

SAMPLE DELIVERABLE

SMB PENTEST PACKAGE

Penetration Test Report

Example Dental Group LLC

Fixed-price external and internal network penetration test with Microsoft 365 configuration review. This document is a fictional sample prepared for marketing purposes and does not describe a real engagement.

PREPARED FOR	Example Dental Group LLC
PREPARED BY	Northline Digital LLC
PRIMARY TESTER	Christopher Smith, MS Cyber Security, CEH
REPORT ID	NL-SAMPLE-EDG-001
CLASSIFICATION	Sample — Fictional Client

CONTENTS

Table of Contents

1. Executive Summary	3
2. Scope and Rules of Engagement	4
3. Methodology	5
4. Risk Rating Method	5
5. Findings Summary	6
6. Detailed Findings	7
7. Retest	14
8. Attestation Letter (Sample)	15

About this sample. Example Dental Group LLC, example.com, and all hostnames, IP addresses, and screenshots in this report are fictional. Network addresses use RFC 5737 documentation ranges (192.0.2.0/24 and 198.51.100.0/24). The findings illustrate issues commonly observed in small and mid-sized business environments.

Executive Summary

Northline Digital LLC performed an SMB Pentest for **Example Dental Group LLC** (a fictional sample client). The goal was to answer a practical question for the owners: if a real attacker targeted the practice today, how far could they get, and what should be fixed first?

Testing covered internet-facing systems, remote access, the Microsoft 365 tenant that holds email and files, and a limited internal network segment. Work was manual and non-destructive. Testing stopped at proof of impact.

6 FINDINGS	1 CRITICAL	2 HIGH	2 MEDIUM	1 LOW
---------------	---------------	-----------	-------------	----------

What this means in plain English

Several gaps would make it easier for an attacker to get into email, remote desktop, or the public website—and from there into patient scheduling data and staff mailboxes. None of the findings required exotic techniques. They are the kinds of issues cyber insurers and auditors regularly ask about, and they are fixable with configuration changes, MFA enforcement, patching, and tighter password policy.

Top priorities for ownership

1. **Turn on and require MFA** for every Microsoft 365 account and for VPN/remote desktop access. Legacy authentication that bypasses MFA should be blocked.
2. **Update the public website plugin** that has a known critical vulnerability (CVE-2023-4596). Until then, treat the site as high risk.
3. **Remove or lock down internet-facing RDP**; require MFA-backed VPN instead.
4. **Publish DMARC** (with SPF and DKIM already in place) so insurers and email providers can see the domain is protected against spoofing.
5. **Strengthen password policy** and eliminate credential reuse across admin accounts; enable SMB signing on file servers.

Overall posture. The practice has a workable IT foundation, but authentication and internet exposure need attention before the next insurance renewal. After the recommended fixes, a retest within 45 days can confirm remediation and support an attestation letter for the insurer.

Scope and Rules of Engagement

Scope and rules were agreed in writing before testing began. The summary below reflects a typical SMB Pentest package engagement for this sample client.

In scope

Asset / area	Details (fictional)
Public website	www.example.com (WordPress)
Mail / productivity	Microsoft 365 tenant example.com
Remote access	vpn.example.com, rdp.example.com (192.0.2.40)
External hosts	mail.example.com (192.0.2.10), files.example.com (192.0.2.20)
Internal sample segment	198.51.100.0/24 (workstations, file server, domain controller)

Out of scope

- Denial-of-service, ransomware simulation, or destructive testing
- Physical security, social engineering of patients, or phishing of real patients
- Third-party SaaS not owned by Example Dental Group LLC (except read-only M365 configuration review)
- Systems outside the signed IP and hostname list

Rules of engagement (summary)

- Written authorization from Example Dental Group LLC ownership before any probing
- Testing windows: evenings and weekends preferred for remote access checks
- Stop at proof of impact; no data exfiltration of real patient records
- Emergency contact: practice IT lead; Northline on-call during active windows
- Findings shared only with designated contacts; sample report sanitized for marketing use

PACKAGE

SMB Pentest

TESTER

Christopher Smith

RETEST WINDOW

45 days after final report

CLIENT TYPE

Fictional sample — dental SMB

SECTION 3

Methodology

Testing followed industry-standard guidance adapted for SMB environments:

- **NIST SP 800-115** — Technical Guide to Information Security Testing and Assessment (planning, discovery, vulnerability analysis, exploitation where authorized, reporting).
- **OWASP Web Security Testing Guide (WSTG)** — for the public WordPress site and related web services (configuration, authentication, session, input validation, and known-vulnerable components).

Activities included OSINT and attack-surface mapping, authenticated and unauthenticated checks against in-scope hosts, Microsoft 365 configuration review (read-only), credential-related controls assessment, and limited internal network testing from an authorized vantage point. Commercial and open-source tools supported manual analysis; automated scanner output was verified by hand before inclusion.

SECTION 4

Risk Rating Method

Each finding is rated using **CVSS v3.1** base scores plus a short **business impact** note tailored to a multi-location dental practice (patient scheduling, insurance billing, email, and shared files).

Rating	CVSS v3.1	Business meaning (plain English)
CRITICAL	9.0 – 10.0	Immediate path to compromise of core systems or sensitive data; fix now.
HIGH	7.0 – 8.9	Likely to enable account takeover or significant access; fix this sprint.
MEDIUM	4.0 – 6.9	Meaningful risk under realistic conditions; plan and remediate soon.
LOW	0.1 – 3.9	Limited impact alone; still worth closing for defense-in-depth and insurance.

Business impact considers confidentiality of patient and business data, integrity of scheduling and billing systems, and availability of clinical operations—not only the CVSS number.

Findings Summary

ID	Title	Severity	CVSS	Status
F-01	Outdated WordPress Forminator plugin (CVE-2023-4596)	CRITICAL	9.8	Open
F-02	Internet-exposed RDP without MFA	HIGH	8.1	Open
F-03	Microsoft 365 legacy authentication still permitted	HIGH	7.5	Open
F-04	Weak domain password policy and credential reuse	MEDIUM	6.5	Open
F-05	Missing DMARC policy on example.com	MEDIUM	5.3	Open
F-06	SMB signing not required on file server	LOW	3.1	Open

Severity reflects CVSS v3.1 base score adjusted with business impact for this sample practice. Status “Open” means remediation had not yet been verified at the time of this sample report.

Detailed Findings

F-01 — Outdated WordPress Forminator plugin (CVE-2023-4596)

CRITICAL

CVSS V3.1

9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

AFFECTED ASSET<https://www.example.com> (WordPress) – Forminator ≤ 1.24.6**DESCRIPTION**

The public website runs the Forminator contact-form plugin at a version vulnerable to unauthenticated arbitrary file upload (CVE-2023-4596). File type validation occurs after the upload is written, which can allow an unauthenticated attacker to place executable content on the server and achieve remote code execution.

EVIDENCE (MOCK, REDACTED)

```
[+] Host: www.example.com (192.0.2.50)
[+] CMS: WordPress 6.x
[+] Plugin: forminator v1.24.4 (read from readme.txt / plugin header)
[+] Advisory: CVE-2023-4596 – unauthenticated arbitrary file upload
[+] Proof stopped at version confirmation and public advisory match
[+] No webshell deployed; testing halted at proof of impact
---
GET /wp-content/plugins/forminator/readme.txt HTTP/1.1
Host: www.example.com
...
Stable tag: 1.24.4
```

BUSINESS IMPACT

A compromised website can be used to steal patient inquiry data from forms, inject malware, or pivot toward staff credentials. For a dental practice this also creates reputation and insurance-questionnaire risk.

REMEDIATION

1. Update Forminator to 1.25.0 or later immediately; verify no other abandoned plugins remain.
2. Restrict PHP execution in upload directories; review web server write permissions.
3. Enable automatic updates or a monthly patch cadence for WordPress core, themes, and plugins.
4. Scan the site for unexpected PHP files after patching; rotate any credentials stored on the host.

REFERENCES

NVD CVE-2023-4596 · Wordfence advisory · OWASP WSTG — Testing for Weak Cryptography / Vulnerable Components · NIST SP 800-115

F-02 — Internet-exposed RDP without MFA

HIGH

CVSS V3.1

8.1 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

AFFECTED ASSET

rdp.example.com → 192.0.2.40:3389 (TCP)

DESCRIPTION

Remote Desktop Protocol was reachable from the public internet. No multifactor authentication gateway or broker was observed in front of the service. Password spray and credential-stuffing attacks against exposed RDP remain common against SMBs.

EVIDENCE (MOCK, REDACTED)

```
PORT      STATE  SERVICE
3389/tcp  open   ms-wbt-server
Nmap banner / SSL cert CN: rdp.example.com
Security layer: CredSSP / TLS
NLA: enabled
MFA broker / RD Gateway: not detected
VPN-only restriction: not enforced
---
External probe from tester egress → 192.0.2.40:3389 SYN-ACK
Login not brute-forced; existence and lack of MFA documented only
```

BUSINESS IMPACT

Successful RDP login yields a desktop on the practice network—often with access to imaging shares, practice-management software, and cached credentials. Insurers frequently ask whether remote access requires MFA.

REMEDIATION

- 1. Remove public RDP. Place remote access behind a VPN or Zero Trust broker that enforces MFA.
- 2. If temporary access is required, restrict source IPs and use an RD Gateway with MFA.
- 3. Monitor failed logons; alert on unusual geographic access.
- 4. Ensure local admin passwords are unique and stored in a vault.

REFERENCES

CIS Controls (Secure Configuration / MFA) · Microsoft RDP hardening guidance · NIST SP 800-115

F-03 — Microsoft 365 legacy authentication still permitted

HIGH

CVSS V3.1

7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

AFFECTED ASSET

Microsoft 365 tenant for example.com

DESCRIPTION

Conditional Access did not block legacy authentication protocols (IMAP, POP, SMTP AUTH, older Office clients). Legacy protocols do not support modern MFA prompts, so a stolen or sprayed password can access mailboxes even when MFA is enabled for browser and modern app sign-ins. Several privileged and shared mailboxes still had MFA registration incomplete.

EVIDENCE (MOCK, REDACTED)

```
Tenant: example.onmicrosoft.com (sample)
MFA status (Entra ID / Security defaults review):
- Modern auth MFA: enabled for interactive browser sign-in
- Legacy auth (IMAP/POP/SMTP AUTH): ALLOWED
- Conditional Access "Block legacy authentication": NOT PRESENT
- Users without registered MFA methods: 4 (incl. frontdesk@example.com)
Sign-in logs (sample, redacted): IMAP success from atypical ASN – password only
Policy recommendation: Block legacy auth + require MFA for all users and admins
```

BUSINESS IMPACT

Mailbox access exposes patient communications, insurance correspondence, and password-reset links. Email compromise is a leading path to business email compromise (BEC) and fraudulent wire instructions.

REMEDIATION

1. Create Conditional Access policies to block legacy authentication tenant-wide.
2. Require MFA for all users, with stronger methods for admins (phishing-resistant where feasible).
3. Disable SMTP AUTH per-mailbox except where a documented application needs it.
4. Review sign-in logs weekly for legacy protocol successes after the change.

REFERENCES

Microsoft: Block legacy authentication with Conditional Access · CIS Microsoft 365 Foundations Benchmark · NIST SP 800-63B

F-04 — Weak domain password policy and credential reuse

MEDIUM

CVSS V3.1

6.5 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

AFFECTED ASSET

Active Directory — example.local (198.51.100.10)

DESCRIPTION

Domain password policy allowed short passwords without complexity enforcement sufficient for modern threats. During authorized internal testing, a service account password matched a password previously observed in a public breach corpus for a similar username pattern, and the same secret unlocked a secondary admin utility account—indicating credential reuse.

EVIDENCE (MOCK, REDACTED)

```
Default Domain Policy (excerpt, sample):
  Minimum password length: 8
  Password complexity: disabled
  Maximum password age: 365 days
  Fine-grained policies: none for admins
---
Internal test (authorized):
  Account: svc-backup (198.51.100.10)
  Observation: password matched weak pattern; reused on util-admin
  Secrets redacted — proof captured via successful LDAP bind only
  No ticket dumping or lateral movement beyond proof
```

BUSINESS IMPACT

Weak and reused passwords make password spraying and secondary account takeover far easier once an attacker has any foothold on the LAN or VPN.

REMEDIATION

1. Raise minimum length (14+ recommended for humans; longer random secrets for service accounts).
2. Enable complexity or, preferably, ban common passwords via Entra Password Protection / similar.
3. Use unique vaulted passwords for every admin and service account; prefer managed service accounts / gMSA.
4. Implement MFA for VPN and privileged access; monitor for spray patterns.

REFERENCES

CIS Password Policy Guide · Microsoft: Password guidance · NIST SP 800-63B

F-05 — Missing DMARC policy on example.com

MEDIUM

CVSS V3.1

5.3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

AFFECTED ASSET

DNS — example.com (email authentication)

DESCRIPTION

SPF and DKIM were present for the primary mail flow, but no DMARC record was published. Without DMARC, receiving servers lack a clear policy for handling spoofed messages that fail authentication, and the practice cannot easily monitor spoofing attempts.

EVIDENCE (MOCK, REDACTED)

```
$ dig TXT example.com +short
"v=spf1 include:spf.protection.outlook.com -all"

$ dig TXT selector1._domainkey.example.com +short
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBA...[redacted]..."

$ dig TXT _dmarc.example.com +short
;; no DMARC record found

Recommendation start: v=DMARC1; p=none; rua=mailto:dmarc@example.com
Then advance to p=quarantine / p=reject after reviewing reports
```

BUSINESS IMPACT

Attackers can more easily impersonate the practice in phishing aimed at patients, vendors, or staff. Many cyber-insurance applications specifically ask whether DMARC is configured.

REMEDIATION

1. Publish a DMARC record at `_dmarc.example.com` starting with `p=none` and a reporting address.
2. Review aggregate reports for a few weeks; fix legitimate senders missing SPF/DKIM.
3. Move policy to quarantine then reject.
4. Document the control for insurance and customer questionnaires.

REFERENCES

RFC 7489 (DMARC) · DMARC.org overview · CIS Controls — Email and Web Browser Protections

F-06 — SMB signing not required on file server

LOW

CVSS V3.1

3.1 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

AFFECTED ASSET

files.example.local — 198.51.100.20 (SMB)

DESCRIPTION

The internal file server accepted SMB connections without requiring signing. On a shared network segment, this can enable certain man-in-the-middle and relay-related attack paths when combined with other weaknesses.

EVIDENCE (MOCK, REDACTED)

```
Target: 198.51.100.20
Protocol: SMB2/SMB3
Signing required: False
Signing enabled: True (but not mandatory)
Null session: denied
Shares enumerated with authorized low-priv test account only
---
Recommendation: RequireSecuritySignature = 1 (server & client)
Validate line-of-business apps after enabling
```

BUSINESS IMPACT

Alone this is limited, but it weakens internal defenses if an attacker is already on the LAN. Closing it is a low-effort hardening step insurers and assessors view favorably.

REMEDIATION

1. Enable and require SMB signing via Group Policy on servers and workstations.
2. Disable SMBv1 everywhere it still exists.
3. Prefer SMB encryption for sensitive shares where supported.
4. Retest after rollout to confirm signing is mandatory.

REFERENCES

Microsoft: Overview of Server Message Block signing · CIS Windows Server Benchmarks · NIST SP 800-115

Retest

The SMB Pentest package includes a retest within **45 days** of the final report. The purpose is to verify that agreed remediations are in place and to update finding status for ownership, the MSP, and cyber-insurance documentation.

What the retest covers

- Re-check of each finding marked for remediation (configuration, patch level, MFA/Conditional Access, DNS/email auth, SMB signing).
- Confirmation that public RDP exposure is removed or MFA-gated.
- Spot-check that no obvious regression reopened a closed issue.
- Updated findings table and, when appropriate, an attestation letter for insurers or auditors.

Sample retest tracker

ID	Finding	Owner	Target	Retest result
F-01	Forminator CVE-2023-4596	MSP / web	Immediate	Pending
F-02	Exposed RDP without MFA	MSP	Immediate	Pending
F-03	M365 legacy auth	MSP / IT lead	This sprint	Pending
F-04	Password policy / reuse	IT lead	30 days	Pending
F-05	DMARC missing	MSP / DNS	14 days	Pending
F-06	SMB signing	MSP	30 days	Pending

How to schedule. When remediations are ready, email the Northline engagement contact. Retest results are delivered as a short addendum plus an optional attestation letter (see next page for a sample).

Attestation Letter (Sample)

The following page illustrates the style of letter Northline can provide after a completed engagement and successful retest. Names and systems below are fictional.

NORTHLINE DIGITAL

Northline Digital LLC
29311 Ann Arbor Trl Unit #1001
Westland, MI 48185
northlinesec.com

Re: Penetration testing attestation — Example Dental Group LLC (sample)

Report ID: NL-SAMPLE-EDG-001

To Whom It May Concern:

Northline Digital LLC conducted a penetration test for **Example Dental Group LLC** under our SMB Pentest package. Testing was performed by Christopher Smith (MS in Cyber Security, CEH) in accordance with a signed statement of work and rules of engagement. Methodology aligned with NIST SP 800-115 and the OWASP Web Security Testing Guide.

Scope included internet-facing hosts under example.com, remote access services, a Microsoft 365 configuration review, and a limited internal network segment. Testing was manual and non-destructive.

Findings were reported to the client with severity ratings (CVSS v3.1 plus business impact), evidence, and remediation guidance. A retest window of 45 days is included to verify remediation of agreed items.

This sample letter is provided for illustration. A production attestation references the actual client, dates of testing and retest, and the final status of each finding after verification.

Christopher Smith

Principal, Penetration Tester
Northline Digital LLC