PCI Penetration Testing Checklist

Test Your Cyber Defenses

Penetration tests are intended to exploit weaknesses in the architecture of your IT network and are essential to determine the degree in which a malicious attacker can gain unauthorized access to your company's assets. Vulnerability scans look for known vulnerabilities in your systems and may report potential exposures.

At Drummond, our experts conduct penetration tests separate from your quarterly vulnerability scanning requirements and adhere to industry-accepted penetration testing methods. The penetration test must identify ways to exploit vulnerabilities circumvent or defeat the security features of system components.

Per the ***PCI SSC Information Supplement: Penetration Testing Guidance,*** the goals of penetration testing include how to:

- Determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files, logs and/or cardholder data
- Confirm the applicable controls required by PCI DSS – cope, vulnerability management, methodology and segmentation – are in place

Black-, White- or Grey-box Assessments

There are three types of penetration tests: black-box, white-box, and grey-box:

- **Black-box Assessment:** A client provides no information prior to the start of testing
- **White-box Assessment:** The entity may provide the penetration tester with full and complete details of the network and applications
- **Grey-box Assessment:** The entity may provide partial details of the target systems

PCI DSS penetration tests are typically performed as either white-box or grey-box assessments. These types of assessments tend to yield higher levels of accurate results and provide a more comprehensive test of the security posture of the environment than a pure black-box assessment. Performing a black-box assessment – when the entity provides no details of the target systems prior to the start of the test – may require more time, money and resources for the deliverables to meet the requirements of PCI DSS.

DRUMMOND

Pen Test Checklist

This list provides guidance to ensure you are compliant with penetration testing requirements, per PCI DSS Requirement 11.3:

1) Pen tests must be performed annually (at least) and upon significant changes to the cardholder data environment (CDE). (Examples of significant changes include infrastructure upgrades, application upgrades, operating system upgrades or new system component installations)
2) Pen tests must be performed by a qualifies internal resource, or qualified external third party
3) If an internal resource is used to perform the pen test, organizational independence must be verified (e.g., those responsible for managing the CDE cannot also pen test the CDE)
4) Pen tests must include a manual process that may include use of vulnerability scanning or other automated tools, resulting in a comprehensive report
5) Pen tests must include network-layer testing
6) Pen tests must conduct application-layer testing
7) Pen tests must include review and consideration of threats and vulnerabilities experienced in the last 12 months
8) The scope of the pen test must include the entire CDE external perimeter (public-facing attack surfaces). This also applies to remote access vectors, such as dial-up and VPN connections
9) The scope of the pen test must include the entire CDE internal perimeter (LAN-LAN attack surfaces), as well as critical systems within and outside of the CDE (critical systems are those involved in the processing or protection of cardholder data)
10) Internal pen testing must include all system components and applications in the CDE, as well as any "Connecting To" systems. Additional systems provide "Shared Services" deemed "in scope" because they impact the security of the CDE
11) Identified exploitable vulnerabilities must be corrected and repeat testing must be performed to confirm the vulnerability was corrected
12) If segmentation is used to isolate the CDE from out-of-scope networks and systems, the pen test must include testing all segmentation controls/methods in use to confirm that the segmentation methods are working as intended and that all out-of-scope systems and networks are completely isolated from systems in the CDE
13) If you are a service provider and use segmentation to isolate the CDE, segmentation pen testing must be performed at least every six months

Reduce your risk today!

For more information about our penetration test solutions and services or to receive a quote, please contact us at ***sales@drummondgroup.com***

DRUMMOND