSM version 3.0 and later Juniper Networks (NetScreen versions 5.0 and later)

2. **Nipper**

Configuration audit using Nipper

Titania Nipper (Evaluation, Free version are available with BackTrack OS)
URL: **https://www.titania.com/nipperstudio**

Requirement 2: *Do not use vendor-supplied defaults for system passwords and other security parameters*

1. **Default Username and password of some Network Devices**
   URL: **http://www.datarecovery.com/default_passwords.php**

2. **Configuration audit using Nipper**
   Titania Nipper (Evaluation, Free version are available with BackTrack OS)
   URL: **https://www.titania.com/nipperstudio**

3. **Open Audit**

   Open-AudIT is an application to tell you exactly what is on your network, how it is configured and when it changes.

   URL: http://www.open-audit.org/

4. **Lynis**

   Security and system auditing tool (Linux Security Audit Tool)
   URL: http://cisofy.com/downloads/

5. **Tiger** (The Unix security audit and intrusion detection tool)

   URL: http://www.nongnu.org/tiger/
   Download: http://download.savannah.gnu.org/releases/tiger/?C=M;O=D

Requirement 3: *Protect stored cardholder data*

Requirement 3.1:

Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- ***Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements***
- ***Processes for secure deletion of data when no longer needed***

Secure Deletion:

1. **Eraser:**

   Eraser is an advanced security tool for Windows which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns.

   URL: http://eraser.heidi.ie/download.php

   OS Supported : It works with Windows XP (with Service Pack 3), Windows Server 2003 (with Service Pack 2), Windows Vista, Windows Server 2008, Windows 7 and Windows Server 2008 R2, Windows 98, ME, NT, 2000 can still be used with version 5.7

2. **Sdelete Utility from SysInternals:**

   SDelete is a command line utility that takes a number of options. In any given use, it allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk. SDelete accepts wild card characters as part of the directory or file specifier.

   URL: http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

3. **Secure Deletion on Mac OS X**
   Apple's advice on preventing forensic undeletion on Mac OS X is as follows:

   To prevent the recovery of files you deleted previously, open Disk Utility (in Applications/Utilities), choose Help > Disk Utility Help, and search for help on erasing free disk space.

4. **Secure Deletion on *nix Operating Systems**

   Secure Deletion of Individual Files

Linux, FreeBSD and many other UNIX systems have a command line tool called ***shred*** installed on them. Shred works quite differently to the Windows cipher.exe program; rather than trying to prevent previously deleted files from being recoverable, it singles out specified files and repeatedly overwrites them and their names with random data.

If you are comfortable using a terminal or command line, secure deletion of files with shred is simple. Just run the following command:

Command: shred -u

5. **Wipe:** Like Eraser, Wipe overwrites deleted files in order to make them impossible to restore. Operating System: Linux.

   URL: http://sourceforge.net/projects/wipe/files/

6. **Darik's Boot And Nuke:**

   DBAN is a self-contained boot disk that automatically deletes the contents of any hard disk that it can detect. This method can help prevent identity theft before recycling a computer.

   URL: http://www.dban.org/

Requirement 3.1b:

A quarterly automatic or manual process is in place to identify and securely delete stored cardholder data.

1. **Refer my previous post on Free Card Scan Tools**
   http://securityncompliance.wordpress.com/2014/05/03/free-commercial-card-scan-tools/#more-52

2. **Open DLP:**
   Data Loss Prevention suite with centralized web frontend to manage Windows agent file system scanners, agentless database scanners, and agentless Windows/UNIX filesystem scanners that identify sensitive data at rest

   URL: https://code.google.com/p/opendlp/

Requirement 3.2.1:

Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

Use this tool to analyze the RAM contents

1. **Wiki : http://www.forensicswiki.org/wiki/Tools:Memory_Imaging**

2. **Helix : http://www.e-fense.com/products.php**

3. **Belkasoft Live RAM Capturer (To analyze RAM Memory Contents) for SAD**

   (Belkasoft Live RAM Capturer is a tiny free forensic tool to reliably extract the entire content of the computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system. Separate 32-bit and 64-bit builds are available in order to minimize the tool's footprint as much as possible.)

   URL: http://forensic.belkasoft.com/en/ram-capturer

4. **MDD:** MDD is a physical memory acquisition tool for imaging Windows based computers created by the innovative minds at ManTech International Corporation. MDD is capable of acquiring memory images from Win2000, XP, Vista and Windows Server.

   URL: http://sourceforge.net/projects/mdd/

5. **WinHEX**
   URL: http://www.x-ways.net/winhex.zip

6. **WinDump**
   URL: http://www.winpcap.org/windump/install/default.htm

Network Protocol Analyzer

7. **Wireshark (http://www.wireshark.org/): Packet Analyzer**

Requirement 3.4:

Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

Disk / File / Directory Encryption:

1. **True Crypt Ver 7.2:**
   URL: http://sourceforge.net/projects/truecrypt/files/TrueCrypt/TrueCrypt-7.2.exe/download

2. **VeraCrypt** - Similar to Truecrypt
   VeraCrypt is a free disk encryption software brought to you by IDRIX URL: (http://www.idrix.fr) and that is based on TrueCrypt
   Download: http://sourceforge.net/projects/veracrypt/

3. **Bitlocker** (Utility comes with Windows Vista / Windows 7 & 8)

4. **Diskcryptor: http://sourceforge.net/projects/diskcryptor/?source=recommended**

5. **Gpg4win:**
   Gpg4win (GNU Privacy Guard for Windows) is encryption software for files and emails.
   URL: http://www.gpg4win.org/download.html

6. **Directory Checksum Tool : http://www.idrix.fr/Root/content/category/7/31/55/**

7. **Ccrypt:**
   ccrypt is a command-line utility for encrypting and decrypting files and streams. It replaces the old UNIX crypt utility. Ccrypt provides strong encryption, based on the Rijndael cipher, the cipher that is also used in the Advanced Encryption Standard.
   URL: http://sourceforge.net/projects/ccrypt/?source=directory

8. **Hash Tool: http://www.idrix.fr/Root/Samples/DirHash.zip**

9. **Secure Mail (Email Encryption & File encryption based on Java)**
   Secure Mail is an email /file encryption - decryption software. It uses RSA-4096 bit asymmetric encryption coupled with AES-128 bit symmetric encryption.
   Any & all data leaving the app & through the internet is completely encrypted as well as the data at rest, at both the inbound & outbound server of your email provider. The app also features an independent file encryption - decryption mode.

   URL: http://sourceforge.net/projects/securemail

Requirement 3.6:

Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data,

Key Management:

If your application is developed using java, you can use the java keytool to implement and manage the Encryption Keys

1. **Java Keytool**

   URL:
   - **http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html**
   - **http://www.networking4all.com/en/support/ssl+certificates/manuals/java/java+based+webserver/keytool+commands/**

2. **Keystore Explorer:**

   URL: http://sourceforge.net/projects/keystore-explorer/?source=directory

3. **Portecle**

   Portecle is a user friendly GUI application for creating, managing and examining key stores, keys, certificates, certificate requests, certificate revocation lists and more.

   URL: http://sourceforge.net/projects/portecle/?source=recommended

4. **Oracle TDE: (Transparent Data Encryption)**
   URL: http://docs.oracle.com/cd/E11882_01/network.112/e10746/asotrans.htm#ASOAG600

Requirement 3.6.4:

Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

1. **Reference: NIST 800-57:**

   a. **SP 800-57 Part 1: Recommendation for Key Management: Part 1: General (Revision 3)**

   URL: http://csrc.nist.gov/publications/nistpubs/800-57/sp800 57_part1_rev3_general.pdf

   b. **SP 800-57 Part 2: Recommendation for Key Management: Part 2: Best Practices for Key Management Organization**

URL:http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

c. **SP 800-57 Part 3: Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance**

URL: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf

d. **http://www.keylength.com/ - Get Details on the Cryptographic Algorithm, its key size, cryptoperiod etc.**

2. **SP 800-57 Part 3-Rev.1**
   (Draft)
   URL: http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-57-Part%203-Rev.1

3. **Secure Password Generator:**
   URL: https://www.grc.com/passwords.htm

4. **Key Generation Tool:**
   URL: http://www.emvlab.org/keyshares/

Requirement 4: *Encrypt transmission of cardholder data across open, public networks*

1. ***Open SSL:***

   URL: https://www.openssl.org/docs/apps/openssl.html

2. **Harden SSL:**

   "Harden SSL/TLS" allows hardening the SSL/TLS settings of Windows 2000, 2003, 2008, 2008R2, XP, Vista,7. It allows locally and remotely set SSL policies allowing or denying certain ciphers/hashes or complete cipher suites.

   URL: http://www.g-sec.lu/sslharden/HardenSSL.zip

3. **SSL Audit:**

   SSL Audit remotely scans web servers for SSL support, unlike other tools it is not limited to ciphers supported by SSL engines such as OpenSSL or NSS but can detect all known cipher suites. It features an innovative Fingerprinting engine that was never seen before.

   URL: http://www.g-sec.lu/sslaudit/sslaudit.zip

4. **Secure File Transfer:**

   WinSCP 5.5.4: Free SFTP, SCP and FTP client for Windows

   URL: http://winscp.net/eng/download.php

5. **Filezila:**

   FileZilla Client is a fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features and an intuitive graphical user interface.

   URL: https://filezilla-project.org/

6. **SSH System Administration Tool**

   - ssh Java interface for Unix, Linux and MS Windows system administration and monitoring.
   - Automates firewall rule checks; exporting the results into Excel. **URL: http://sshadmincontrol.com/**

Requirement 5: Maintain a Vulnerability Management Program

Many commercial AV Products are available (McAfee, Symantec, Kaspersky, CA, K7, Comodo etc...), recommended to use the paid version rather than free version. The features available in the paid version may not be available in the free version. Some of the well-known free AV providers are mentioned below; Use free AV on the Risk Based approach

1. ***FREE Anti-Virus:***

   URL:
   - Malware bytes http://www.malwarebytes.org/
   - AVG http://free.avg.com/in-en/homepage
   - AVIRA http://www.avira.com/en/avira-free-antivirus
   - Microsoft Security Essentials http://windows.microsoft.com/en-IN/windows/security-essentials-download

   AV Comparison Wiki:
   - http://en.wikipedia.org/wiki/Comparison_of_antivirus_software

2. ***Linux Open Source Anti-Virus:***

   Clam AV: http://www.clamav.net/lang/en/

Requirement 6: *Develop and maintain secure systems and applications*

Requirement 6.3.2:

Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated

Code Review: Java

1. **PMD from http://pmd.sourceforge.net/**
2. **FindBug from http://findbugs.sourceforge.net**
3. **Clover from http://www.cenqua.com/clover/**
4. **https://www.owasp.org/index.php/Source_Code_Analysis_Tools**
5. **Source Navigator NG**
6. **Eclipse Checkstyle Plug-in**
7. **http://java-source.net/open-source/code-analyzers**

Code Review: PHP

1. **RIPS: http://sourceforge.net/projects/rips-scanner/**

Code Review: Objective C Program – Source Code Analysis

1. **http://clang-analyzer.llvm.org/**

Requirement 6.6:

For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks

- ***Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes***
- ***Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.***

1. **Modsecurity:** Open Source Web Application Firewall
   URL: www.modsecurity.org/

2. **ARACHNI**

Arachni is an Open Source, feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications. Systems like Arachni are complementary to a manual audit and verification and further investigation of results will always be necessary. Automated audits have come a long way but cannot replace a human.

URL: http://www.arachni-scanner.com/

3. **OS Discover Vulnerability Scanning:**

osDiscover is an open source modular web framework for discovering, analyzing and managing vulnerability threats.

URL: http://www.osdiscover.org/
http://www.clone-systems.com/open-source.html

4. **W3af**

W3af is a **Web Application Attack and Audit Framework**. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities.

URL: http://w3af.org/download

5. **Wapiti**

Wapiti is a vulnerability scanner for web applications. It currently search vulnerabilities like XSS, SQL and XPath injections, file inclusions, command execution, XXE injections, CRLF injections... It use the Python programming language.

URL: http://wapiti.sourceforge.net/

6. **OWASP Zed Attack Proxy**

The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

URL: https://www.owasp.org/index.php/ZAP

7. **OWASP Links to various Web Application Security Scanner**

URL: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

8. **Watcher (Web security testing tool and passive vulnerability scanner)**

Watcher is a Fiddler addon which aims to assist penetration testers in passively finding Web-application vulnerabilities.

URL: http://websecuritytool.codeplex.com/releases/view/22212

9. **Fiddler:**

The free web debugging proxy for any browser, system or platform
URL: http://www.telerik.com/download/fiddler

Requirement 7: Restrict access to cardholder data by business need to know

Requirement 8: Identify and authenticate access to system components

Requirement 7.2:

Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

1. **Fortress:**

   Fortress is a standards-based and open source IAM system that provides ANSI RBAC (INCITS 359) management and enforcement capabilities to networked applications and systems.

   OS Supported:
   Centos 6.3 32/64 bit
   Ubuntu 12.04 32/64 bit
   Windows 32 bit
   Debian
   Redhat

   URL: http://iamfortress.org/download

2. **Central Authentication Service (CAS)**

   CAS provides enterprise single sign on service and is an open and well-documented protocol, an open-source Java server component, a library of clients for Java, .Net, PHP, Perl, Apache, uPortal, and others, integrates with uPortal, BlueSocket, TikiWiki, Mule, Liferay, Moodle and others, offers community documentation and implementation support, and includes an extensive community of adopters.

   URL: http://www.jasig.org/cas/download

3. **ForgeRock**

   Open AM
   The only "all-in-one" open source access management solution provides the most comprehensive consumer-facing identity relationship management (IRM) services, as well as traditional access management capabilities.

   URL: https://backstage.forgerock.com/#/downloads/enterprise/OpenAM

Open IDM

OpenIDM allows organizations to automate user identity lifecycle management in real time, including the management of user accounts and access privileges in applications. Lightweight and agile, OpenIDM was designed to help organizations ensure compliance with policies and regulatory requirements across enterprise, cloud, social and mobile environments, and adapt to today's unique identity relationship management (IRM) challenges with ease.

URL: https://backstage.forgerock.com/#/downloads/enterprise/OpenIDM

Open DJ

OpenDJ is the only 100 percent open-source big data platform that combines the security of a proven directory with the accessibility of a database. Lightweight and easy to embed, it allows you to easily share real-time identity data across enterprise, cloud, social and mobile environments - a practical necessity for managing today's identity relationship management challenges (IRM).

URL: https://backstage.forgerock.com/#/downloads/enterprise/OpenDJ

4. **Open LDAP**

OpenLDAP Software is an open source implementation of the Lightweight Directory Access Protocol.

URL: http://www.openldap.org/software/

5. **Soffid IAM**

Soffid is a highly distributed Identity Manager, featuring a single identity of users across enterprise. It supports lots of authentication systems and applications: Active Directory, LDAP, SQL based and file based authentication. It supports high workloads. It has been tested in production environment with 50.000+ users and 300+ applications.

URL: http://sourceforge.net/projects/soffid/?source=directory

6. **Open IAM Identity Manager**

OpenIAM's Identity Manager provides a comprehensive Identity Management solution which allows organizations to to manage the full user life cycle. Features includes: User provisioning and de-provisioning, active synchronization, password management, audit, self-service and delegated administration.

Community edition includes connectors for LDAP, Active Directory, Google Apps and Relational Databases

URL: http://sourceforge.net/projects/openiam/?source=directory
Source: http://www.openiam.com/

Requirement 8.7.a:

Review database and application configuration settings and verify that all users are authenticated prior to access.

1. **Oracle 11g Hardening:**
   URL: docs.oracle.com/cd/B28359_01/network.111/b28531.pdf
2. **Secure Oracle Auditor – Trial Version**
   URL: http://www.secure-bytes.com/soa.php

Requirement 9: Restrict physical access to cardholder data

Requirement 9.8.2:

Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

Refer Section **"Secure Deletion"** in this document. Applicable only for the secure deletion of the Files / Directories and Hard drives.

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 10.5.3:

Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

Requirement 10.5.4:

Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

Centralized Logging:

1. **Logalyze**

   URL: **http://logalyze.com/downloads**

2. **Syslog – ng**

   URL: **http://www.balabit.com/network-security/syslog-ng/opensource-logging-system/downloads/3rd-party**

3. **Nxlog:**
   URL: **http://nxlog.org/download**

4. **Octopussy (**Open Source Log Management Solution)

   URL: **http://www.octopussy.pm/**

5. **ZLogFabric**

URL: **http://www.zlogfabric.com/downloads**

6. **Splunk (Free) – 500 Mb Logging per day**

   URL: **http://www.splunk.com/view/free-vs-enterprise/SP-CAAAE8W**

7. **Snare – Auditing and EventLog Management**

   URL: **http://sourceforge.net/projects/snare/?source=directory**

Requirement 11: Regularly test security systems and processes.

Requirement 11.1:

Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

Wireless Auditors

1. **Aircrack-NG: http://aircrack-ng.org/ -** Wireless Network Auditor and WEP, WPA-PSK Keys Cracker

2. **NetStumbler (http://www.stumbler.net/)**

3. **NetSurveyor (http://www.performancewifi.net/performance-wifi/main/NetSurveyor.htm)**

4. **Xiwtool :** On Linux systems that have a wireless network interface, xiwtool can scan and view statistics for nearby Wireless Access Points. Xiwtool has many internal features that provide reliable network scanning and management in crowded environments.

   URL: http://sourceforge.net/projects/xiwtool

5. **Kismet:**

   Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins which allow sniffing other media such as DECT.

   URL: http://www.kismetwireless.net/

Requirement 11.2:

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

10. **OPEN VAS:**

    The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

The actual security scanner is accompanied with a daily updated feed of Network Vulnerability Tests (NVTs), over 35,000 in total (as of April 2014).

URL: http://www.openvas.org/install-packages-v6.html

11. **Nmap:** Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

    (http://nmap.org/) Port & Services discovery tool

12. **Zenmap (GUI Version of nMap) http://nmap.org/zenmap/**
    OS Supported: Windows, Linux, Mac, and BSD

13. **Angry IP Scanner (http://angryip.org/)**

14. **Microsoft Baseline Security Analyzer (MBSA) Only for Windows**

    Microsoft Baseline Security Analyzer (MBSA) lets administrators scan local and remote systems for missing security updates as well as common security misconfigurations.

    URL: http://technet.microsoft.com/en-us/security/cc184924.aspx#current-version

15. **Cloud Based Vulnerability Scanner:**

    a. **Tripwire Secure Scan (Only for Publicly accessible systems)**

       URL: **http://www.tripwire.com/securescan/**

Penetration Testing:

Requirement 11.3.1:

Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Requirement 11.3.2:

Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

1. **Kali Linux:**

   From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system

   URL: http://www.kali.org/downloads/

2. **BackTrack Linux:**

   BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. Regardless if you're making BackTrack you Install BackTrack, boot it from a Live DVD or thumbdrive, the penetration distribution has been customized down to every package, kernel configuration, script and patch solely for the purpose of the penetration tester.

   URL: http://www.kali.org/downloads/

3. **Hcon Security Testing Framework**

   HconSTF is Open Source Penetration Testing Framework based on different browser technologies, Which helps any security professional to assists in the Penetration testing or vulnerability scanning assessments.contains webtools which are powerful in doing xss(cross site scripting), Sql injection, siXSS, CSRF, Trace XSS, RFI, LFI, etc.

   URL: http://www.hcon.in/

4. **Revenssis Penetration Testing Suite (Mobile Device)**

Nicknamed as the "Smartphone Version of Backtrack", Revenssis Penetration Suite is a set of all the useful types of tools used in Computer and Web Application security. Tools available in it include: Web App scanners, Encode/Decode & Hashing tools, Vulnerability Research Lab, Forensics Lab, plus the must-have utilities (Shell, SSH, DNS/WHOIS Lookup, Traceroute, Port Scanner, Spam DB Lookup, Netstat... etc).

URL: http://ssyrix.com/

5. **Samurai Web Testing Framework**

The Samurai Web Testing Framework is a live linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focus on testing and attacking websites.

URL: http://sourceforge.net/projects/samurai/files/

Requirement 11.4:

Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

1. **Security Onion**

Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools

URL: http://blog.securityonion.net/p/securityonion.html

2. **Snort:**

Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.

URL: http://www.snort.org/

Requirement 11.5:

Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

File Integrity Monitoring Solution

1. **OSSEC**

   About OSSEC:

   OSSEC is an Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.

   It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows.

   http://www.ossec.net/?page_id=19

2. **Tripwire (Supports AIX 7.1)**

   Change may be the way of the world, but it's the sworn enemy of IT security. Compliance regulations like PCI DSS, NIST 800-53 and the SANS 20 Critical Security Controls require file integrity monitoring to pass ongoing audits.

   It only takes one accidental, misguided, undocumented—or malicious—change to undermine the state of your IT infrastructure and turn integrity into uncertainty. Tripwire's File Integrity Monitoring finds, assesses and acts on those changes as soon as they occur. It assures ongoing system integrity and automates detecting, auditing and reconciling changes—even the low profile, obscure ones that reveal advanced hacks and exploits.

   http://www.ibm.com/developerworks/aix/library/au-usingtripwire/#resources
   http://www.perzl.org/aix/index.php?n=Main.HomePage

3. **AIDE - Advanced Intrusion Detection Environment**

   AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker.
   Platform Support: Any UNIX Based

   URL: http://aide.sourceforge.net/

4. **Samhain**

The Samhain host-based intrusion detection system (HIDS) provides file integrity checking and log file monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes.

Samhain been designed to monitor multiple hosts with potentially different operating systems, providing centralized logging and maintenance, although it can also be used as standalone application on a single host.

Samhain is an open-source multiplatform application for POSIX systems (UNIX, Linux, and Cygwin/Windows).

URL: http://www.la-samhna.de/samhain/index.html

Some References URL's and Names:

1. http://www.datamation.com/osrc/article.php/12068_3882711_2/50-Open-Source-Tools-To-Replace-Popular-Security-Software.htm
2. http://www.net-security.org/software.php?id=125
3. http://sectools.org/
4. http://sourceforge.net/
5. http://www.gfi.com/blog/18-free-security-tools-for-sysadmins/
6. NIST
7. Gibson Research Corporation (https://www.grc.com/default.htm)
8. http://www.keylength.com/
9. http://www.wikipedia.org/

Disclaimer:

The information provided in this document is provided "as is" without any express or implied warranties. I have put reasonable efforts to include accurate, complete and current information. However, I don't warrant that the content herein is accurate, complete, current, or free of technical or typographical errors. It is your responsibility to verify any information before relying on it. This document doesn't warrants or guarantees you on using these software's will make you fully PCI-DSS Compliant and also it doesn't replace the PCI-DSS Standards. All the FOSS applications/utilities/Tools mentioned here are developed and released by its respective owners/company/publisher/forums or groups under various open source licensing methodologies, Terms & Conditions. Review their licensing terms & conditions before using the software.