CYART

inquiry@cyart.io

www.cyart.io

Author: Harshal Harekar
Date: 15/10/2025

# PTES Report

## Executive Summary:

A full penetration test was conducted against the Kioptrix vulnerable virtual machine using Kali Linux. The objective was to simulate a realistic exploitation scenario, validate detection capabilities, and verify remediation steps in alignment with the PTES framework.

## Findings:

Initial reconnaissance using Nmap revealed multiple open ports, including Samba (port 139), Apache (port 80), and SSH (port 22). OpenVAS confirmed a critical vulnerability in the Samba service. Using Metasploit's "usermap_script" and "trans2open" exploits, a reverse shell was successfully obtained. Privilege escalation was achieved via a vulnerable SUID binary (/usr/bin/nmap), granting root access. Sensitive files such as '/etc/passwd' and '/etc/shadow' were collected and hashed using SHA-256 to preserve forensic integrity and support chain-of-custody documentation.

## Recommendations:

Upgrade Samba to a secure, supported version to eliminate known vulnerabilities. Disable unused services and restrict access to SMB ports (139/445) using firewall rules. Review and harden Samba configuration files to limit exposure. Enforce least privilege across user accounts and monitor for suspicious activity. A follow-up OpenVAS scan will confirm the successful remediation. Regular patching, vulnerability scanning, and service audits are recommended to maintain a secure environment and prevent future exploitation.