Penetration Testing Agreement

Parties

Client: ParoCyber

Pentester: Nsonta

1. Purpose

This agreement defines the scope, rules of engagement, and deliverables for penetration testing services to assess the security posture of ParoCyber's IT infrastructure, including resilience against ransomware attacks.

2. Scope of Engagement

Systems in Scope:

- Ecommerce services hosted on public cloud platforms.
- Communications, warehousing, and shipping IT services managed in-house.
- Local datacenter located in Houston, comprising: 25 servers divided into Administration, Operations, and Logistics clusters.
- Development Microsoft SQL Server (configured identically to production) included for database testing.

Testing Objectives:

- ✓ Identify vulnerabilities that could allow privilege escalation from end-user accounts to administrative access.
- ✓ Validate security controls on operations and logistics clusters.
- ✓ Ensure software and operating systems are up-to-date and free of known vulnerabilities.
- ✓ Assess resilience against social engineering attacks targeting warehouse and operations staff.
- ✓ Simulate ransomware attack scenarios to evaluate detection, containment, and recovery capabilities without causing actual data loss.

3. Rules of Engagement

Access Method: Internal access provided via isolated VLAN within IT department.

Testing Restrictions:

Disruptive tasks (e.g., load testing, DoS simulations, ransomware simulation) must only occur during the scheduled maintenance window: Friday, Saturday, Sunday: 2:00 AM – 6:00 AM CST.

Non-disruptive tests may be conducted during normal business hours.

Production System Protection: Testing must not impact Amazon storefront clusters or production inventory systems.

Social Engineering: Email-based phishing simulations permitted using provided staff email list. End users will not be informed of testing activities.

Confidentiality: NDA must be signed prior to engagement. Only designated IT staff will be aware of testing schedule.

4. Deliverables

I. Weekly Updates: Progress reports and teleconference with IT Director, Warehouse Manager, and Operations Manager.
II. Final Report: Comprehensive penetration test report delivered within 60 days of contract signing, including vulnerability findings, ransomware simulation results, and recommendations for remediation and hardening.

5. Timeline

- Engagement begins two weeks after contract and NDA signing.

- Testing and reporting must be completed within agreed timeframe.

6. Legal & Compliance

- Testing will adhere to industry standards (OWASP, PTES, ISO 27001).
- Pentester agrees to avoid any activity outside the defined scope.
- Client agrees to provide necessary access and resources.

7. Signatures

Client Representative:
Name: _____
Title: _____
Signature: _____
Date: _____

Pentester:
Name: Nsonta
Title: Penetration Tester
Signature: _____
Date: _____