**How to Comply to Requirement 11 of PCI DSS**

Malicious individuals regularly aim to discover new vulnerabilities in systems and new software. It is hence very important to perform a regular test on system components, software and processes to verify security controls of the organization.

**PCI DSS Requirement 11: Regularly test security systems and processes.**

To validate that your organization is compliant to the PCI DSS, it is very important to regularly test your organization’s security system. Thought it may seem taxing at first, but it is the best way to achieve PCI DSS compliance. It not only confirms the required level of network protection in your system, it also ensures that no vulnerabilities are left out during routine operations and information security procedures.

**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.**

If a wireless device is installed on a system or a network without the knowledge of the organization, it can be easily used by a malicious individual to access all information on the network, particularly the cardholder data. This is a very common technique used by criminals to gather cardholder information. Such devices may be attached to a system component or to a network port or device, such as router or switch. It is thus, very important for the administrators to keep a check on authorized wireless devices and watch out for any unauthorized devices installed on the network. To scan unauthorized wireless devices, some of the methods used are physical/logical inspections, wireless network scans, network access control, wireless IPS/IDS, etc.

To achieve compliance, the following measures must be taken:

* Verification of policies and procedures to detect and identify authorized and unauthorized wireless devices.
* Verification of the methodology used for detection. This should be adequate enough to identify basic wireless devices such as WLAN cards, portable devices, and wireless devices connected to network ports.
* Ensuring that network scans are performed on a quarterly basis
* Verification of automatic notifications in case automatic monitoring mechanism such as wireless IPS/IDS is being used.
* Examine the incident response plan to verify that a mechanism to properly respond to incident reporting is implemented.

**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).**

This requirement mandates that both internal and external vulnerability scans must be performed once in every quarter or after any change in the system or network. A vulnerability scan is an automated tool that scans internal and external network devices to identify any potential vulnerabilities lying in between.

To achieve compliance, the following steps must be ensured:

* It should be verified that at least four quarterly scans were conducted in last 12 months.
* Scan reports should be reviewed to verify that all results are rescanned until all high risk vulnerabilities are removed.
* Verify that the internal scan was conducted by qualified personnel and that the external scan was conducted by an Approved Scanning Vendor (ASV).
* Examine the change control documentation and verify that any change in system components was also made a part of the scanning process.

**11.3 Implement a methodology for penetration testing that includes the following:**

* **Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)**
* **Includes coverage for the entire CDE perimeter and critical systems**
* **Includes testing from both inside and outside the network**
* **Includes testing to validate any segmentation and scope-reduction controls**
* **Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5**
* **Defines network-layer penetration tests to include components that support network functions as well as operating systems**
* **Includes review and consideration of threats and vulnerabilities experienced in the last 12 months**
* **Specifies retention of penetration testing results and remediation activities results.**

A penetration test serves to evaluate a system in terms of how far a malicious hacker will be able to penetrate into the network, by simulating an attack. It is a proactive approach and serves as a counter mechanism by the organization to develop protective strategies against a potential attack. A penetration test is one step ahead of a vulnerability scan as a penetration tester attempts to exploit the vulnerabilities detected in a vulnerability scan.

It is important that in order to comply with the above requirement, the penetration testing mechanism must be examined and penetration testers should be interviewed to verify the above mentioned fulfillments. Results should be verified to validate that penetration tests are performed at least once a year and also after every change within the network. Network and application penetration tests must be verified at all levels of the organization. The results of penetration tests must also be examined to verify that the discovered vulnerabilities were removed and a retest confirmed the removal of those vulnerabilities.

**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.**

This requirement mandates that organizations should employ the use of network and host-based intrusion detection systems and intrusion prevention systems (IDS/IPS) for monitoring network traffic through the CDE. These technologies can help to alarm the organization of any possible data breach. Moreover, the intrusion prevention and detection engines should be properly maintained, otherwise the organization may not be able to identify the threats.

System configurations and network diagrams should be inspected to verify that IDS/IPS techniques are functioning properly at cardholder perimeter and cardholder critical points. Personnel should be interviewed to confirm that these systems inform the responsible individuals of any compromise of data. Furthermore, the vendor documentation and configurations should be examined to verify that the IDS/IPS are regularly maintained and updated according to the vendor instructions.

**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.**

Change detection tools are important to identify any modifications in important files and to notify the management in case of any such changes. Organizations that need to seek compliance with this requirement need to install file-integrity monitoring software which alerts the personnel of any unauthorized modifications in the system. This requirement also enforces the configuration of the software so that it analyzes the files at least once a week. Doing this ensures that modifications in the system are identified soon after they are applied.

To achieve compliance, review the change detection mechanism and examine the system settings of all monitored files. It should also be verified that the detection mechanism is configured to inform the personnel of any unauthorized changes and also to perform file comparisons once a week.

**11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.**

To achieve compliance, it should be verified that all security policies and operational procedures for this requirement are put in a documented format, are followed throughout the organization and are communicated to all the involved parties.