WHITE PAPER

Demystifying SMB Penetration Testing

A Practical Guide for Small and Medium-Sized Businesses

What penetration testing is, why SMBs need it, how to scope the right engagement, how to read the deliverables, and how to choose a provider that fits your budget and goals.

Version 1.0

Prepared By Lorikeet Security

lorikeetsecurity.com

OVERVIEW

1. Executive Overview

Small and medium-sized businesses are disproportionately targeted by attackers. SMBs have real data and real money — but without enterprise-scale security budgets. Penetration testing is one of the most effective tools SMBs can deploy to understand their true exposure before attackers do.

> **The SMB Threat Reality**
>
> 61% of SMBs reported a cyberattack in the past year. The average breach cost for small businesses exceeded $150,000 — enough to permanently close many organizations.

COMPARISON

2. Penetration Testing vs. Vulnerability Scanning

Penetration Testing	Vulnerability Scanning
Performed by skilled human testers with manual techniques.	Performed automatically by scanning software.
Validates whether vulnerabilities are actually exploitable.	Identifies potential vulnerabilities without confirming exploitability.
Simulates realistic attack chains from recon through exploitation.	Produces a list of detected issues sorted by CVSS score.
Includes proof-of-concept evidence and business impact analysis.	Includes CVE references and vendor patch links.
Recommended annually or after significant infrastructure changes.	Recommended continuously or quarterly as a detection baseline.

TYPES

3. Common Testing Types for SMBs

Type	Description
External Network	Tests internet-facing infrastructure — firewalls, VPNs, exposed services, and cloud-hosted systems. The entry point for most SMB programs.
Internal Network	Simulates a compromised endpoint or malicious insider. Tests lateral movement, privilege escalation, and access to sensitive data from inside the network.
Web Application	Covers web apps, customer portals, and SaaS products. Identifies OWASP Top 10 vulnerabilities including injection, broken auth, and IDOR.
Phishing / Social Engineering	Tests employee susceptibility to phishing campaigns. Particularly valuable for SMBs where security awareness training is limited.

Type	Description
Cloud Configuration Review	Assesses AWS, Azure, or GCP for misconfigurations: exposed storage, over-permissive IAM, and insecure defaults.
Vibe Coding / AI Code Review	Right-sized security review for apps built with Lovable, Claude, or Cursor. Catches hardcoded secrets, missing auth, and wide-open APIs common in AI-generated code.

SCOPING

4. How to Scope a Penetration Test

- Define the target inventory: List all IP ranges, domains, web applications, and cloud environments in scope.
- Choose the testing model: Black-box (no prior knowledge), gray-box (credentials provided), or white-box (full source access) based on budget and objectives.
- Set testing windows: Identify whether production testing is acceptable. Establish low-traffic windows for destructive test cases.
- Agree on rules of engagement: Define what is off-limits and confirm emergency contact procedures.
- Define success: Determine what findings would be most valuable — compliance evidence, specific attack path validation, or comprehensive coverage.

DELIVERABLES

5. Understanding the Deliverables

Deliverable	Description
Executive Summary	Non-technical summary of overall risk posture and recommended priorities. Written for leadership.
Technical Findings	Each finding includes CVSS severity, reproduction steps, evidence (screenshots, request/response logs), and remediation guidance.
Remediation Roadmap	Prioritized action plan grouped by severity and effort, enabling effective resource allocation.
Attestation Letter	Signed letter confirming scope and completion — suitable for auditors, insurers, and enterprise customers.
Free Retest	Lorikeet Security includes retest at no additional cost within 30 days to verify critical and high findings are resolved.

HOW WE HELP

6. Why Lorikeet Security for SMBs

- Right-sized engagements: We scope to your actual environment and budget — not an enterprise template.
- Manual testing by experienced researchers: No automated scanners, no false positives. Real findings that matter.
- Free retesting included: Fix the issues, we verify the fix and update your report. No extra charge.
- Audit-ready reports: Formatted for SOC 2, PCI-DSS, ISO 27001, and HIPAA auditors out of the box.
- 24-hour proposal turnaround: Tell us about your project and receive a custom proposal within one business day.

Get Started

Contact Lorikeet Security at lorikeetsecurity.com or call (689) 202-3940 to discuss your first or next penetration test. No commitment required — we'll send a proposal within 24 hours.