PENETRATION TESTING

as defined by PCI DSS Requirement 11.3
and PCI's Guidance Document

Goal 1:
To determine if and how a malicious user can gain unauthorized access to assets that affect the security of a system, files, and/or cardholder data

Goal 2:
To confirm that the applicable controls required by PCI DSS (vulnerability management, methodology, scope, and segmentation) are in place

COMPONENTS

EXTERNAL PENETRATION TESTING

tests external perimeter of CDE* and critical systems
required for PCI DSS compliance

INTERNAL PENETRATION TESTING

tests internal perimeter of CDE* and critical systems
required for PCI DSS compliance

APPLICATION / NETWORK LAYER TESTING

tests for security defects from app design, configuration, software implementation, usage, or maintenance
required for PCI DSS compliance

SEGMENTATION CHECKS

validates that segmentation controls are operational and effectively isolate out-of-scope systems from CDE* systems
required for PCI DSS compliance

SOCIAL ENGINEERING

identifies risks associated with end users' failure to follow documented policies and procedures
highly recommended by the PCI Council

*CDE is the Cardholder Data Environment:
the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data

DARA SECURITY