■ SERVICE BRIEF

External Penetration *Testing*

re

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's External Penetration Testing services. These services simulate real-world cyberattacks on externally accessible systems to identify vulnerabilities and provide actionable remediation guidance.

This service engagement is governed by this Service Brief and associated with SKU: SEC-PENEXT.

The quantity defined in the quote determines the number of external IPs to be tested under this engagement.

The *future* belongs to the *curious*.

Table of Contents

01. Services Overview

Redesign's External Penetration Testing Services assess the security posture of customer-facing infrastructure by identifying vulnerabilities in publicly accessible systems and services. Testing simulates attacker behavior while taking reasonable measures to avoid disruption to production systems. This service follows frameworks such as OWASP, NIST SP 800-115, and MITRE ATT&CK.

The services are divided into distinct stages:

- Pre-Engagement Planning
- Reconnaissance & Enumeration
- Vulnerability Analysis
- Exploitation & Validation
- Reporting & Close-Out

The engagement is considered complete upon delivery of the final Penetration Testing Report and completion of the Findings Review Session.

02. Offer Structure

PRIMARY SERVICES

- Includes scoping, testing, analysis, and reporting of the defined number of external IP addresses under the associated SKU.

OPTIONAL ADD-ONS

Separate SOW

May include:

- Social engineering
- Web app testing
- Red teaming
- Or internal infrastructure testing

03. Project Scope

This engagement includes penetration testing of the Customer's internet-exposed infrastructure. The scope is governed by the quantity of external IPs specified in the associated quote and SKU.

In-Scope Assets:

- **Public IP addresses explicitly authorized for testing**
- **Associated domains, services, and basic web apps (surface-level enumeration only)**
  - Surface-level enumeration includes identification of exposed endpoints, technologies, and misconfigurations, but does not include authenticated testing, business logic testing, or full OWASP Top 10 coverage.
- **Cloud-hosted external assets (owned or managed by Customer), subject to any required authorization or approval from the applicable cloud service provider or third-party infrastructure owner**

Requirements:

- **Assets must be reachable from the public internet**
- **Legal ownership or contractual authorization for all in-scope systems**
- **Testing must align with Customer's internal risk management and approval processes**

All devices must be functional, supported, and reachable for inclusion.

04. Quantity & Effort Model

- **Service SKU: SEC-PENEXT**
- **Quantity: Number of external IP addresses covered under this engagement referenced in quote**
- **Work per Unit:**
  - Asset discovery and mapping
  - Vulnerability scanning and validation
  - Manual verification of key issues
  - Reporting for each tested IP

Example: A quantity of 10 under SKU: SEC-PENEXT authorizes testing of 10 external IP addresses. Any increase in IP count requires a Change Request (CR).

MONTHLY SUPPORT TERMS

This service includes up to the number of hours specified in the associated quote for operational support per month, limited to the activities defined in this Service Brief.

Unused hours do not carry over to subsequent months. Additional support hours may require a revised quote or a separate Statement of Work (SOW).

05. Services & Key Activities

Stage	Key Activities
Pre-Engagement Planning	▪ Confirm authorized targets ▪ Finalize Rules of Engagement ▪ Schedule test window ▪ Assign primary technical contact
Reconnaissance & Enumeration	▪ Identify public IPs, domains, and services ▪ Perform DNS and WHOIS queries ▪ Map external attack surface
Vulnerability Analysis	▪ Run authenticated and unauthenticated scans ▪ Authenticated testing is performed only if Customer-provided credentials are explicitly authorized and supplied in advance. ▪ Analyze results manually ▪ Severity ratings are assigned by Redesign based on CVSS scoring, threat intelligence, exploitability, and observed risk context.
Exploitation & Validation	▪ Attempt safe exploitation of verified vulnerabilities ▪ Gather evidence (screenshots, logs) ▪ Assess actual risk
Reporting & Close-Out	▪ Deliver formal Penetration Testing Report ▪ Host findings review session with Customer ▪ Provide remediation guidance

06. Deliverables

Rules of engagement (ROE) document

External penetration testing report, including:

- Executive Summary
- Technical Findings with Prioritized Severity Rankings
- Proof-of-Concept Evidence
- Remediation Recommendations

Findings review session (virtual, 1 hour)

07. Services Scope Changes

Changes to the authorized IP list, schedule, or volume may result in scope or cost adjustments and require a Change Request (CR).

08. Services Scope Exclusions

This engagement does not include:

- **Internal network penetration testing**
- **Web application testing beyond enumeration full OWASP Top 10 analysis)**
- **Denial of Service (DoS) or stress testing**
- **Social engineering or phishing simulations**
- **Source code review**
- **Configuration changes or remediation activities**
- **Testing of third-party infrastructure not owned or authorized by the Customer**
- **Red Team/Adversary Simulation exercises**

09. Customer Responsibilities

Maintain valid vendor support agreements:

- **Authorization: Provide explicit, written authorization for each in-scope IP address.**
- **Third-Party Authorization: Customer is responsible for confirming and obtaining any required approvals from cloud service providers (e.g., public cloud platforms) or third-party infrastructure owners before penetration testing is performed.**
- **System Ownership: Ensure all systems in-scope are owned or contractually managed by the Customer.**
- **Access and Support: Assign a technical contact to coordinate during the testing window.**

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

10. Services Schedule

- **Start Date:** Confirmed after Redesign receives a signed quote and completed ROE document
- **Testing Window:** Dependent on quantity of IPs and complexity
- **Report Delivery:** Within 14 business days following test completion
- **Completion:** Customer signs off via DocuSign upon receipt of final deliverables

---

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

- www.redesign-group.com/legal

ONSITE SERVICES WILL NOT BEGIN UNTIL THE FOLLOWING PREREQUISITES ARE MET

- A signed quote referencing SKU: SEC-PENEXT and the agreed quantity of external IPs
- A completed and signed Rules of Engagement (ROE) document
- A verified list of in-scope assets authorized for testing

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

redesign

The *future* belongs
to the *curious*.

↗ redesign-group.com