AUTONOMOUS PENETRATION TEST · HYBRID

Executive Summary

Tessier-Ashpool S.A. · ENG-2026-0353

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

CONFIDENTIAL — Tessier-Ashpool S.A. & Section 31 Security

EXECUTIVE SUMMARY

Engagement Outcome & Narrative

Full Domain Compromise

13 stages demonstrated

4m 38s	22	30
TIME TO DOMAIN ADMIN	CRITICAL + HIGH	TOTAL FINDINGS

Between July 25 and August 8, 2026, our team conducted an adversarial security assessment of Tessier-Ashpool S.A.'s environment, targeting the tashpool.local domain and associated cloud infrastructure. The assessment simulated a realistic external attacker with no prior knowledge or credentials. The results are severe: testers achieved full administrative control over Tessier-Ashpool's entire Windows domain, accessed cloud storage containing sensitive credentials, and extracted every password and authentication secret held in the company's identity systems — a total of 19 credential records including the master key used to authenticate every user and system in the organization.

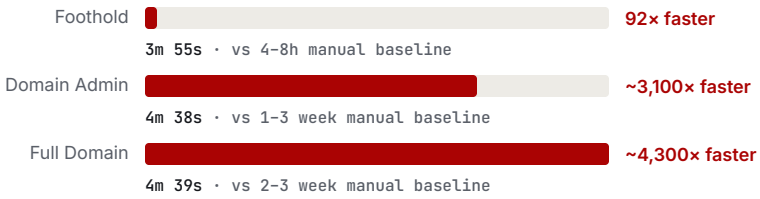
The attack began through a publicly reachable web application that could be tricked into making requests on an attacker's behalf to Amazon's internal cloud management service. This gave testers temporary cloud credentials, which they used to access a cloud storage bucket labeled for cardholder data. Inside that bucket, a plain-text password file intended for VPN domain-join operations was discovered. That password worked directly against Tessier-Ashpool's on-premises directory — meaning a single misconfigured web application created a bridge from the public internet straight into the internal network. From there, a series of misconfigured certificate and authentication services allowed testers to impersonate the domain controller itself, replicate every credential in the directory, and confirm administrative access across multiple internal systems.

The organization faces 11 critical-severity and 11 high-severity findings across its cloud and on-premises environments, with no significant barriers encountered at any stage of the attack. The credentials stolen include the Kerberos master key (krbtgt), which — if compromised by a real attacker — would allow forged authentication passes for any user or system for an extended period, even after passwords are reset, unless a specific and deliberate remediation process is followed. The breadth of access achieved means a real-world attacker could exfiltrate all data, disrupt all operations, deploy ransomware, or conduct fraud entirely undetected.

The findings carry direct regulatory exposure. The storage bucket involved is named for cardholder data, and the combination of unencrypted credential storage, lack of transport enforcement, and

absent monitoring controls represents a probable failure state under PCI DSS, and potentially GDPR if personal data is co-located. Tessier-Ashpool should treat this assessment as confirmation of an active material risk to business continuity, customer data, and regulatory standing. Immediate action on the priority recommendations below is strongly advised before any further delay.

Engagement Tempo vs. Manual Baseline



Business Impact

- **CRITICAL** Complete takeover of the company's identity and access system means every user account, every server, and every internal application can be accessed or impersonated by an attacker — equivalent to handing over every key to every lock in the organization simultaneously.
- **CRITICAL** A plain-text password stored in a cloud storage bucket labeled for cardholder data created a direct path from the public internet to the internal network, representing a probable PCI DSS breach-disclosure and regulatory-penalty trigger if the same path was used by a malicious actor.
- **CRITICAL** The Kerberos master key (krbtgt) was extracted, meaning a real attacker could issue their own authentication passes for any account for weeks or months without detection, surviving even a full password reset cycle unless a specific multi-step remediation is performed.
- **CRITICAL** A web application vulnerability gave external attackers access to internal cloud credentials, demonstrating that a customer-facing service is a direct gateway to the company's cloud and on-premises infrastructure, placing all hosted data and services at risk.
- **HIGH** Absent cloud configuration monitoring and storage safeguards mean Tessier-Ashpool would not be alerted to data exposure or resource misuse in its AWS environment, leaving any breach — or ongoing attacker presence — invisible to the security and operations teams.
- **HIGH** Weak Active Directory password controls and absent account-protection policies for privileged users lower the effort required for any authenticated attacker or malicious insider to escalate privileges, broadening the population of threats the organization faces.

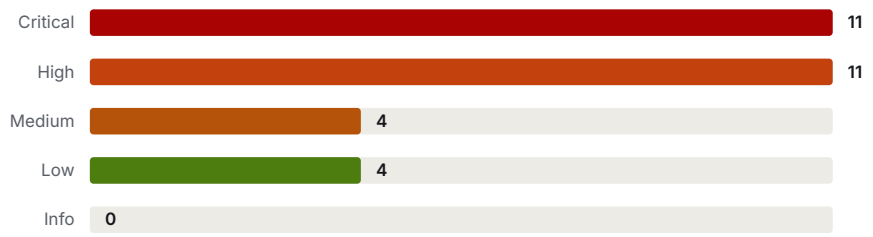
Priority Recommendations

1. **Rotate All Stolen Credentials and Perform Full krbtgt Reset** Immediately reset the krbtgt account password twice (with a waiting period between resets), reset all 19 extracted domain account credentials, and revoke any AWS temporary credentials issued to the compromised EC2 role. This is a prerequisite before any other remediation has meaningful effect, as attackers holding these secrets can bypass most other controls.
2. **Remediate the SSRF Vulnerability on the Public Web Application** Remove or restrict the server-side request capability that allowed access to the cloud metadata service; enforce an allow-list of permitted

outbound destinations and block access to the 169.254.169.254 metadata endpoint from all application-tier hosts. This closes the external entry point that initiated the entire attack chain.

3. **Fix the ADCS ESC8 Misconfiguration on the Certificate Authority** Enforce Extended Protection for Authentication (EPA) and require HTTPS with channel binding on all certificate enrollment web endpoints, and enable LDAP signing and channel binding on domain controllers. This eliminates the relay path that allowed the domain controller's identity to be stolen.
4. **Remove Plaintext Credentials from Cloud Storage and Enforce Encrypted Transport** Audit all S3 buckets for stored secrets, remove any credentials or sensitive configuration files found, replace them with a secrets-management service, and enforce SecureTransport-only bucket policies. Enable account-level Block Public Access as an additional safety net.
5. **Enable AWS Config and Deploy Continuous Compliance Monitoring** Turn on AWS Config in all active regions and deploy the baseline CIS rule set so that storage misconfigurations, public-access exposures, and credential issues are detected automatically and alerted in real time rather than discovered only during periodic assessments.
6. **Harden Active Directory Privileged Account Controls** Add all privileged accounts to the Protected Users security group and assign authentication-policy silos, empty the Schema Admins group of standing members, and enforce a password policy that meets current length and complexity baselines. These steps reduce the blast radius if any privileged credential is compromised in the future.

OVERVIEW

Findings Overview

30 findings by severity