This document outlines the test methodology used in the penetration testing project, based on the PTES (Penetration Testing Execution Standard). It includes scope, objectives, tools, timeline, and documentation used for a full engagement simulation.

Scope of Engagement

- Type of Test: Internal Lab-Based Penetration Test
- Tester: Saad Laksabi
- Environment: UTM Virtual Machine running Parrot OS
- Target System IP: 10.0.2.15
- IP Range: 10.0.2.1 – 10.0.2.255 (Virtual Network)
- Tools Used: Nmap, Wireshark, Terminal, Parrot OS tools
- Out-of-Scope Assets: None (lab environment only)

This engagement focuses on internal reconnaissance and vulnerability scanning within a controlled lab network using virtual machines. No real or production systems are involved.

Penetration Test Plan - Saad Laksabi

1. Scope

- **Target IP(s):** 10.0.2.15 (Parrot OS VM)
- **Environment:** Virtual machine hosted in UTM on macOS
- **Testing Type:** Internal Network Penetration Test (Blackbox)

2. Objectives

- Discover active services and ports on the VM
- Identify potential vulnerabilities
- Document reconnaissance and scanning
- Simulate an attack using safe exploitation techniques

3. Timeline

- **Day 1:** Setup environment and perform reconnaissance
- **Day 2:** Conduct vulnerability scan and analysis
- **Day 3:** Document findings and prepare report

4. Deliverables

- Reconnaissance Report
- Vulnerability Assessment Report
- Exploitation Proof of Concept

- Final Penetration Test Report (PDF)

Authorization Statement: This penetration test is being performed by Saad Laksabi in a closed, controlled environment on a personal virtual machine for academic purposes. No unauthorized systems will be tested.

Testing Boundaries:

- Only the VM `10.0.2.15` is in scope
- No denial of service (DoS) attacks
- All actions are confined within the UTM VM