Kioptrix Enumeration Summary

Target Host Information

Target IP: 192.168.59.130

Scan Tools Used: Nmap, Nikto

Operating System: Linux-based

Hostname: kioptrix.level1

Open Ports Identified (via Nmap)

Port 22 - SSH - OpenSSH 3.9p1 (protocol 1.99)

Port 80 - HTTP - Apache/2.0.52 (CentOS)

Port 139 - NetBIOS-SSN - Samba smbd 3.X - 4.X

Port 445 - Microsoft-DS - Samba smbd 3.X - 4.X

HTTP (Port 80) Enumeration

Nikto identified the following:

- Apache version is outdated: Apache/2.0.52 (CentOS)

- Directories found: /manual/, /icons/

- Directory listing enabled in /icons/

- No SSL detected

- Exposed to CVEs related to Apache 2.0.52

Full report available in nikto_scan.pdf

SMB Enumeration (Ports 139, 445)

Samba version likely 2.2.x

Exploitable using linux/samba/trans2open module in Metasploit

Key Findings

- Outdated Apache server exposed

- Vulnerable Samba service exploitable via Metasploit

- Potential for privilege escalation post-exploitation