PCI DSS Penetration Testing

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

The Compliance Requirement - And More

Since 2015, Payment Card Industry Data Security Standards (PCI DSS) Requirement 11 mandates any company that processes, stores, or transmits electronic card transactions is required to perform a yearly PCI Penetration Test. You are also required to perform this type of testing if there are any significant changes to your network infrastructure. Beyond the compliance requirements, your company wants and needs to protect your customer data. If an attacker were able to get to this sensitive information, it could be devastating to your business and your reputation.

Tried and True Testing

Our PCI Penetration Testing involves a network scan for vulnerabilities, followed by manual testing that mimics a real-world attack on your cardholder data environment. If you've recently had a change to your network, we can help ensure that any controls in place are working effectively after the upgrade or migration. To show improvement, our PCI Penetration Testing engagements include a retest once you've completed remediation on vulnerabilities found the first time around.

To prove compliance, you must be able to show your Qualified Security Assessor (QSA) that penetration testing has been completed by a qualified external third party or by qualified internal resources. Our PCI DSS Penetration Test provides a PCI-accepted independent internal penetration test, external penetration test, wireless segmentation test (when applicable), and application test (when applicable) of your organization's cardholder data environment.

PCI DSS Penetration Testing Includes:

- **Engagement Interview**
- **Network Documentation Collection**
- **Network Scope**
- **Segmentation Checks**
- **Application and Network Testing**
- **Immediate Notification of Critical Risks and/or Encountered Cardhodler Data**
- **Post-Engagement Retesting and Environment Clean-Up**

Frequently Asked Questions

What is the difference between vulnerability scanning and penetration testing?

Vulnerability Scanning is an automated method that identifies vulnerabilities that may exist on an organization's network. Penetration testing is by nature more accurate than vulnerability scanning since it actually confirms that a suspected weakness is exploitable.

Will this hurt my network?

This is extremely unlikely. We very rarely have any reported problems. We do not attempt any denial of service attacks.

What information does my core provider or IT MSP need to provide during the scoping call?

IP addresses of external interfaces, best times for the automated scans, white-listing process for our IPs, contact information, and domain lockout policy so that we can mitigate the risk of locking out domain users during testing up front. For the internal network, any network devices that touch PCI data should be identified and provided for the test.

Are the vulnerability scan results included in the report?

No. If scan results were included, it would be a very long report and there is really no reason to include them. We will often take a screenshot to show the client scans were run and sometimes the specific vulnerability that we were able to exploit.

What is the Information Security Analyst looking for?

We are looking for system and service level vulnerabilities which can potentially be exploited on systems that can be accessed from the public internet. These vulnerabilities could include out-of-date software versions, insecure system configurations, or other technical flaws. The goal is to identify these exploitable vulnerabilities by attempting to compromise these systems using real-world techniques and provide subsequent recommendations on how to mitigate the confirmed attack methods.

What if x hour(s) of testing isn't enough? Do you stop at x hour(s) if you are still finding things?

We do our best to work with you upfront to identify how long testing will take. If after the ISA runs their initial port and networking scans and finds a lot more open ports than expected, or is in the middle of testing and realizes they will need significantly more time, they will contact you and arrangements can be made to extend the service.