CYBERLABS

OFFENSIVE SECURITY & PENETRATION TESTING

CONFIDENTIAL

PENETRATION TEST REPORT

Internal Network Penetration Test

Assessment Findings & Remediation Report

PREPARED FOR

O'Brien & Associates Solicitors

ENGAGEMENT REFERENCE

CL-2026-0417-INT

REPORT DATE

24 April 2026

CyberLabs Ltd · Dublin, Ireland · hello@cyberlabs.ie

Version 1.0 · TLP:RED

1 Document Control

Confidentiality Notice

This report contains sensitive security information relating to the systems and infrastructure of O'Brien & Associates Solicitors ("the Client"). It details vulnerabilities that could be used to compromise the Client's environment. Distribution is restricted to authorised personnel on a strict need-to-know basis. It must be stored securely, transmitted only through encrypted channels, and must not be shared with third parties without the written consent of the Client. This document is classified **TLP:RED**.

Document Details

Document Title	Internal Network Penetration Test — Findings & Remediation Report
Client	O'Brien & Associates Solicitors
Engagement Reference	CL-2026-0417-INT
Assessment Type	Internal Network Penetration Test (Assumed Breach)
Testing Window	13–17 April 2026
Report Version	1.0 (Final)
Report Date	24 April 2026
Classification	Confidential — TLP:RED

Version History

Version	Date	Author	Description
0.1	19 Apr 2026	Lead Consultant	Initial draft — findings documented
0.9	22 Apr 2026	QA Reviewer	Technical peer review and quality assurance
1.0	24 Apr 2026	Lead Consultant	Final release to client

Assessment Team & Contact

Role	Name	Contact
Lead Penetration Tester	[Redacted — CyberLabs Consultant]	hello@cyberlabs.ie
Quality Assurance Reviewer	[Redacted — CyberLabs Consultant]	hello@cyberlabs.ie
Client Technical Contact	[Redacted — Client MSP]	On call throughout testing

Disclaimer: *All client details, company names, IP addresses, usernames, credentials, and findings in this report are entirely fictional and have been created for illustrative purposes only. This is a sample deliverable produced by CyberLabs to demonstrate the structure and quality of a professional internal network penetration test report. It does not describe any real assessment of any real organisation.*

Table of Contents

2 Executive Summary

2.1 Overview & Business Context

O'Brien & Associates Solicitors engaged CyberLabs to conduct an internal network penetration test of its corporate environment. The firm operates from two offices, holds highly sensitive client data — including litigation files, property transactions and confidential correspondence — and had never previously undergone a formal security assessment. The engagement was prompted by a cyber-insurance renewal during which the firm's insurer flagged the absence of penetration testing.

The assessment was conducted as an **assumed-breach exercise**: CyberLabs simulated an attacker who had already obtained a foothold on the internal network, whether through a malicious insider, a compromised workstation, or a breach of the perimeter. The objective was to determine what such an attacker could realistically achieve against the firm's Active Directory environment, servers and data.

> **Bottom Line**
>
> Starting from an unauthenticated position on the internal network — with no credentials — CyberLabs achieved full **Domain Administrator** control of the entire Active Directory environment. From that position, every user account, server, workstation and file store was accessible. The compromise chain began with a single user's machine querying a mistyped network path and completed in a matter of hours.

2.2 Summary of Results

A total of **twelve findings** were identified. The distribution by severity is shown below.

3	3	4	2
CRITICAL	HIGH	MEDIUM	LOW

The three critical findings are not isolated issues — they combine into a single, reliable path from zero access to complete domain compromise. Each is individually well understood in the security industry, and each is exploitable using freely available tooling requiring only moderate skill.

2.3 Key Risk Themes

- **Legacy and unpatched systems.** A Windows Server 2008 R2 host, unsupported since January 2020, remained in production holding archived client files and was vulnerable to a seven-year-old exploit (EternalBlue).
- **Insecure Active Directory defaults.** LLMNR/NBT-NS name resolution, disabled SMB signing, and legacy Group Policy Preferences credentials provided multiple reliable footholds.
- **Credential and privilege hygiene.** Predictable passwords, a service account with unnecessary Domain Admin rights, and no password expiry policy meant credentials were both easy to obtain and highly valuable once obtained.
- **No detection capability.** The absence of centralised logging meant none of the attack activity would have been detected. A real attacker could have operated undisturbed.

2.4 Strategic Recommendations

The individual technical fixes are set out in Section 9. At a strategic level, CyberLabs recommends the firm:

1. Treat the three critical findings as an emergency remediation priority, actionable within days at minimal cost.
2. Establish a basic patch and asset lifecycle process so unsupported systems are identified and retired before they become liabilities.
3. Invest in detection — even lightweight centralised logging would transform the firm's ability to notice an intrusion.
4. Adopt a recurring assessment cycle (at least annually) as security posture degrades over time as environments change.

3 Scope & Rules of Engagement

Prior to testing, scope and rules of engagement were agreed in writing between CyberLabs and the Client. This protects both parties and ensures testing is controlled, legal and targeted.

In Scope

Target	Detail
Internal network subnets	`192.168.1.0/24` (Dublin) and `10.10.0.0/24` (Cork)
Active Directory	Domain `obrien-solicitors.local`
Windows servers & workstations	All domain-joined hosts
Network-attached storage	QNAP NAS device

Out of Scope

- Production client data — not to be accessed, read or exfiltrated at any point
- Microsoft 365 cloud services (tested only where domain credentials naturally granted access, to demonstrate impact)
- Any denial-of-service activity or deliberate disruption of business operations
- Internal Wi-Fi (assessed separately under a distinct wireless scope)

Rules of Engagement

Testing dates	13–17 April 2026 (five working days)
Testing hours	09:00–18:00 IST, business days
Source of testing	CyberLabs secure testing host on the internal network
Client contact	Technical contact briefed and on call throughout
Data handling	Evidence sanitised; no client data retained post-engagement
Stop conditions	Testing to pause immediately on any sign of unintended disruption

> **Assumed-Breach Model**
> This engagement deliberately started from a position of internal network access with no credentials, rather than attempting to breach the perimeter first. This model reflects the reality that perimeters are frequently bypassed (phishing, stolen laptops, insider access) and produces a more useful picture of internal resilience.

4 Methodology

CyberLabs follows a structured methodology aligned with the **Penetration Testing Execution Standard (PTES)** and maps all findings to the **MITRE ATT&CK** framework. This provides a consistent, repeatable process and contextualises findings against known real-world attacker tactics.

Phase	Activities
1. Internal Reconnaissance	Passive and active discovery of live hosts, services and the Active Directory environment. Network sweeping and service identification.
2. Enumeration	Detailed interrogation of discovered services, user accounts, group memberships, share permissions and trust relationships.
3. Exploitation	Controlled attempts to leverage identified weaknesses to gain access, capture credentials, or elevate privileges.
4. Post-Exploitation & Lateral Movement	Demonstration of realistic attacker impact once inside — privilege escalation, credential harvesting, lateral movement and persistence, without accessing production client data.
5. Reporting	Documentation of all findings with risk ratings, evidence, and prioritised, actionable remediation guidance.

Testing was conducted manually by an experienced consultant, supported by industry-standard tooling. Automated scanning was used only for discovery and enumeration; all exploitation and impact demonstration was performed and validated by hand to eliminate false positives and to control the blast radius of testing.

5 Risk Rating Methodology

Each finding is assigned a risk rating derived from its **likelihood of exploitation** and its potential **business impact**, using a framework aligned with the **CVSS v3.1** scoring system. Ratings reflect risk in the context of this specific environment, not severity in the abstract.

Rating	CVSS Range	Definition
CRITICAL	9.0 – 10.0	Trivially exploitable with severe impact. Enables full compromise of systems or data. Requires emergency remediation.
HIGH	7.0 – 8.9	Readily exploitable with significant impact, or a key link in a compromise chain. Remediate as a priority.
MEDIUM	4.0 – 6.9	Exploitable under specific conditions, or meaningfully increases attacker capability. Remediate in a planned manner.
LOW	0.1 – 3.9	Limited direct impact or difficult to exploit. Represents hygiene, hardening, or defence-in-depth improvements.

A note on chained risk

Several findings rated individually as Medium or High become far more dangerous in combination. The overall risk to the firm is driven not by any single issue but by how readily they chain together into a complete compromise. Remediation priority reflects this.

6 Findings Summary

The table below lists all findings in priority order. Full technical detail for each is provided in Section 8.

Ref	Finding	Rating	CVSS	MITRE ATT&CK
INT-01	LLMNR/NBT-NS poisoning enabling credential capture	CRITICAL	9.8	T1557.001
INT-02	Credentials exposed in SYSVOL via Group Policy Preferences	CRITICAL	9.1	T1552.006
INT-03	Unpatched MS17-010 (EternalBlue) on legacy server	CRITICAL	9.8	T1210
INT-04	Kerberoastable service account with Domain Admin rights	HIGH	8.1	T1558.003
INT-05	Weak and predictable password policy	HIGH	7.5	T1110.002
INT-06	Sensitive HR data on open SMB share	HIGH	7.1	T1039
INT-07	SMB signing disabled — enables relay attacks	MEDIUM	6.5	T1557.001
INT-08	MFA not enforced for all Microsoft 365 users	MEDIUM	6.3	T1078
INT-09	Excessive local administrator rights on workstations	MEDIUM	5.5	T1078.003
INT-10	No network segmentation between workstations and servers	MEDIUM	5.3	T1021
INT-11	QNAP NAS running outdated firmware with known CVEs	LOW	3.7	T1190
INT-12	No centralised logging or SIEM	LOW	3.1	T1562.002

7 Attack Narrative

This section describes the end-to-end compromise as a continuous story, to illustrate how the individual findings combine. It reflects the actual path taken during testing.

Step 1 — A foothold from thin air

With no credentials, the tester ran a name-resolution poisoning tool (`Responder`) on the local network. Within eleven minutes a fee earner's workstation attempted to resolve a non-existent path and its NTLMv2 hash was captured (**INT-01**). The password `Summer2023!` — policy-compliant but structurally predictable — was cracked offline in under four minutes (**INT-05**). The tester now held valid domain credentials.

Step 2 — From a user to every workstation

Using those credentials, the tester read a Group Policy Preferences file left in SYSVOL containing an encrypted local administrator password. Microsoft's encryption key for this format has been public since 2012, so the password was recovered instantly (**INT-02**), granting local admin on all 42 workstations.

Step 3 — Owning a server without a password

In parallel, the unsupported Windows Server 2008 R2 host was found vulnerable to EternalBlue. A single exploit yielded a SYSTEM shell with no credentials required (**INT-03**). This server held archived client matter files dating back to 2011.

Step 4 — Becoming Domain Admin

A Kerberoasting attack requested service tickets for service accounts. The over-privileged `svc_backup` account — needlessly a Domain Admin — used the password `Backup@2019`, cracked offline in under two hours (**INT-04**). The tester now held **Domain Administrator** rights.

Step 5 — Total control

With Domain Admin, the tester dumped all domain hashes including the KRBTGT account (enabling forged "Golden Tickets" for persistent access), accessed volume shadow copies, and confirmed Microsoft 365 mailbox access where MFA was absent (**INT-08**). No client data was accessed. The entire environment was under the tester's control, and — absent any logging (**INT-12**) — none of it would have been detected.

> **The uncomfortable truth**
>
> The entire chain was triggered by an ordinary user's computer looking for a network path that did not exist — something that happens naturally whenever a server name is mistyped. No phishing, no malware, no user error beyond a typo was required.

8 Detailed Findings

Each finding below includes a description, evidence, business impact, affected assets and specific remediation guidance. Command output has been sanitised and is representative.

FINDING INT-01

CRITICAL

LLMNR/NBT-NS Poisoning Enabling Credential Capture

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
9.8	**T1557.001**	**Entire subnet**	**Open**

Description

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) were both active across the network. These legacy fallback name-resolution protocols allow any host on the local segment to answer name-lookup broadcasts. An attacker can respond to these broadcasts and coerce the requesting machine into authenticating to the attacker, exposing the user's NTLMv2 challenge-response hash.

Evidence

```
RESPONDER — CAPTURED NTLMV2 HASH (SANITISED)
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 192.168.1.64 for name FILESRV-01
[SMB] NTLMv2-SSP Client   : 192.168.1.64
[SMB] NTLMv2-SSP Username : OBRIEN\m.connolly
[SMB] NTLMv2-SSP Hash     : m.connolly::OBRIEN:1122334455667788:A1B2...[truncated]
# Hash submitted to Hashcat with rockyou.txt wordlist
$ hashcat -m 5600 hash.txt rockyou.txt
m.connolly::OBRIEN:...:Summer2023!     (recovered in 00:03:41)
```

Business Impact

This finding provided the initial foothold for the entire compromise. Any user on the network could have their credentials captured passively, with no interaction beyond a mistyped or stale network path. Because the captured credential belonged to a legitimate domain user, all subsequent activity appeared as normal authenticated behaviour.

Remediation

- **Disable LLMNR** via Group Policy: *Computer Configuration → Administrative Templates → Network → DNS Client → Turn off multicast name resolution → Enabled*.
- **Disable NBT-NS** on all interfaces via DHCP option or scripted registry change.
- Ensure DNS is correctly configured so legitimate lookups never fall back to these protocols.

> **Effort vs. impact**
>
> This is a Group Policy change that takes minutes to deploy and eliminates the single most damaging attack vector in this report at no cost.

FINDING INT-02

CRITICAL

Credentials Exposed in SYSVOL via Group Policy Preferences

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
9.1	**T1552.006**	**All workstations**	**Open**

Description

A Group Policy Preferences (GPP) XML file in the domain's SYSVOL share contained a local administrator password in the `cpassword` field. While AES-256 encrypted, Microsoft published the static decryption key in 2012, rendering any such credential trivially recoverable by any authenticated domain user, since SYSVOL is world-readable within the domain.

Evidence

```
RECOVERING THE GPP CPASSWORD (SANITISED)
$ smbclient //DC01/SYSVOL -U 'OBRIEN\m.connolly'
smb:\> get obrien-solicitors.local\Policies\{...}\Machine\Preferences\Groups\Groups.xml
# Groups.xml contains:  cpassword="j1Uyj3Vx8..."
$ gpp-decrypt "j1Uyj3Vx8To3RtN..."
Local@dmin!2021   <-- plaintext local administrator password
```

Business Impact

The recovered password was valid for the local administrator account on all 42 workstations, providing reliable lateral movement and a fallback route to any user's machine independent of INT-01.

Remediation

- Remove the offending `Groups.xml` (and any other GPP files containing `cpassword`) from SYSVOL.
- Deploy **LAPS** (Local Administrator Password Solution) so each machine has a unique, automatically rotating local admin password.
- Rotate the exposed local administrator password across all affected machines immediately.

FINDING INT-03

CRITICAL

Unpatched MS17-010 (EternalBlue) on Legacy Server

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
9.8	**T1210**	**WS2008R2 host**	**Open**

Description

A Windows Server 2008 R2 host — unsupported since January 2020 — was unpatched against MS17-010 ("EternalBlue"), the SMBv1 vulnerability weaponised in the 2017 WannaCry outbreak. It was exploitable remotely with no authentication, yielding SYSTEM-level code execution.

Evidence

METASPLOIT — ETERNALBLUE EXPLOITATION (SANITISED)

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] 10.10.0.20:445 - Connecting to target for exploitation.
[+] 10.10.0.20:445 - The target is vulnerable.
[*] 10.10.0.20:445 - Sending SMB payload...
[+] 10.10.0.20:445 - WIN! Meterpreter session 1 opened
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Business Impact

Full control of a production server holding archived client matter files back to 2011, obtained with no credentials. This same class of vulnerability is routinely used by ransomware to spread automatically across networks.

Remediation

- **Immediate:** isolate the host behind a firewall rule blocking all inbound SMB until it can be dealt with.
- **Priority:** decommission the server and migrate its workload to a supported platform.
- Disable SMBv1 across the entire estate; it should not be in use anywhere in a modern environment.

FINDING INT-04

HIGH

Kerberoastable Service Account with Domain Admin Rights

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
8.1	**T1558.003**	**svc_backup**	**Open**

Description

Any authenticated domain user can request Kerberos service tickets for accounts with a Service Principal Name and crack them offline. The `svc_backup` account had a weak, long-lived password *and* was a member of Domain Admins — an unnecessary and dangerous combination.

Evidence

```
KERBEROASTING SVC_BACKUP (SANITISED)
$ GetUserSPNs.py obrien-solicitors.local/m.connolly -request
ServicePrincipalName   Name         MemberOf
--------------------   ----------   ----------------
MSSQLSvc/db01:1433     svc_backup   Domain Admins
# Ticket cracked offline:
$ hashcat -m 13100 spn.txt rockyou.txt
svc_backup:Backup@2019   (recovered in 01:52:07)
```

Business Impact

Cracking this single account granted **Domain Administrator** — complete control of the Active Directory environment. This was the final step to total compromise.

Remediation

- Remove `svc_backup` from Domain Admins; grant only the specific rights its backup function requires.
- Reset the password to a 30+ character random string, or migrate to a Group Managed Service Account (gMSA) with automatic password management.
- Audit all accounts with Service Principal Names for weak passwords and excessive privilege.

FINDING INT-05

HIGH

Weak and Predictable Password Policy

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
7.5	**T1110.002**	**Domain-wide**	**Open**

Description

The domain password policy permitted short, structurally predictable passwords and enforced no expiry. 37 accounts had not changed their password in over 18 months. Passwords such as `Summer2023!` and `Backup@2019` satisfied complexity rules yet followed the word-season-year pattern present in every major cracking wordlist.

Business Impact

Predictable passwords made both the initial foothold (INT-01) and the privilege escalation (INT-04) fast and reliable. Complexity requirements alone provide little protection when the underlying structure is guessable.

Remediation

- Enforce a minimum length of 14+ characters; length defeats cracking far more effectively than complexity.
- Deploy a banned-password list (e.g. Azure AD / Entra Password Protection) to block seasons, company names and common patterns.
- Encourage passphrases and roll out a password manager for staff.

FINDING INT-06

HIGH

Sensitive HR Data Accessible on Open SMB Share

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
7.1	**T1039**	**File server**	**Open**

Description

The `\\FILESERVER\General` share was readable by all authenticated domain users and contained an *HR Documents* folder holding staff salary information and personal data. No least-privilege access control was applied.

Business Impact

Any compromised or curious user account could read sensitive personal and payroll data. This carries direct GDPR implications, given the personal data of staff was exposed to the entire user population.

Remediation

- Restrict the HR folder to HR personnel using role-based NTFS permissions.
- Review all shares for over-permissive access; adopt least privilege as the default.
- Consider data classification so sensitive stores are identified and protected consistently.

FINDING INT-07

MEDIUM

SMB Signing Disabled — Enables Relay Attacks

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
6.5	**T1557.001**	**Most workstations**	**Open**

Description

SMB signing was not enforced on the majority of hosts. Combined with the name-resolution poisoning in INT-01, this permits **SMB relay** attacks, where a captured authentication attempt is forwarded to another host in real time to gain access without ever cracking the hash.

Business Impact

Amplifies INT-01: an attacker need not even crack a captured credential, but can relay it directly to authenticate to other systems, expanding reach and speed of compromise.

Remediation

- Enforce SMB signing on all domain members via Group Policy (*Microsoft network client/server: Digitally sign communications (always)*).
- Prioritise servers, then roll out to workstations after validating for performance impact.

FINDING INT-08

MEDIUM

MFA Not Enforced for All Microsoft 365 Users

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
6.3	**T1078**	**M365 tenant**	**Open**

Description

Multi-factor authentication was not enforced for all users. Domain credentials obtained on-premises granted access to Exchange Online mailboxes, as the same passwords worked against the cloud tenant with no second factor required.

Business Impact

A single cracked password exposed email — one of the most sensitive data stores in a law firm. Without MFA, any credential leak (internal or external) directly threatens the cloud environment.

Remediation

- Enforce MFA for **all** users via Conditional Access. This is achievable at no additional licensing cost on most tenants and is among the single highest-impact controls available.
- Block legacy authentication protocols that bypass MFA.

FINDING INT-09

MEDIUM

Excessive Local Administrator Rights on Workstations

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
5.5	**T1078.003**	**Multiple users**	**Open**

Description

Several users were members of the local Administrators group on machines they did not administer. Local admin rights make credential theft, persistence and lateral movement significantly easier for an attacker who compromises that user.

Business Impact

Increases the value of every compromised workstation account and lowers the barrier to escalating from a single foothold to broader control.

Remediation

- Remove standing local admin rights from standard users; adopt least privilege.
- Where elevation is genuinely needed, use a just-in-time / privileged access approach rather than permanent membership.

FINDING INT-10

MEDIUM

No Network Segmentation Between Workstations and Servers

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
5.3	**T1021**	**Both subnets**	**Open**

Description

Workstations and servers shared flat network segments with no filtering between them. Any workstation could reach any server on any port, giving an attacker unrestricted lateral movement once a single host was compromised.

Business Impact

A flat network turns a single compromised endpoint into a launch point against the entire estate, and materially increases the blast radius of ransomware.

Remediation

- Separate workstations and servers into distinct VLANs with firewall rules restricting inter-VLAN traffic to only what is required.
- Restrict administrative protocols (RDP, SMB, WinRM) to designated management hosts.

FINDING INT-11

LOW

QNAP NAS Running Outdated Firmware with Known CVEs

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
3.7	**T1190**	**QNAP NAS**	**Open**

Description

The QNAP NAS was running outdated firmware associated with several published CVEs. While not exploited during this engagement, unpatched storage appliances are a recurring target, particularly for ransomware families that specifically hunt NAS devices.

Business Impact

Potential exposure of stored data and a possible secondary foothold. Storage appliances often hold backups — an attractive target for attackers seeking to disable recovery.

Remediation

- Update firmware to the current supported release and enable automatic updates where possible.
- Remove any exposure to untrusted networks; restrict management to trusted hosts.

FINDING INT-12

LOW

No Centralised Logging or SIEM

CVSS V3.1	MITRE ATT&CK	AFFECTED	STATUS
3.1	**T1562.002**	**Enterprise-wide**	**Open**

Description

No centralised log collection or security monitoring was in place. Security-relevant events remained isolated on individual hosts, where they are easily missed or cleared. None of the activity performed during this engagement would have generated an alert.

Business Impact

Without detection, an intrusion can continue indefinitely. The difference between a contained incident and a catastrophic breach is very often the speed of detection — which here was effectively zero.

Remediation

- Deploy Windows Event Forwarding to a central collector as a low-cost starting point.
- Adopt a SIEM or log-aggregation platform with alerting on credential attacks, privilege escalation and lateral movement.
- Define an incident response process so that alerts lead to action.

9 Remediation Roadmap

Recommendations are prioritised by risk and sequenced for practical delivery. Timeframes are indicative and assume the firm's managed service provider undertakes the work.

Immediate — within 72 hours

Ref	Action	Effort
INT-01	Disable LLMNR and NBT-NS domain-wide via Group Policy	Low
INT-03	Isolate the Windows Server 2008 R2 host behind strict SMB firewall rules	Low
INT-02	Remove GPP password from SYSVOL and rotate the exposed local admin password	Low
INT-04	Remove Domain Admin from `svc_backup` and reset to a strong password	Low

Short term — within 30 days

Ref	Action	Effort
INT-08	Enforce MFA for all Microsoft 365 accounts via Conditional Access	Low
INT-07	Enable SMB signing on all domain members	Medium
INT-06	Restrict the General share and apply role-based access to HR data	Low
INT-05	Implement a 14+ character password policy with a banned-password list	Medium
INT-02	Deploy LAPS across all workstations	Medium

Medium term — 30 to 90 days

Ref	Action	Effort
INT-03	Decommission the legacy server and migrate its workload	High
INT-10	Introduce VLAN segmentation between workstations and servers	High
INT-12	Implement centralised logging and alerting (WEF / SIEM)	Medium
INT-09	Remove standing local admin rights; adopt least privilege	Medium
INT-11	Update NAS firmware and review for known CVEs	Low
—	Deliver user awareness training on password hygiene and phishing	Low

> **Retest included**
>
> CyberLabs recommends a remediation retest once the immediate and short-term actions are complete, to confirm the critical and high findings are no longer reproducible and to provide documented assurance for the firm's insurer and clients.

10 Appendix A — Tools Used

All tools used are industry-standard and were operated under the agreed rules of engagement.

Tool	Purpose
Nmap	Host discovery and service enumeration
Responder	LLMNR/NBT-NS poisoning and hash capture
Hashcat	Offline password cracking
BloodHound	Active Directory attack-path analysis
ldapdomaindump	LDAP / AD object enumeration
CrackMapExec	SMB / AD enumeration and validation
Impacket suite	GetUserSPNs, secretsdump and related AD tooling
gpp-decrypt	Decryption of GPP cpassword values
Metasploit Framework	Validated exploitation (MS17-010)

11 Appendix B — MITRE ATT&CK Mapping

Technique	Name	Finding
T1557.001	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	INT-01, INT-07
T1552.006	Unsecured Credentials: Group Policy Preferences	INT-02
T1210	Exploitation of Remote Services	INT-03
T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting	INT-04
T1110.002	Brute Force: Password Cracking	INT-05
T1039	Data from Network Shared Drive	INT-06
T1078 / T1078.003	Valid Accounts / Local Accounts	INT-08, INT-09
T1021	Remote Services (lateral movement)	INT-10
T1190	Exploit Public-Facing Application	INT-11
T1562.002	Impair Defenses: Disable Windows Event Logging	INT-12

12 Appendix C — CVSS Vector Reference

Representative CVSS v3.1 base vectors for the critical findings, for reference.

Finding	Base Score	Vector
INT-01	9.8	`AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
INT-02	9.1	`AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L`
INT-03	9.8	`AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
INT-04	8.1	`AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N`

CyberLabs Ltd

Penetration Testing & Offensive Security · Dublin, Ireland

hello@cyberlabs.ie · www.cyberlabs.ie

All testing conducted under signed rules of engagement and in full compliance with Irish and EU law.