SANITIZED SAMPLE / ACTUAL ENGAGEMENT

Penetration test report

Assessment: External and internal network penetration test
Client: Anonymized organization
Assessment window: 10 business days
Original report: June 2025
Editorial revision: 08 September 2026

This is a sanitized sample from a real Exploit Technology engagement. Client identifiers and operational evidence are not included in this public edition. The editorial revision does not represent a new test or a remediation retest.

Executive summary

Exploit Technology conducted an independent penetration test to evaluate the effectiveness of security controls protecting externally accessible systems and internal network resources. Testing focused on connected attack paths.

Perimeter defenses were generally effective. However, credential exposure and insufficient internal access controls enabled an attack path to internal resources and sensitive systems. No evidence of active compromise was identified at the time of testing.

Overall risk rating: Moderate
The original assessment identified credential reuse across internal systems, excessive access permissions, and insufficient detection of lateral movement as risk drivers.

Finding	Severity	Detail
F01 · Credential exposure leading to internal network access	High	Page 3
F02 · Excessive internal privileges enabled lateral movement	Medium	Page 4
F03 · Limited detection of internal attack activity	Medium	Page 5

Original framework labels: PCI DSS v4.0; NIST SP 800-171 / SP 800-53. The source did not specify NIST revisions. Supplemental references added to this edition appear on pages 7–8; they do not change the original assessment baseline.

01 / SCOPE & METHODOLOGY

Scope and attack path

Assessment scope

In scope	Out of scope
Public-facing web applications; VPN and authentication services; internal Active Directory environment; limited sample of internal user workstations.	Denial-of-service testing; social engineering; physical security testing.

Methodology

Testing followed an adversary-emulation approach: an external attacker attempting to gain unauthorized access and escalate privileges. Activities included external reconnaissance, authentication and access-control testing, credential-exposure validation, internal lateral movement simulation, and privilege-escalation attempts. Findings were validated through exploitation where appropriate and documented with supporting evidence.

Observed attack path

• External service enumeration identified exposed authentication endpoints.

• Valid credentials were obtained through indirect exposure, without brute force.

• VPN access was achieved using those credentials.

• Internal network access enabled lateral movement.

• Excessive role permissions allowed privileged access to sensitive systems.

The path shows how credential exposure, excessive permissions, and detection gaps combined into material risk. The individual findings retain the High and Medium ratings in the original report.

Public-sample limits. This edition does not include the target inventory, exact test dates, account identifiers, commands, or raw evidence. Evidence categories from the source are retained on the finding pages. The underlying artifacts were not revalidated during this editorial revision.

02 / FINDING F01 · HIGH

Credential exposure leading to internal network access

Severity: High **Status:** Open in the original report

Description and impact

Testing identified valid user credentials exposed through an external system not protected by multi-factor authentication. These credentials allowed successful authentication to internal resources.

An external attacker could gain internal network access without triggering alerts. The documented access path used valid credentials to traverse the remote-access boundary.

Evidence recorded in the source

• Successful authentication logs

• VPN session establishment

• Internal resource access confirmation

These are evidence categories, not reproduced logs. The public sample contains no passwords, account identifiers, or raw session records.

Remediation recommendations

• Enforce MFA on externally accessible authentication services and review credential exposure risks across third-party platforms.

• As part of remediation, revoke or rotate exposed credentials and review associated sessions or tokens as appropriate to the exposure. Confirm the affected authentication paths and any policy exceptions.

Verification after remediation

Repeat authorized checks to confirm that exposed credentials no longer grant access and that the intended authentication policy is enforced. Record the systems tested, results, and residual exceptions. No completed retest is asserted in this sample.

Original references: PCI DSS v4.0 Requirements 8 and 11; NIST IA, AC, and CA families. Supplemental finding-level references are on page 7.

03 / FINDING F02 · MEDIUM

Excessive internal privileges enabled lateral movement

Severity: Medium **Status:** Open in the original report

Description and impact

Internal testing identified multiple user accounts with access exceeding operational requirements, allowing lateral movement between systems. An attacker with initial internal access could expand control and access sensitive systems without exploiting a software vulnerability.

Evidence recorded in the source

• Access-control listings

• Privilege-inheritance paths

• Lateral-access confirmation

Raw access listings and account or resource identifiers are not included in this public sample.

Remediation recommendations

• Implement least-privilege access reviews and monitor lateral authentication attempts.

• Correct unnecessary group membership, direct permissions, or inherited privileges after checking operational dependencies. Establish ownership for reviewing subsequent access changes.

Verification after remediation

Repeat the authorized access checks using the affected roles. Confirm that unapproved access is denied while legitimate workflows remain available. Record the specific resources checked and any remaining exceptions. No completed retest is asserted in this sample.

Original references: PCI DSS v4.0 Requirement 7; NIST AC and RA families. Supplemental references are on page 7. The finding addresses permissions; a full segmentation conclusion requires the relevant boundary-test evidence.

04 / FINDING F03 · MEDIUM

Limited detection of internal attack activity

Severity: Medium **Status:** Open in the original report

Description and impact

Security monitoring controls did not generate alerts for lateral movement or privilege-escalation activity during testing. A detection gap of this kind could allow an attacker to operate internally for longer before investigation.

Evidence presentation

Supporting alert records, event timestamps, and screenshots are not included in this public sample. The reported observation is retained from the original assessment.

Remediation recommendations

• Enhance internal logging and alerting, and validate detection through periodic adversarial testing.

• Determine whether the gap lies in event collection, detection logic, alert routing, or operational review. Correct the relevant configuration or workflow and make alert ownership explicit.

Verification after remediation

Repeat the authorized scenario and record the test event, observation window, telemetry sources, and expected alert. Confirm that the event is collected, the alert reaches its intended destination, and the designated team can respond. No completed retest is asserted in this sample.

Original references: PCI DSS v4.0 Requirement 10; NIST AU and CA. The CA family name is Assessment, Authorization, and Monitoring; CA-7 is the specific Continuous Monitoring control. The original abbreviated label has been corrected. See page 7 for supplemental references.

05 / ORIGINAL RISK SUMMARY & HANDOVER

Risk summary and next steps

Risk areas reported in the original assessment

Risk area	Original observation
External perimeter	Generally effective
Credential hygiene	Needs improvement
Internal segmentation	Weak
Detection and response	Limited

The original overall rating remains Moderate. The table preserves the source report's conclusions; this public sample does not include the evidence needed to independently reassess those conclusions or their aggregation.

Conclusion

The assessment found that security controls were present, but their effectiveness under real attack conditions was inconsistent. Correcting the identified weaknesses is intended to reduce the risk of successful compromise and improve the technical evidence available for assessment review.

Remediation handover

Agree an owner and target date for each corrective action. Record changes, supporting evidence, and retest results before closing a finding. Where an exception remains, document it through the organization's risk process.

The Open statuses in this document describe the June 2025 report, not the organization's current remediation state. No later remediation status or new test result has been added.

Independent technical validation

A penetration test supports an assessment by providing technical findings. This sample does not certify compliance, guarantee an audit outcome, or establish that the environment is free of compromise.

06 / SUPPLEMENTAL FRAMEWORK REFERENCES

Finding-level control references

Added in the September 2026 editorial revision. These references explain relationships to current reference editions; they do not assert that the June 2025 assessment tested these versions or that a requirement was satisfied or failed.

ID	PCI DSS v4.0.1	NIST SP 800-53 Rev. 5	Relationship and condition
F01	8.4.3	IA-5 · Authenticator Management	Remote access from outside the network that could access or impact the cardholder data environment (CDE) needs MFA. IA-5 addresses authenticator management. Confirm the actual access path and PCI scope.
F02	7.2.2	AC-6 · Least Privilege	User access should follow job duties and necessary privileges. Relate actual excess access to the approved role and affected resources.
F03	10.4.1.1	AU-6 · Audit Record Review, Analysis, and Reporting; SI-4 · System Monitoring	Automated audit-log review and monitoring relate to the detection workflow. A missed alert alone does not establish absence or noncompliance of a required review mechanism.

Limits. Detailed assessment mappings need the applicable revision, evidence references, rationale, and scope. These are selected relationships, not exhaustive tests or a compliance crosswalk. No CDE boundary is defined in the source sample.

Other frameworks

The original report named SP 800-171 without a revision. No new SP 800-171 mapping is added because the applicable CUI context and revision have not been established. No HIPAA, ISO, or SOC 2 compliance or equivalence is asserted. NIST control references can inform healthcare security discussions, but are not a substitute for a scoped healthcare assessment.

07 / SUPPLEMENTAL PCI CONTEXT & SOURCES

Testing requirements and assessment boundaries

PCI DSS v4.0.1 references below support future scoping and report review. They do not replace the original v4.0 label, establish a historical baseline, or demonstrate completion of Requirement 11.4. This is a focused guide, not a complete checklist.

Requirement	What an applicable live engagement must address
11.4.1	A documented and implemented methodology, including required coverage, internal/external perspectives, relevant attack layers, and segmentation validation where applicable.
11.4.2 / 11.4.3	Internal and external testing under the defined methodology, required frequency/change triggers, qualified resources, and organizational independence.
11.4.4	Risk-based correction of exploitable weaknesses and repeat testing to verify corrections.
11.4.5	Testing of CDE segmentation where segmentation is used, including applicable methods and boundaries. Additional service-provider requirements may also apply.

The public sample does not include a full CDE inventory, complete timing records, tester-qualification evidence, or remediation retest. A testing guide such as OWASP WSTG is a methodology resource, not a compliance control; this revision does not claim a WSTG test suite was performed.

Primary references

PCI SSC document library: PCI DSS v4.0.1
NIST SP 800-53 Rev. 5: control catalog and mapping limitations
PCI SSC: v4.0.1 publication and v4.0 retirement notice

Discuss an assessment: Exploit Technology · (657) 877-3274