WHITE PAPER

Penetration Testing vs Vulnerability Scanning

Understanding the Difference and When to Use Each

A comprehensive breakdown of penetration testing and vulnerability scanning: how they work, what they find, when to use each, and how to build a proactive security program that leverages both.

Version 1.0

Prepared By Lorikeet Security

lorikeetsecurity.com

OVERVIEW

1. Executive Overview

Vulnerability scanning and penetration testing are both proactive security tools — but they are fundamentally different activities with distinct outputs, use cases, and audiences. Conflating them leads to misaligned security investments and false confidence.

SCANNING

2. Vulnerability Scanning: What It Is

A vulnerability scan is an automated process that compares a target environment against a database of known CVEs, misconfigurations, and weaknesses. Scanners probe systems for open ports, service versions, and configurations, then cross-reference against vulnerability databases.

> **Key Limitation**
>
> Vulnerability scanning tells you what might be vulnerable. It does not confirm exploitability, business impact, or how vulnerabilities chain together into real attack paths.

PENTEST

3. Penetration Testing: What It Is

A penetration test is a structured, authorized simulation of a real-world attack. Skilled testers combine automated tooling with manual techniques to identify, exploit, and chain vulnerabilities into realistic attack paths with confirmed business impact.

COMPARISON

4. Side-by-Side Comparison

Attribute	Vulnerability Scanning	Penetration Testing
Execution	Automated	Manual + tool-assisted
Exploitability Confirmation	No	Yes — actively exploited
Attack Path Simulation	No	Yes
Output	List of potential vulnerabilities	Exploited findings with proof of concept
False Positive Rate	High — requires triage	Low — findings are validated
Recommended Frequency	Continuous / monthly	Annual or change-triggered
Compliance Use Case	Continuous monitoring	Point-in-time attestation

Relative Cost	Low (tooling)	Higher (skilled labor)

WHEN TO USE

5. When to Use Each

Use Vulnerability Scanning When...	Use Penetration Testing When...
You need continuous visibility across a large infrastructure footprint.	You need to confirm that vulnerabilities are actually exploitable.
You want to track remediation velocity over time.	You are preparing for a compliance audit (PCI DSS 11.3, SOC 2, ISO 2700
You need a cost-effective detection baseline.	You have launched a new application, API, or major feature.
You are meeting continuous monitoring control requirements.	You are pursuing cyber insurance or enterprise vendor qualification.

PROGRAM DESIGN

6. Building a Program That Uses Both

- Run continuous or monthly vulnerability scans to maintain baseline visibility and track remediation.
- Conduct annual penetration tests against your most critical assets to validate exploitability.
- Use penetration test findings to calibrate scanner thresholds and prioritize remediation.
- Trigger additional penetration tests on significant changes: new product launches, cloud migrations, major feature releases.
- Use scan data between tests to track remediation progress and identify emerging exposure.

> **How Lorikeet Security Helps**
>
> Lorikeet Security provides both penetration testing and vulnerability scanning services designed to complement each other. Our findings are suitable as compliance evidence across PCI DSS, SOC 2, HIPAA, and ISO 27001. Contact us at lorikeetsecurity.com.