PENETRATION TESTING AGREEMENT

ParoCyber

4th December,2025

Introduction 3
Purpose of the Engagement 4
Scope 4
Types 4
Assets 5
Out-of-Scope 5
Rules of Engagement (RoE) 5
Testing Window 5
Communication Protocols 5
Handling of Sensitive Information 5

Third-Party Involvement 6

Prohibited Activities 6

Legal Authorization 6

Responsibilities 6

Client Responsibilities 7

Pentester Responsibilities 7

Deliverables 7

Confidentiality Agreement 8

Liability and Limitations 8

Payment Terms 8

Termination Clause 9

Intellectual Property Rights 9

Acceptance & Authorization 9

Client: 10

Introduction

This Penetration Testing Agreement explains the terms and conditions for a student-led penetration test. This document sets clear expectations, boundaries, and responsibilities during the penetration test duration.

The purpose of the engagement is to identify security vulnerabilities and strengthen the Client’s security posture under mutually defined boundaries.

Purpose of the Engagement

This engagement seeks to evaluate the security posture of ParoCyber by testing the security controls implemented in ParoCyber. The pentest is to identify weaknesses within systems, networks, or applications in ParoCyber’s infrastructure as well as providing a score to measure the effectiveness of existing security controls.

The pentester at the end of this engagement is to provide recommendations to patch vulnerabilities found and strategies to mitigate the risks.

Scope

During this engagement the pentester is to perform their functions within the scope defined below; the scope defines assets, applications and types of activities authorized for this engagement.

Types

- Network penetration testing (internal/external)
- Web application testing
- API testing
- Social engineering (only if explicitly approved)
- Wireless security testing
- Cloud configuration review

Assets

- **Operating Systems**: Windows,Linux,MacOS
- **Databases**: MySQL, Oracle
- **Network**: 10.10.7.0/24, 192.168.1.0/24 (VPN), Parocyber.com
- **Applications**: Web Applications, Azure

Out-of-Scope

The pentester shall not test the following systems:

- Third party Databases
- Physical Assets

Rules of Engagement (RoE)

The following rules apply during the engagement:

Testing Window

Testing may be conducted between:
Start Date: 4th December,2025
End Date: 30th December,2025

Communication Protocols

- Emergencies must be reported immediately to the Client's security contact via the provided phone or email.
- Daily or weekly status updates will be provided as requested.

Handling of Sensitive Information

- All data accessed during testing will be kept strictly confidential.
- Data shall not be stored beyond the engagement period.

- No client information will be shared publicly.

Third-Party Involvement

The Pentester shall not involve any third party without written authorization.

Prohibited Activities

The Pentester is not permitted to:

- Execute denial-of-service (DoS/DDoS) attacks.
- Access or modify sensitive personal data.
- Cause system downtime or service disruption.
- Interfere with production-critical systems.

Legal Authorization

ParoCyber grants explicit written permission for the Pentester to perform all activities defined in the scope of this Agreement. This serves as a **"Get Out of Jail Free"** authorization, protecting the Pentester from legal liability related to authorized testing.

Any actions performed **outside the authorized scope** will not be protected under this Agreement.

Responsibilities

Client Responsibilities

ParoCyber agrees to:

- Provide accurate information needed for the pentest activity.
- Ensure system stability before testing begins.
- Notify internal teams to avoid false security alarms.
- Provide necessary credentials, tokens, or network access.

Pentester Responsibilities

Pentester agrees to:

- Conduct testing ethically and professionally.
- Perform all assessments with minimal system interference.
- Document findings with clarity and accuracy.
- Immediately report discovered critical vulnerabilities.
- Maintain confidentiality at all times.

Deliverables

At the end of the engagement, pentester is to provide:

Final Report, containing:

- Executive summary
- Methodology
- Detailed vulnerability findings
- Risk ratings (CVSS-based)
- Screenshots and evidence
- Remediation recommendations

Debrief Session

A short walkthrough session (online or in-person) to explain what I found and what it means.

Confidentiality Agreement

Both parties agree to maintain confidentiality regarding:

- Testing methods
- System details
- Vulnerabilities discovered
- Credentials or access tokens
- Final reporting materials

This confidentiality obligation shall extend beyond the termination of this Agreement.

Liability and Limitations

- System reactions may be unpredictable. Therefore, I cannot be held liable for unintended issues that arise from normal, approved testing steps.
- The Client acknowledges inherent risks associated with penetration testing.
- Any claims must be made within **30 days** after report delivery.

Payment Terms

Payment is due within **30 days** of invoice unless otherwise agreed.

Termination Clause

Either party may terminate this Agreement with **written notice** if:

- Scope violations occur
- Security risks become unacceptable
- Mutual agreement is breached

Upon termination, all work will cease and all client data will be securely deleted.

Intellectual Property Rights

- The Client retains ownership of all systems, data, and assets tested.
- The Pentester retains ownership of testing methodologies.
- Final reports belongs to the Client.

Acceptance & Authorization

By signing below, both parties acknowledge and agree to the terms of this Penetration Testing Agreement.

Client:

Name: ParoCyber
Title: Peneration Testing Agreement
Signature: ___________________________________
Date: 4th December,2025

Pentester:

Name: Selinam Fudzi-Amesu
Signature: ___________________________________
Date: 4th Decembr,2025

End of Agreement