BLUE GOAT CYBER

Penetration Testing Services for **PCI Compliance**

Steps to Schedule Your PCI Penetration Test:

- Schedule a 30-minute Discovery Session
- We determine IF and HOW we can help
- We provide a Tailored Proposal
- Together, we review the Proposal

PCI DSS stands for Payment Card Industry Data Security Standard. It's the rulebook that governs how customer card data gets managed. Recently, it was adapted to require both a vulnerability scan and a pen test. The vulnerability assessment and penetration test must include the perimeter of the Cardholder Data Environment (CDE) and any systems which, if compromised, could impact the security of the CDE. Penetration tests must be performed at least once annually and every six months for service providers.

Penetration Testing assesses the controls used to protect the CDE for PCI DSS.

Specifically, PCI DSS 3.2 distinguishes between a vulnerability scan (Requirement 11.2) and a penetration test (Requirement 11.3), both of which are required for PCI DSS compliance. PCI DSS Requirement 11.3.4.1 requires an organization to perform penetration testing on CDE segmentation controls every six months. The PCI Security Standard Council's guidance states organizations should:

Examine the results from the most recent penetration test to verify that:

- Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods.
- The penetration testing covers all segmentation controls/methods in use.
- The penetration testing verifies that segmentation controls/methods are operating and effective and isolate all out-of-scope systems from systems in the CDE.
- Verify that the test was performed by a qualified internal resource or a qualified external third party and, if applicable, the organizational independence of the tested exists (not required to be a QSA or ASV)

Although PCI DSS only specifies a penetration test every 180 days, we recommend a quarterly program that includes validation testing.

METHODOLOGY

We follow a seven-phase methodology designed to maximize our efficiency, minimize risk, and provide complete and accurate results. The overarching seven phases of the methodology are:

- Planning and Preparation
- Reconnaissance / Discovery
- Vulnerability Enumeration / Analysis
- Initial Exploitation
- Expanding Foothold / Deeper Penetration
- Cleanup
- Report Generation

BENEFITS / RETURN ON INVESTMENT (ROI)

It is better to have an ethical hacker find the holes in your healthcare environment than an adversary. Our PCI Penetration Testing Services provide details on exploitable vulnerabilities in a prioritized, tangible manner. Our report allows you to understand better what your environment looks like from an attacker's perspective; what the "attack surface" looks like. This helps you prioritize efforts to mitigate risk to reduce data breach likelihood.

Not only do our PCI Penetration Testing Services show you what your attack surface looks like to an adversary, but they can also be used as a safe way to test your organization's incident response capabilities. Our Penetration Testing services can also be used to tune and test your security controls, such as your IDS, Firewall, Web Application Firewall (WAF), Router Access Control Lists (ACLs), etc.

DELIVERABLE

The PCI Penetration Test Report includes URLs tested, vulnerabilities discovered, steps taken during the assessment, exploitable areas discovered, and prioritized recommendations. For any systems we exploit, an "Attack Narrative" section is used to discuss step-by-step the process we used to gain access, escalate privileges, etc.

Blue Goat Cyber
PO Box 20310
PMB 45092
Cheyenne, Wyoming 82003-7007

(307) 317-8884
info@bluegoatcyber.com