# Capstone Project: Full VAPT Cycle (Kioptrix VM)

Author: Harshal Harekar

Date: 14/10/2025

## Objective

Full VAPT cycle on Kioptrix/VulnHub VM: discovery, exploit, privilege escalation, evidence collection, remediation verification.

## Environment

* Attacker: Kali Linux (host-only)
* Target: Kioptrix VM (e.g., 192.168.56.150)
* Tools: Nmap, OpenVAS, Metasploit, Meterpreter,

## Discovery

1. Using netdiscover from kali

A computer screen shot of a computer code

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

2. Scan for services and OS detection

sudo nmap -sV -p- -O 192.168.18.139

A screenshot of a computer

AI-generated content may be incorrect.

3. OpenVAS scan

A screenshot of a computer

AI-generated content may be incorrect.

## Exploitation

The classic exploit for Samba (Kioptrix Level 1) is exploit/linux/samba/trans2open

Steps:

Launch msfconsole, use the exploit, set RHOSTS, LHOST, PAYLOAD and exploit.

A screen shot of a computer

AI-generated content may be incorrect.



A screenshot of a computer code

AI-generated content may be incorrect.



After exploiting, confirming the access

A screenshot of a computer

AI-generated content may be incorrect.

There is no need of Privilege Escalation, as we have already got root access.

## Evidence Collection

### Harvesting Files

1.cat /etc/passwd

A screenshot of a computer screen

AI-generated content may be incorrect.

2.cat /etc/shadow

A screenshot of a computer

AI-generated content may be incorrect.

### Hash Files

A computer screen shot of numbers

AI-generated content may be incorrect.

Log Table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Description | Collected By | Date | Hash Value |
| passwd file | user account information | VAPT Analyst | 14-10-2025 | bcb3cd6223a859e97e75e436923730408c09335dc08c6a02f439c25c0ef10fd4 |
| shadow file | hashed passwords for user accounts | VAPT Analyst | 14-10-2025 | 6578a00432b987151d02431ae8c96943674d415bd963048ebca1abee21e5cd31 |

## Remediation

The Samba service was found vulnerable to remote code execution via the ‘trans2open’ exploit. Remediation involves upgrading Samba to a secure version, disabling unnecessary shares, and restricting SMB access via firewall. A follow-up OpenVAS scan will confirm the successful mitigation.