SECTION 31
SECURITY

AUTONOMOUS PENETRATION TEST · HYBRID

PCI DSS v4.0 — Penetration Test Report

Tessier-Ashpool S.A. · ENG-2026-0353

VERSION	v1.1
GENERATED	August 19, 2026
PREPARED FOR	Tessier-Ashpool S.A.

PENETRATION TEST REPORT

PCI DSS v4.0 Requirement 11.4 — Conformance

This report documents that the penetration test performed for **Tessier-Ashpool S.A.** provides evidence toward PCI DSS v4.0 Requirement 11.4. It is provided as evidence for the entity's assessor; it is a penetration test report, **not** a formal attestation, certification, or audit opinion — Section 31 Security is the independent testing provider, not the entity's assessor, QSA, or ASV.

ENTITY	Tessier-Ashpool S.A.	TESTING WINDOW	2026-07-25 – 2026-08-08
TESTER	Section 31 Security	INDEPENDENCE	Organizationally independent third party

SCOPE

Cardholder Data Environment (CDE)

In-scope Cardholder Data Environment: the AWS account hosting the Freeside payments stack, including the S3 bucket designated for cardholder data. Connected-to and security-impacting systems in scope: the tashpool.local Windows domain (10.100.10.0/24) and its domain controllers, whose credentials govern access to that environment, and the internet-facing booking application, which holds network reachability into the cloud tenancy.

ENGAGEMENT

Methodology & Scope

METHODOLOGY	Hybrid Penetration Test	APPROACH	Black Box
ENGAGEMENT WINDOW	July 25, 2026 → August 8, 2026	PRIMARY TARGET	tashpool.local

Scope & Limitations

- This assessment is a **point-in-time** evaluation; findings reflect the environment during the engagement window and may not account for later changes.
- Testing prioritized demonstrable impact over exhaustive enumeration — the absence of a finding is not proof that no weakness exists.

REQUIREMENT 11.4

Requirement Coverage

Ref	Requirement	Status	Evidence
11.4.1	Documented penetration testing methodology	Met	Industry-accepted methodology (NIST SP 800-115 / PTES) covering the in-scope boundary and critical systems, with application- and network-layer testing.
11.4.2	Internal penetration testing	Met	Internal testing performed by Section 31, an organizationally independent third party.
11.4.3	External penetration testing	Met	External testing performed by Section 31, an organizationally independent third party.
11.4.4	Exploitable findings corrected and retested	Partial	No corrections have yet been verified by retest; all 22 exploitable findings remain open.
11.4.5	Segmentation control testing	Met	Segmentation controls were tested and found ineffective. No control prevented movement from the internet-facing application tier into the cloud tenancy holding cardholder data, or onward into the corporate Windows domain; all three were traversed from an unauthenticated external position with no segmentation boundary encountered. The environment is effectively flat with respect to the Cardholder Data Environment.

FINDINGS

Exploitable Findings & Remediation

Severity	Finding	Status
CRITICAL	SSRF → IMDS Credentials Extracted (AWS role cg-ec2-role-cgidlft30u2hpk)	Open
CRITICAL	ADCS ESC8 cert captured for DC1$@TASHPOOL.LOCAL — cross-host coerce → CA	Open
CRITICAL	ADCS ESC8 cert PKINIT-authenticated — DC machine-account NT hash recovered, DCSync-capable	Open
CRITICAL	DCSync exploited via dc1$@tashpool.local → 19 domain hashes extracted (incl. krbtgt)	Open
CRITICAL	Domain Admin compromise proven on tashpool.local via DCSync	Open
CRITICAL	Credential Grants WinRM Administrative Access	Open
CRITICAL	Credential Reuse Confirmed on 1 Host	Open
CRITICAL	AD CS Web Enrollment Permits NTLM Relay (ESC8)	Open
CRITICAL	Credential Extracted from S3 Object (cg-cardholder-data-bucket-cgidlobnfe01ce/ops/straylight-vpn/domain-join-readme.txt)	Open
CRITICAL	Cloud-Sourced Credential Validated Against On-Prem AD	Open
CRITICAL	Server-Side Request Forgery to Cloud Metadata	Open
HIGH	ADIDNS write viable (TASHPOOL.LOCAL) — domain-wide wildcard/WPAD poisoning possible	Open
HIGH	Credential Reuse Chokepoints (2)	Open
HIGH	NTLM → LDAP relay VIABLE — coerce → relay → RBCD path is live	Open
HIGH	Schema Admins Group Non-Empty (1 Non-Default Member(s): tashpooladm)	Open
HIGH	Privileged Accounts Lack Both Protected Users + AuthN Policy	Open
HIGH	Weak Active Directory Password Policy	Open
HIGH	S3 Account-Level Block Public Access Not Fully Enabled (CIS 1.20)	Open
HIGH	AWS Config Not Enabled in Region (us-east-1)	Open
HIGH	AWS Config Required Baseline Rules Missing	Open
HIGH	Reflected Cross-Site Scripting	Open
HIGH	Windows Authentication Endpoint Exposed	Open

Exploitable vulnerabilities are corrected per the entity's risk assessment and verified by retest; remediation and retest status is tracked across report versions.

SEGMENTATION

Segmentation Control Testing

Segmentation controls were tested and found ineffective. No control prevented movement from the internet-facing application tier into the cloud tenancy holding cardholder data, or onward into the corporate Windows domain; all three were traversed from an unauthenticated external position with no

segmentation boundary encountered. The environment is effectively flat with respect to the Cardholder Data Environment.