GRILLI

PENETRATION TEST REPORT

Offensive Security Assessment

Penetration Test Report

Network Infrastructure — Offensive Security Assessment

Document Control

Report reference	GS-PT-2026-0482
Report title	Network Infrastructure Penetration Test — PayNova
Client	the Client (anonymized)
Assessment type	External & internal network penetration test with CDE segmentation validation
Scope (summary)	External perimeter, internal network, and PCI CDE segmentation validation
Testing window	1 June 2026 – 5 June 2026 (5 business days)
Report date (initial issue)	7 June 2026
Final issue (incl. retest)	16 June 2026
Remediation completed	14 June 2026
Retest date	15 June 2026 (24h after remediation)
Document version	1.0 (Final)
Classification	CONFIDENTIAL
Prepared by	Grilli Security — lime@grillisecurity.com

Version History

Version	Date	Author	Notes
0.1	6 June 2026	Lead Consultant	Internal draft
0.9	7 June 2026	Technical Reviewer (QA)	Report delivered (pre-retest) / QA
1.0	16 June 2026	Grilli Security	Final issue incl. retest results

Distribution

This document is classified CONFIDENTIAL and is restricted to the named recipients within the Client organization and their authorized assessors and regulators (e.g. acquiring bank / QSA, where applicable). It must not be redistributed without written consent.

Anonymization note. *This is a sample report. The client name, the platform name (“PayNova”), all hostnames (example domains), IP addresses (RFC 5737 documentation ranges) and evidence have been anonymized or redacted. No real data is contained herein.*

Attestation & Statement of Independence

Grilli Security attests that the penetration test described in this report was performed in accordance with the methodology stated herein (NIST SP 800-115; PTES) by qualified, suitably-certified personnel, and that the assessment team maintained organizational independence from the development and operation of the systems under test, consistent with PCI DSS v4.0 Requirement 11.4.1 (penetration-testing methodology, qualified resources and tester independence).
The findings, severity ratings and conclusions represent the independent professional opinion of the assessment team based on the evidence gathered during the testing window. This attestation supports the Client's PCI DSS Req 11.4 and DORA (Art. 24–25) assurance obligations.

Sign-off

Role	Name / Reference	Date
Lead Penetration Tester	[Anonymized] — OSCP, OSWE, CREST CRT	15 Jun 2026
Technical Reviewer / QA	[Anonymized] — CREST CCT App, OSCP	16 Jun 2026
Authorized by (Grilli Security)	[Anonymized] — Head of Offensive Security	16 Jun 2026

Signatures are held on file in the secure project record; names are anonymized in this sample. Sign-off dates are on or before the final-issue date (16 June 2026).

Table of Contents

1. Executive Summary

1.1 Overview

Grilli Security performed an external and internal network penetration test of the PayNova infrastructure, including explicit validation of the segmentation controls isolating the Cardholder Data Environment (CDE). Testing was conducted between 1 June 2026 and 5 June 2026, following NIST SP 800-115 and PTES, with findings scored using CVSS v4.0.
The assessment identified exploitable perimeter exposures and, most significantly, ineffective segmentation between the corporate network and the CDE, alongside common internal-network weaknesses enabling credential capture and lateral movement. In total, 10 findings were raised.

1.2 Overall Risk Rating

At the time of testing the overall risk was assessed as **CRITICAL**. Following the engagement, the Client remediated all findings; an independent retest (15 June 2026, 24 hours after remediation) confirmed every issue as closed. The post-remediation residual risk is assessed as **LOW**.

1.3 Summary of Findings

Severity	Count	Description
Critical	**3**	Immediate, business-critical exposure or full compromise.
High	**3**	Serious weakness materially increasing breach likelihood or impact.
Medium	**3**	Notable hardening gap to be remediated in the normal cycle.
Low	**1**	Lower-risk best-practice item.
Informational	**0**	Observational; no direct risk.

Total findings: **10** | Status: all remediated and verified at retest.

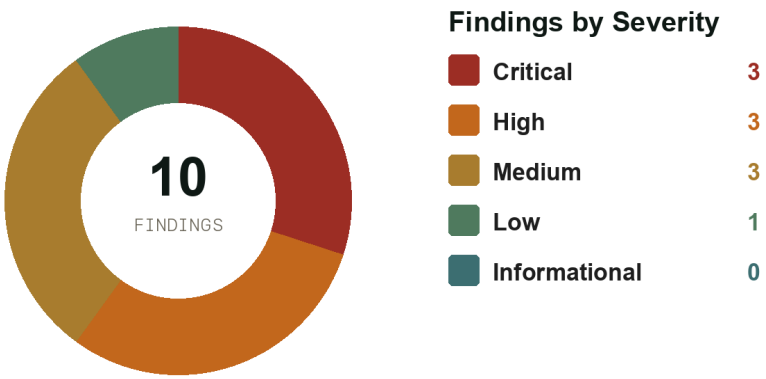

Figure 1 — Findings by severity (n = 10).

Note. *Severity reflects the CVSS v4.0 base-score band, refined by business context and the data sensitivity of affected segments (notably the CDE).*

1.4 Key Risks

- The CDE segmentation could be bypassed (N-03): a standard corporate-VLAN host could reach cardholder-data systems directly — the most significant finding and a PCI scope/containment failure.

- The perimeter was directly attackable (N-01, N-02): an Internet-exposed management interface and an unpatched edge service with a known RCE provided footholds.
- Internal-network weaknesses (N-04, N-05, N-06) enabled credential capture, NTLM relay and device takeover — classic lateral-movement chains.
- Containment was weak (N-07): the CDE permitted unrestricted outbound traffic, easing exfiltration.

1.5 Strategic Recommendations

- Re-establish deny-by-default segmentation around the CDE and validate it on the PCI six-monthly cadence (Req 11.4.6) as a multi-tenant service provider.
- Remove Internet exposure of management planes and enforce a patch SLA for all Internet-facing assets.
- Harden the internal network (disable LLMNR/NBT-NS, require SMB signing, remove default credentials) and add egress filtering from the CDE.

2. Engagement Details

Engagement type	External & internal network penetration test with CDE segmentation validation
Objective	Identify and safely demonstrate network-layer exposures across the external perimeter and internal estate, and validate segmentation controls isolating the PayNova CDE; support PCI DSS and DORA assurance.
Standards & frameworks	NIST SP 800-115; PTES; CVSS v4.0
Compliance drivers	PCI DSS v4.0 (Req 11.4.2, 11.4.3, 11.4.5, 11.4.6); DORA — Reg. (EU) 2022/2554 (Art. 24–25)
Environment	Production-representative network with external (RFC 5737) perimeter and internal/CDE ranges
Approach	External (black-box) perimeter testing followed by authenticated internal testing from a standard corporate-VLAN position
Testing window	1 June 2026 – 5 June 2026 (5 business days)
Retest	15 June 2026 (24 hours after remediation) — all findings re-tested and confirmed closed
Report date	7 June 2026 (initial) · 16 June 2026 (final, incl. retest)
Assessment team	Lead Consultant (OSCP, OSWE, CREST CRT); Consultant (OSCP, eWPTX); Technical Reviewer / QA (CREST CCT App, OSCP)

3. Scope

3.1 In-Scope Assets

Asset	Address / Boundary	Description
External perimeter	203.0.113.0/24	Internet-facing hosts and services
Internal corporate network	192.0.2.0/24	Standard corporate VLAN
Cardholder Data Environment (CDE)	198.51.100.0/24	Segmentation target / in-scope CDE
Network & management devices	various	Firewalls, switches, OOB management

3.2 Out of Scope

- Application-layer testing of the web app and API — covered by the Web Application & API report (GS-PT-2026-0481).
- Denial-of-service and load/stress testing.
- Wireless and physical security.
- Third-party / carrier-managed infrastructure.

3.3 Assumptions, Exclusions & Limitations

- Testing was time-boxed; absence of a finding does not guarantee absence of all vulnerabilities.
- Testing was performed against staging; configuration drift from production is a residual risk to be managed by the Client.
- Destructive actions and bulk data extraction were avoided in line with the Rules of Engagement; exploitation was limited to safe proof-of-concept.
- Findings reflect the state of the assessed systems during the testing window only.

4. Rules of Engagement

- Written authorization was obtained from the Client prior to testing; testing was confined to in-scope assets.
- Testing was conducted against staging during agreed hours, with an emergency contact available throughout.
- No denial-of-service techniques were used; data extraction was limited to the minimum needed to evidence a finding.
- Any critical finding posing immediate risk was reported to the Client without delay (N-01, N-02, N-03 were flagged in real time).
- All test data and evidence are handled per the data-handling terms (Appendix G) and securely destroyed after the retention period.

5. Methodology

5.1 Approach

Testing followed NIST SP 800-115 and PTES: an external (black-box) phase enumerating and validating the Internet-facing perimeter, then an authenticated internal phase from a standard corporate-VLAN host, including explicit validation of segmentation controls isolating the CDE.

5.2 Standards & Frameworks

- NIST SP 800-115 — Technical Guide to Information Security Testing and Assessment (primary)
- PTES — Penetration Testing Execution Standard (engagement structure)
- MITRE ATT&CK — technique classification for internal findings
- CVSS v4.0 — vulnerability severity scoring

5.3 Testing Phases

Phase	Coverage
Discovery	Host/service discovery, OS & service fingerprinting
External perimeter	Internet-facing exposure, management interfaces, remote-access, patch level
Vulnerability validation	Manual confirmation of identified weaknesses (no DoS)
Internal network	LAN attacks (poisoning/relay), credentials, share & service exposure
Segmentation validation	CDE isolation from corporate and other zones; egress filtering
Cryptography	TLS configuration of internal and external services
Lateral movement	Privilege-escalation and pivot-path analysis (PoC only)

5.4 Tooling

nmap, Nessus, testssl.sh, Responder, CrackMapExec, impacket, snmpwalk, ldapsearch and bespoke scripts. All activity was throttled and scoped per the Rules of Engagement; no denial-of-service techniques were used. **Evidence handling.** Findings are evidenced with redacted transcripts and annotated captures (e.g. Figure 3). Full, unredacted evidence — including screenshots — is retained in the secure project record and made available to the Client and, where applicable, the QSA.

5.5 Risk Rating Methodology

Each finding is scored with CVSS v4.0 (base) and assigned a final business risk rating using a likelihood × impact matrix that accounts for data sensitivity and exploitability in context. Severity bands:

Rating	CVSS v4.0	Definition
Critical	9.0 – 10.0	Immediate, business-critical exposure; remediate within days.
High	7.0 – 8.9	Serious weakness; remediate within weeks.
Medium	4.0 – 6.9	Address in the normal remediation cycle.
Low	0.1 – 3.9	Best-practice hardening.
Informational	N/A	Observation with no direct security risk.

Likelihood Ratings

Likelihood	Definition
High	Readily exploitable by a typical attacker with low effort and no special conditions.
Medium	Exploitable with moderate effort, specific preconditions, or some level of privilege.
Low	Difficult to exploit; requires significant effort, chained conditions, or a privileged position.

Risk Matrix (Likelihood × Impact)

Likelihood ↓ / Impact →	Low	Medium	High	Critical
High	Medium	High	Critical	Critical
Medium	Low	Medium	High	Critical
Low	Low	Low	Medium	High

CVSS scope. *Scores are CVSS v4.0 Base metrics; Threat and Environmental metrics were not applied. The final risk rating combines the CVSS base band with the likelihood × impact assessment and the sensitivity of the affected data.*

6. Findings Summary

ID	Finding	Severity	CVSS	Status
N-01	Internet-Exposed Device Management Interface	**Critical**	9.3	**Closed**
N-02	Unpatched Perimeter Service with Known Remote-Code-Execution CVE	**Critical**	9.3	**Closed**
N-03	Inadequate Network Segmentation Between Corporate VLAN and CDE	**Critical**	9.2	**Closed**
N-04	LLMNR / NBT-NS Poisoning Enables Credential Capture	**High**	7.6	**Closed**
N-05	SMB Signing Not Required — NTLM Relay Exposure	**High**	7.6	**Closed**
N-06	Default Credentials on Out-of-Band Management Device	**High**	8.7	**Closed**
N-07	Missing Egress Filtering from the CDE	**Medium**	5.3	**Closed**
N-08	SNMP Default Community String Exposes Configuration	**Medium**	6.9	**Closed**
N-09	Weak TLS on Internal Services	**Low**	2.3	**Closed**
N-10	Anonymous LDAP Information Disclosure	**Medium**	5.3	**Closed**

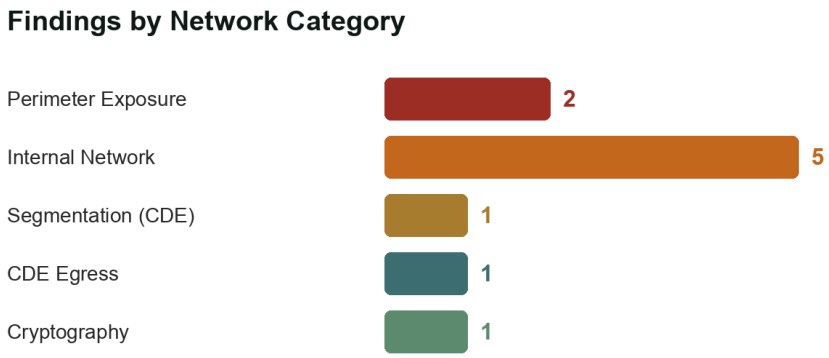

Figure 2 — Findings by network category.

7. Framework Mapping

This mapping shows evidentiary support toward each framework's testing provisions; it is not a certification or attestation.

Findings and methodology map to the testing provisions of the frameworks below using a three-tier status: Directly addresses (a pentest is the named requirement), Provides evidence supporting (a pentest is accepted evidence, not the mandate), and Conforms to (methodology). Items out of this report's scope are marked Separate engagement.

Framework / Requirement	Status	Basis
PCI DSS v4.0 — Req 11.4.2 (internal) & 11.4.3 (external) penetration testing	**Directly addresses**	Internal and external network penetration testing performed to a documented NIST/PTES methodology.
PCI DSS v4.0 — Req 11.4.5 & 11.4.6 (segmentation testing, incl. SP six-monthly cadence)	**Directly addresses**	Segmentation controls isolating the CDE were tested (N-03). As a multi-tenant service provider the Client must repeat segmentation testing at least every six months (11.4.6).
DORA — Art. 24–25 (testing of ICT tools & systems)	**Directly addresses**	Network-layer penetration test feeding the ICT risk-management framework. TLPT (Art. 26–27) is a separate engagement.
ISO/IEC 27001:2022 — A.8.8, A.8.20, A.8.21, A.8.22	**Provides evidence supporting**	Technical-vulnerability management and network security, segregation and security of network services.
NIS2 — Dir. (EU) 2022/2555 Art. 21(2)(e)–(f)	**Supports**	Network security and policies to assess the effectiveness of risk-management measures.
NIST SP 800-115	**Conforms to (methodology)**	The engagement methodology conforms to this recognized testing standard.

7.1 Scope Boundaries & Separate Assessments

- PCI DSS scope: this network report (11.4.2 / 11.4.3 / 11.4.5 / 11.4.6) must be read together with the Web Application & API Penetration Test (GS-PT-2026-0481), which covers application-layer testing (11.4.1). Neither alone satisfies PCI DSS Req 11.4.
- DORA Art. 26–27 (Threat-Led Penetration Testing / TLPT) is a separate, threat-led engagement type and is not represented by this assessment.
- PCI PIN Security is not a penetration test; it is a key-management / HSM / dual-control assessment (PCI PIN Security Requirements + ASC X9 TR-39), handled by Grilli Security as a separate assessment service.

8. Detailed Findings

N-01 — Internet-Exposed Device Management Interface

Severity	CRITICAL	**CVSS v4.0**	**9.3**
Category	Perimeter — Management-Plane Exposure	**Method Reference**	NIST SP 800-115 (External)
CWE	CWE-284	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1133
Component	203.0.113.10:8443 (perimeter firewall)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N		

Description
The perimeter firewall's HTTPS administrative interface was reachable from the public Internet and presented a vendor login that accepted authentication attempts. Device management planes must never be Internet-facing.

Business Impact
An Internet-exposed management plane is a direct target for brute-force, credential-stuffing and device-CVE exploitation. Compromise yields control of the network boundary and a pivot toward the internal network and CDE.

Likelihood
High — discoverable by untargeted Internet scanning; management interfaces are high-value, heavily-attacked assets.

Affected Endpoints
- https://203.0.113.10:8443/ (firewall administration)

Steps to Reproduce
1. From an external host, scan the perimeter address range.
2. Identify the device-management service on 203.0.113.10:8443.
3. Confirm the vendor administration login is reachable and accepts authentication attempts.

Evidence (redacted)
```
nmap -p443,8443 203.0.113.10  ->  8443/tcp open  ssl/https-alt
Title: <Vendor> Firewall — Administration  (login reachable from the Internet)
```

Remediation
1. Remove Internet exposure of all management interfaces; restrict to a dedicated management network/VPN requiring MFA.
2. Apply source ACLs and rate limiting as defence-in-depth.
3. Patch the device to current firmware and rotate administrative credentials.

References & Mappings
NIST SP 800-115 · CWE-284 · PCI DSS v4.0 Req 1.3, 8.x · MITRE ATT&CK T1133

Retest Result
Closed — Remediation Verified (15 June 2026). Management interface no longer reachable externally; restricted to the management VLAN with MFA.

N-02 — Unpatched Perimeter Service with Known Remote-Code-Execution CVE

Severity	**CRITICAL**	**CVSS v4.0**	**9.3**
Category	Perimeter — Missing Patches	**Method Reference**	NIST SP 800-115 (External)
CWE	CWE-1395	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1190
Component	203.0.113.12 (edge VPN service)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N		

Description
An Internet-facing edge service (VPN concentrator) ran a build affected by a publicly-known, exploitable remote-code-execution vulnerability. The vulnerable version was confirmed by a safe banner/version check; exploitation was not performed per the Rules of Engagement.

Business Impact
Reliable unauthenticated RCE on an Internet-facing host gives an attacker an immediate perimeter foothold and a path toward the internal network and CDE.

Likelihood
High — public exploit code typically exists for such CVEs and the host is Internet-reachable.

Affected Endpoints
- 203.0.113.12 (edge VPN service)

Steps to Reproduce
1. Fingerprint the edge service and version.
2. Map the version to the known CVE.
3. Confirm the vulnerable build via banner/version only (no exploitation, per ROE).

Evidence (redacted)
```
Service banner indicates a vulnerable build  [version REDACTED]
Mapped to [VERIFY: cite the specific CVE for the affected version] — exploitation not performed per ROE
```

Remediation
1. Patch/upgrade the edge service to a fixed version immediately.
2. Establish a vulnerability-management SLA for all Internet-facing assets.
3. Deploy IPS/virtual patching as interim mitigation.

References & Mappings
NIST SP 800-115 · [VERIFY: CVE-XXXX-XXXXX] · PCI DSS v4.0 Req 6.3.3, 11.3.1 · MITRE ATT&CK T1190

Retest Result
Closed — Remediation Verified (15 June 2026). Edge service upgraded to a fixed version; vulnerable banner no longer present.

N-03 — Inadequate Network Segmentation Between Corporate VLAN and CDE

Severity	**CRITICAL**	**CVSS v4.0**	**9.2**
Category	Segmentation — CDE Isolation	**Method Reference**	NIST SP 800-115 (Segmentation)
CWE	CWE-923	**MITRE**	PCI DSS 11.4.5 / 11.4.6

		ATT&CK / PCI	
Component	Corporate VLAN → CDE (198.51.100.0/24)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:H/SI:L/SA:N		

Description
From a standard host on the corporate VLAN, multiple services within the declared CDE (198.51.100.0/24) — including database, SSH and management ports — were directly reachable. The segmentation controls intended to isolate the CDE were ineffective.

Business Impact
Segmentation is the control that limits PCI DSS scope and contains a corporate-network compromise. Its failure means any compromised corporate host can reach cardholder-data systems directly, expanding both breach impact and PCI scope.

Likelihood
High — reachable from a normal internal position with no special privilege.

Affected Endpoints
- corp-VLAN host → 198.51.100.20:3306, 198.51.100.21:22, 198.51.100.10:443

Steps to Reproduce
1. From a corporate-VLAN host, scan the CDE range.
2. Confirm CDE services accept connections from outside the CDE.
3. Document the permitted flows that should be denied.

Evidence (redacted)

```
corp-host$ nc -vz 198.51.100.20 3306  -> open
corp-host$ nc -vz 198.51.100.21 22    -> open   [should be denied]
```

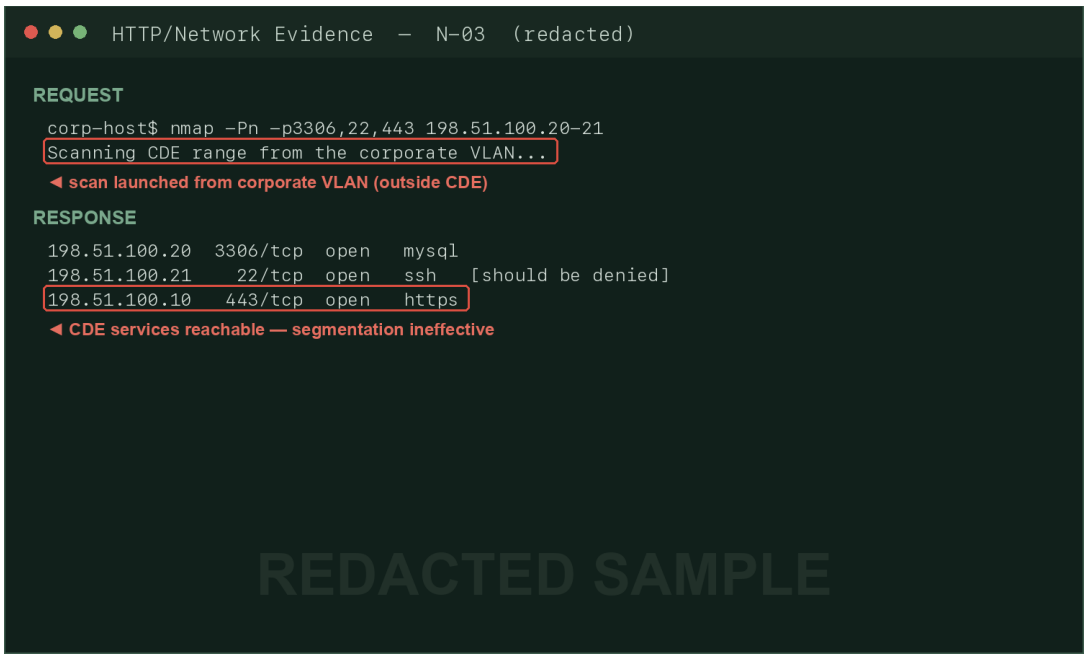

Figure 3 — Annotated segmentation evidence for N-03 (redacted).

Remediation
1. Implement deny-by-default segmentation between corporate and CDE networks; permit only documented, necessary flows.
2. Validate segmentation by ACL review and re-testing.

3. As a multi-tenant service provider, test segmentation controls at least every six months (PCI DSS Req 11.4.6).

References & Mappings
NIST SP 800-115 · CWE-923 · PCI DSS v4.0 Req 1.3, 11.4.5, 11.4.6

Retest Result
Closed — Remediation Verified (15 June 2026). Deny-by-default rules deployed; CDE services no longer reachable from the corporate VLAN.

N-04 — LLMNR / NBT-NS Poisoning Enables Credential Capture

Severity	**HIGH**	**CVSS v4.0**	**7.6**
Category	Internal — Spoofing	**Method Reference**	NIST SP 800-115 (Internal)
CWE	CWE-290	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1557.001
Component	Internal broadcast domain	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N		

Description
LLMNR and NBT-NS name resolution were enabled on the internal network, allowing an attacker on the LAN to answer broadcast name-resolution requests and capture NetNTLM authentication for offline cracking or relay.

Business Impact
Capture and cracking/relay of credentials enables lateral movement and privilege escalation across the internal estate — a common path to domain and CDE compromise.

Likelihood
Medium-High — requires an internal foothold but is otherwise trivial and reliable.

Affected Endpoints
- Internal broadcast domain (LLMNR/NBT-NS)

Steps to Reproduce
1. Run a name-resolution responder on the internal LAN.
2. Observe broadcast LLMNR/NBT-NS requests being answered.
3. Capture NetNTLM authentication (proof-of-concept only; no cracking).

Evidence (redacted)

```
responder -I eth0 ...  [+] Captured NetNTLMv2 from 198.51.100.55  [REDACTED]
```

Remediation
1. Disable LLMNR and NBT-NS via Group Policy across the estate.
2. Enforce SMB signing (see N-05) and segment broadcast domains.
3. Monitor for poisoning activity.

References & Mappings
NIST SP 800-115 · CWE-290 · MITRE ATT&CK T1557.001

Retest Result
Closed — Remediation Verified (15 June 2026). LLMNR/NBT-NS disabled via GPO; responder no longer captures authentication.

N-05 — SMB Signing Not Required — NTLM Relay Exposure

Severity	HIGH	**CVSS v4.0**	**7.6**
Category	Internal — Authentication Relay	**Method Reference**	NIST SP 800-115 (Internal)
CWE	CWE-294	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1557.001
Component	Internal Windows hosts (445/tcp)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N		

Description
SMB signing was not required on internal Windows hosts, permitting NTLM relay: authentication captured (e.g. via N-04) can be relayed to other hosts to gain access without cracking.

Business Impact
Relay of privileged authentication enables lateral movement and potential takeover of internal systems and, where reachable, CDE systems.

Likelihood
Medium-High — combined with N-04, a well-understood internal attack chain.

Affected Endpoints
- Internal Windows hosts (SMB/445)

Steps to Reproduce
1. Enumerate hosts where SMB signing is not required.
2. Demonstrate relay feasibility against a non-production target (PoC only).

Evidence (redacted)

```
crackmapexec smb 198.51.100.0/24 --gen-relay-list  ->  multiple hosts: signing:False
```

Remediation
1. Require and enforce SMB signing on all hosts and domain controllers via GPO.
2. Disable NTLM where feasible; prefer Kerberos.
3. Remediate alongside N-04.

References & Mappings
NIST SP 800-115 · CWE-294 · MITRE ATT&CK T1557.001 · PCI DSS v4.0 Req 8.x

Retest Result
Closed — Remediation Verified (15 June 2026). SMB signing required estate-wide; relay list now empty.

N-06 — Default Credentials on Out-of-Band Management Device

Severity	HIGH	**CVSS v4.0**	**8.7**
Category	Internal — Weak Credentials	**Method Reference**	NIST SP 800-115 (Internal)
CWE	CWE-798	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1078.001
Component	198.51.100.30 (OOB management controller)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N		

Description
An out-of-band management controller accepted documented vendor default credentials.

Business Impact
Administrative control of infrastructure hardware, enabling configuration change, traffic interception and persistence.

Likelihood
High — default credentials are trivially known/guessed.

Affected Endpoints
- https://198.51.100.30/ (OOB management)

Steps to Reproduce
1. Identify the management controller.
2. Attempt the vendor default credential pair.
3. Confirm administrative access (read-only PoC).

Evidence (redacted)

```
Login admin/<default>  ->  administrative dashboard  [access confirmed; no changes made]
```

Remediation
1. Change all default credentials; enforce a strong, unique-password standard.
2. Integrate device authentication with central IAM and MFA where supported.
3. Restrict management access to the management VLAN.

References & Mappings
NIST SP 800-115 · CWE-798 · PCI DSS v4.0 Req 2.2, 8.3 · MITRE ATT&CK T1078.001

Retest Result
Closed — Remediation Verified (15 June 2026). Default credentials replaced; the default pair is no longer valid.

N-07 — Missing Egress Filtering from the CDE

Severity	**MEDIUM**	**CVSS v4.0**	**5.3**
Category	CDE — Egress Control	**Method Reference**	NIST SP 800-115
CWE	CWE-1327	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1048
Component	CDE egress	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Description
Hosts within the CDE could initiate outbound connections to arbitrary Internet destinations and ports, with no egress filtering.

Business Impact
Unrestricted egress facilitates command-and-control and data exfiltration following any compromise, and weakens containment.

Likelihood
Medium — relevant once an attacker has a CDE foothold.

Affected Endpoints
- CDE host → arbitrary Internet:any

Steps to Reproduce
1. From a CDE host, attempt outbound connections to uncommon ports/destinations.

2. Confirm connections succeed (no egress policy).

Evidence (redacted)

```
cde-host$ connect external:4444  ->  connection established  [should be denied]
```

Remediation

1. Implement default-deny egress filtering from the CDE; allow only required destinations/ports.
2. Route egress through monitored proxies and alert on anomalies.

References & Mappings
NIST SP 800-115 · CWE-1327 · PCI DSS v4.0 Req 1.3 · MITRE ATT&CK T1048

Retest Result
Closed — Remediation Verified (15 June 2026). Default-deny egress implemented; arbitrary outbound now blocked.

N-08 — SNMP Default Community String Exposes Configuration

Severity	**MEDIUM**	**CVSS v4.0**	**6.9**
Category	Internal — Information Disclosure	**Method Reference**	NIST SP 800-115
CWE	CWE-200	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1592
Component	UDP/161 on infrastructure devices	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Description
Network devices responded to SNMPv1/2c queries using the default 'public' community string, disclosing configuration and topology.

Business Impact
Leaked configuration aids targeting and may expose credentials/keys; a writable community could permit configuration change.

Likelihood
Medium.

Affected Endpoints

- UDP/161 on infrastructure devices

Steps to Reproduce

1. Query a device with community 'public'.
2. Confirm configuration/system data is returned.

Evidence (redacted)

```
snmpwalk -v2c -c public 198.51.100.30  ->  sysDescr, interfaces, config  [REDACTED]
```

Remediation

1. Disable SNMPv1/2c; use SNMPv3 with authentication and encryption.
2. Remove default community strings and restrict SNMP to the management network.

References & Mappings
NIST SP 800-115 · CWE-200 · PCI DSS v4.0 Req 2.2

Retest Result

Closed — Remediation Verified (15 June 2026). SNMPv3 enforced; the default community is no longer accepted.

N-09 — Weak TLS on Internal Services

Severity	LOW	**CVSS v4.0**	**2.3**
Category	Internal — Cryptography	**Method Reference**	NIST SP 800-115
CWE	CWE-326	**MITRE ATT&CK / PCI**	—
Component	Internal HTTPS services	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Description
Several internal services offered TLS 1.0/1.1 and weak cipher suites.

Business Impact
Limited (internal, requires a privileged network position) but a strong-cryptography gap.

Likelihood
Low.

Affected Endpoints
- Internal HTTPS services

Steps to Reproduce
1. Scan internal services with a TLS scanner.
2. Confirm legacy protocols/ciphers are offered.

Evidence (redacted)

```
testssl 198.51.100.40  ->  TLS 1.0/1.1 enabled; weak CBC ciphers
```

Remediation
1. Disable TLS 1.0/1.1; require TLS 1.2+ and restrict to strong ciphers.

References & Mappings
NIST SP 800-115 · CWE-326 · PCI DSS v4.0 Req 2.2.7, 4.2.1

Retest Result
Closed — Remediation Verified (15 June 2026). Internal services restricted to TLS 1.2/1.3 with strong ciphers.

N-10 — Anonymous LDAP Information Disclosure

Severity	MEDIUM	**CVSS v4.0**	**5.3**
Category	Internal — Information Disclosure	**Method Reference**	NIST SP 800-115 (Internal)
CWE	CWE-200	**MITRE ATT&CK / PCI**	MITRE ATT&CK T1087
Component	198.51.100.50 (directory service)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Description
The internal directory permitted anonymous LDAP binds, allowing enumeration of users and groups.

Business Impact
User/group enumeration supports targeted credential attacks and privilege mapping.

Likelihood
Medium.

Affected Endpoints
- ldap://198.51.100.50

Steps to Reproduce
1. Perform an anonymous bind.
2. Enumerate directory objects.

Evidence (redacted)

```
ldapsearch -x -H ldap://198.51.100.50 -b '...' '(objectClass=user)'  ->  user list  [REDACTED]
```

Remediation
1. Disable anonymous binds; require authenticated LDAP.
2. Restrict directory queries and monitor enumeration.

References & Mappings
NIST SP 800-115 · CWE-200 · MITRE ATT&CK T1087

Retest Result
Closed — Remediation Verified (15 June 2026). Anonymous binds disabled; enumeration no longer possible.

9. Remediation & Retest

All findings were remediated by the Client within one week of report delivery and independently re-tested on 15 June 2026 (24 hours after remediation). Section 9.1 sets out the prioritized remediation plan and tracking; Section 9.2 records the retest outcome. Per-finding detail appears in Section 8.

9.1 Prioritized Remediation Plan

ID	Finding	Priority	Effort	Owner	Done
N-01	Internet-Exposed Device Management Interface	**P1**	M	Network Engineering	08 Jun 2026
N-02	Unpatched Perimeter Service with Known Remote-Code-Execution CVE	**P1**	M	Network Engineering	09 Jun 2026
N-03	Inadequate Network Segmentation Between Corporate VLAN and CDE	**P1**	M	Network Engineering	10 Jun 2026
N-04	LLMNR / NBT-NS Poisoning Enables Credential Capture	**P2**	S	IT Operations	11 Jun 2026
N-05	SMB Signing Not Required — NTLM Relay Exposure	**P2**	S	IT Operations	11 Jun 2026
N-06	Default Credentials on Out-of-Band Management Device	**P2**	S	Infrastructure	10 Jun 2026
N-07	Missing Egress Filtering from the CDE	**P3**	S	Network Engineering	12 Jun 2026
N-08	SNMP Default Community String Exposes Configuration	**P3**	S	Infrastructure	12 Jun 2026
N-09	Weak TLS on Internal Services	**P3**	S	Infrastructure	13 Jun 2026
N-10	Anonymous LDAP Information Disclosure	**P3**	S	Identity	13 Jun 2026

Priority: P1 immediate (≤7 days) · P2 high (≤2 weeks) · P3 planned (≤1 month) · P4 backlog. **Effort:** S < 1 day · M 1–3 days · L > 3 days. All items completed and verified at retest.

9.2 Retest Results

Every finding was confirmed closed at retest. Per-finding retest detail appears in Section 8.

ID	Finding	Severity	Retest Result
N-01	Internet-Exposed Device Management Interface	**Critical**	**PASS — Closed**
N-02	Unpatched Perimeter Service with Known Remote-Code-Execution CVE	**Critical**	**PASS — Closed**
N-03	Inadequate Network Segmentation Between Corporate VLAN and CDE	**Critical**	**PASS — Closed**
N-04	LLMNR / NBT-NS Poisoning Enables Credential Capture	**High**	**PASS — Closed**
N-05	SMB Signing Not Required — NTLM Relay Exposure	**High**	**PASS — Closed**
N-06	Default Credentials on Out-of-Band Management Device	**High**	**PASS — Closed**
N-07	Missing Egress Filtering from the CDE	**Medium**	**PASS — Closed**
N-08	SNMP Default Community String Exposes Configuration	**Medium**	**PASS — Closed**
N-09	Weak TLS on Internal Services	**Low**	**PASS — Closed**
N-10	Anonymous LDAP Information Disclosure	**Medium**	**PASS — Closed**

Outcome. Critical findings were remediated within 2 days of report delivery; full remediation across all 10 findings completed within one week, and retesting was performed 24 hours after remediation. Retest passed on first review and the supporting evidence was suitable for PCI assessor (QSA) acceptance.

10. Conclusion

The assessment found exploitable perimeter exposures and, critically, ineffective segmentation isolating the CDE, together with common internal-network weaknesses enabling credential capture and lateral movement. The Client remediated all 10 findings, independently verified as closed within the retest window.
Subject to maintaining the remediations and the PCI six-monthly segmentation-testing cadence, the network's residual risk is assessed as LOW. For full PCI DSS Req 11.4 coverage, this report is read together with the Web Application & API Penetration Test (GS-PT-2026-0481).

10.1 Next Steps & Contact

- Maintain deny-by-default segmentation and validate it at least every six months (PCI DSS Req 11.4.6).
- Operationalize the prioritized plan (Section 9.1) and enforce a patch SLA for Internet-facing assets.
- Re-test the network at minimum annually and after significant change (PCI DSS Req 11.4.2 / 11.4.3).
- Contact Grilli Security at lime@grillisecurity.com for the next assessment.

Appendix A — Severity & CVSS Methodology

Severity bands and CVSS v4.0 ranges are defined in Section 5.5. CVSS base scores were calculated using the FIRST.org CVSS v4.0 calculator; full vector strings are recorded per finding in Section 8. Final business risk ratings incorporate data sensitivity and contextual exploitability.

Appendix B — Network Testing Coverage Checklist

The table below records coverage of the network testing areas (NIST SP 800-115 / PTES) against the in-scope ranges. Tested = exercised, no issue or covered by hardening; → N-xx = yielded the referenced finding; N/A = not applicable / out of scope.

Test Area	Description	Result
DISC-01	Host discovery / live-host enumeration	Tested
DISC-02	TCP/UDP service & port enumeration	Tested
DISC-03	OS & service fingerprinting	Tested
EXT-01	External perimeter exposure review	Tested
EXT-02	Internet-exposed management interfaces	→ N-01
EXT-03	Unpatched perimeter services (known CVEs)	→ N-02
EXT-04	VPN / remote-access security	Tested
EXT-05	Email / DNS exposure (SPF/DMARC, zone transfer)	Tested
VULN-01	Vulnerability validation (no DoS)	Tested
VULN-02	Default / weak credentials on devices	→ N-06
SEG-01	CDE segmentation from corporate VLAN	→ N-03
SEG-02	CDE segmentation from other zones	Tested
SEG-03	Egress filtering from the CDE	→ N-07
INT-01	LLMNR / NBT-NS / mDNS poisoning	→ N-04
INT-02	SMB signing / NTLM relay	→ N-05
INT-03	Kerberoasting / AS-REP roasting	Tested
INT-04	SMB / NFS share exposure	Tested
INT-05	SNMP exposure	→ N-08
INT-06	LDAP anonymous bind	→ N-10
INT-07	IPv6 / DHCPv6 attacks	Tested
CRYP-01	TLS configuration (internal & external)	→ N-09
CRYP-02	IPsec / VPN cryptography	Tested
WIFI-01	Wireless network testing	N/A
PIVOT-01	Lateral movement / privilege-escalation paths	Tested

Appendix C — Tooling

nmap, Nessus, testssl.sh, Responder, CrackMapExec, impacket, snmpwalk, ldapsearch and bespoke scripts. All activity was throttled and scoped per the Rules of Engagement; no denial-of-service techniques were used.

Appendix D — PCI DSS v4.0 & DORA Cross-Reference

PCI DSS v4.0 Req 11.4.2 (internal), 11.4.3 (external) and 11.4.5 / 11.4.6 (segmentation, including the multi-tenant service-provider six-monthly cadence) are directly supported by this report; Req 11.4.1 (application layer) is covered by the Web Application & API report (GS-PT-2026-0481). DORA Art. 24–25 are supported as part of the ICT risk-management framework; DORA Art. 26–27 TLPT is a separate engagement.

Appendix E — Glossary

- **BOLA/IDOR —** Broken Object-/Function-Level Authorization / Insecure Direct Object Reference
- **CDE —** Cardholder Data Environment (PCI DSS)
- **3DE —** 3-D Secure Environment
- **CVSS —** Common Vulnerability Scoring System (v4.0)
- **DORA —** Digital Operational Resilience Act (EU 2022/2554)
- **EMVCo —** EMV company governing the EMV 3-D Secure specification
- **MFA —** Multi-Factor Authentication
- **NIS2 —** Directive (EU) 2022/2555 on network & information security
- **QSA —** Qualified Security Assessor (PCI)
- **TLPT —** Threat-Led Penetration Testing (DORA Art. 26–27)
- **CDE —** Cardholder Data Environment
- **NTLM —** NT LAN Manager authentication
- **OOB —** Out-of-Band (management)
- **SNMP —** Simple Network Management Protocol

Appendix F — Assessment Team & Qualifications

The engagement was delivered by certified offensive-security consultants (certifications include OSCP, OSWE, eWPTX, CREST CRT and CREST CCT Application). Individual identities are recorded in the secure project record and anonymized in this sample. Quality assurance was performed by an independent senior reviewer prior to issue.

Appendix G — Data Handling, Confidentiality & Disclaimer

All evidence and test artefacts are stored encrypted, access-controlled, and destroyed after the agreed retention period. This report is provided for the Client's internal security and compliance use and does not by itself constitute a compliance certification. It reflects the state of the assessed systems during the testing window and does not guarantee the absence of all vulnerabilities. Remediation should be validated in a controlled environment. Grilli Security accepts no liability for actions taken on the basis of this report.