LFMSecurity

CLIENT CONFIDENTIAL

Internal Security Assessment Report

Acme Example Co.

ENGAGEMENT ID	SAMPLE-INT-001
ASSESSMENT TYPE	Internal Security Assessment
ASSESSMENT DATES	2026-05-13 to 2026-05-15
REPORT DATE	2026-05-18
PREPARED BY	LFMSecurity
CLASSIFICATION	Client Confidential

Executive Risk Snapshot

Acme Example Co. engaged LFMSecurity to perform a fixed-scope Internal Security Assessment review. The assessment objective was to identify practical security issues within the approved scope and provide evidence-backed remediation priorities. This package is a mock sample generated from local files; no live testing is represented.

Executive Dashboard

Assessment posture, finding count, and remediation priorities.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	0	2	0	0

Priority Actions

1. Assign a business owner, reduce write access to the smallest practical group, separate read-only and write-capable roles, and enable change monitoring.
2. Disable legacy protocols where business requirements allow, require signing or encryption for administrative protocols, and document compensating controls for
3. Complete owner review and confirm remediation priorities.

Key Findings Snapshot

FW-INT-SAMPLE-001 | Medium Broad Write Access On Shared Operations Folder	\\\\fileserver01\\operations
FW-INT-SAMPLE-002 | Medium Legacy Protocol Exposure On Internal Servers	10.10.20.0/24

Table Of Contents

Executive Summary

Acme Example Co. engaged LFMSecurity to perform a fixed-scope Internal Security Assessment review. The assessment objective was to identify practical security issues within the approved scope and provide evidence-backed remediation priorities. This package is a mock sample generated from local files; no live testing is represented.

The report includes 2 finding(s): Medium 2.

Key Findings

ID	SEVERITY	TITLE	AFFECTED ASSET	ASSESSMENT AREA
FW-INT-SAMPLE-001	Medium	Broad Write Access On Shared Operations Folder	\\\\fileserver01\\operations	Shares And Permissions
FW-INT-SAMPLE-002	Medium	Legacy Protocol Exposure On Internal Servers	10.10.20.0/24	Internal Exposure Review

Priority Actions

1. Assign a business owner, reduce write access to the smallest practical group, separate read-only and write-capable roles, and enable change monitoring.
2. Disable legacy protocols where business requirements allow, require signing or encryption for administrative protocols, and document compensating controls for exceptions.
3. Complete owner review and confirm remediation priorities.

Scope And Objectives

Objective

Assess internal security posture across approved networks, identity systems, and access controls, with emphasis on misconfigurations that could increase blast radius after account or workstation compromise.

Scope

Anything not explicitly listed as in scope was not included in this assessment. The report is limited to the approved assets, testing windows, and test classes.

ASSET	TESTING NOTES

Internal range: 10.10.20.0/24	Approved in-scope asset

Testing Windows

WINDOW	NOTES
2026-05-13 09:00-17:00 America/New_York	Approved testing window

Methodology

Internal Security Assessment reviews evaluate approved internal networks, identity controls, and configuration exposure from authorized internal vantage points. Coverage typically includes internal inventory, exposed services, weak protocols, share and permission review, Active Directory posture, patch and configuration exposure, and only explicitly approved identity attack-path modules.

PHASE	COVERAGE
Preparation	Confirm approved internal ranges, access method, test account constraints, optional modules, exclusions, stop conditions, and data handling requirements.
Internal inventory	Review reachable systems, exposed services, identity context, and security-relevant configuration exposure.
Control review	Review weak protocols, risky shares, permissions, AD posture, privileged access patterns, and approved attack-path analysis modules.
Risk analysis	Rank findings by blast radius, privilege exposure, operational impact, and remediation sequencing.
Reporting	Document evidence-backed findings, prioritized hardening actions, and validation criteria.

Standards And References

- CIS Controls for inventory, access control, vulnerability management, and audit logging.
- Microsoft security baselines and Active Directory hardening guidance where applicable.
- Client-approved Rules of Engagement for optional identity attack-path modules.

Assessment Summary

Internal Security Assessment testing identified the findings and remediation priorities below. The assessment did not expand beyond the approved assets, and evidence was limited to sanitized observations needed to support each issue.

Risk Summary

SEVERITY	COUNT
Critical	0
High	0
Medium	2
Low	0
Informational	0

Findings

Shares And Permissions

Finding ID: FW-INT-SAMPLE-001: Broad Write Access On Shared Operations Folder

Severity: Medium

Affected asset: \\\\fileserver01\\operations

Summary

A fictional internal file share grants write access to a broad staff group instead of a smaller business-owner group.

Business Impact

Broad write access increases the blast radius of accidental changes, ransomware activity, or compromised internal accounts, especially when operational documents or automation inputs are stored in the share.

Evidence

Evidence item EV-INT-001 contains a sanitized permissions listing with group names generalized. No

file contents, customer records, credentials, or personal data are included.

Remediation And Validation

Assign a business owner, reduce write access to the smallest practical group, separate read-only and write-capable roles, and enable change monitoring. Validate that the approved write-capable group is limited to intended owners and ordinary staff accounts have only the required access level.

References

- CIS Controls account and access management guidance.
- Microsoft file share and NTFS permission management guidance.

Internal Exposure Review

Finding ID: FW-INT-SAMPLE-002: Legacy Protocol Exposure On Internal Servers

Severity: Medium

Affected asset: 10.10.20.0/24

Summary

The fictional internal range includes systems with legacy protocol exposure that can weaken authentication protections and increase relay or downgrade risk when combined with other weaknesses.

Business Impact

Legacy protocols can increase the impact of a compromised workstation or account by giving attackers more options to move, relay authentication, or target older services.

Evidence

Evidence item EV-INT-002 contains a sanitized service inventory excerpt. The sample does not include credential material, packet captures, hashes, or sensitive host data.

Remediation And Validation

Disable legacy protocols where business requirements allow, require signing or encryption for administrative protocols, and document compensating controls for exceptions. Validate that legacy exposure is removed or restricted on the affected subnet.

References

- CIS Controls secure configuration guidance.
- Microsoft hardening guidance for SMB and legacy authentication.

Conclusion

The highest-priority remediation work should focus on the issues listed in Priority Actions. Closing those items first will reduce the most realistic risk identified during this Internal Security Assessment while preserving a clear path for validation.

Appendix A: Consolidated Remediations

ID	SEVERITY	REMEDIATION PRIORITY
FW-INT-SAMPLE-001	Medium	Assign a business owner, reduce write access to the smallest practical group, separate read-only and write-capable roles, and enable change
FW-INT-SAMPLE-002	Medium	Disable legacy protocols where business requirements allow, require signing or encryption for administrative protocols, and document compensating

Severity Definitions

SEVERITY	DEFINITION
Critical	Issue is likely exploitable and could cause severe business impact, broad compromise, or material data exposure.
High	Issue presents significant risk and should be prioritized quickly, especially if exposed to untrusted users or the internet.
Medium	Issue creates meaningful risk or weakens important controls, but exploitation usually requires additional conditions.
Low	Issue is a hardening gap or limited-impact weakness that should be addressed through normal remediation planning.
Informational	Observation improves security awareness, documentation, or future planning but is not currently a confirmed vulnerability.

Appendix B: Assessment Coverage

ASSESSMENT TYPE	AREAS REVIEWED	EVIDENCE STYLE
Internal Security Assessment	10.10.20.0/24	Sanitized evidence excerpts and screenshot notes where relevant