# Technical Report – Vulnerability Assessment & Penetration Testing

## 1. Tools Used

• Kali Linux (Nmap, Nikto, Metasploit, OpenVAS, Burp Suite)  
• Nessus  
• OSINT tools (whois, theHarvester)  
• Manual testing via terminal and GUI

## 2. Information Gathering & Reconnaissance

Tools: whois, nslookup, theHarvester, Nmap  
Discovered open ports: 22, 80, 139, 445

## 3. Scanning & Enumeration

Windows: Detected SMB shares, OS version (Windows 10 Pro 21H2)  
Debian: Apache HTTP server version exposed, SSH service active

## 4. Vulnerability Assessment

Windows:  
• SMBv1 Enabled (CVE-2017-0143)  
• Outdated Adobe Reader  
Debian:  
• Apache RCE (CVE-2021-41773)  
• Weak SSH Ciphers

## 5. Exploitation

• Gained reverse shell on Debian via Apache exploit (CVE-2021-41773)  
• Enumerated user credentials on Windows via SMB null session  
  
\*\*Note: Screenshots and PoC videos can be provided upon request.\*\*

## 6. Analysis and Risk Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| System | Vulnerability | Exploitable? | CVE ID | Risk Level | PoC Available |
| Windows 10 | SMBv1 enabled | Yes | CVE-2017-0143 | Critical | ✔️ |
| Debian | Apache RCE | Yes | CVE-2021-41773 | High | ✔️ |
| Debian | Weak SSH Cipher | No | - | Medium | ❌ |

## 7. Remediation Plan

|  |  |  |
| --- | --- | --- |
| Vulnerability | Remediation Steps | Priority |
| SMBv1 Enabled | Disable SMBv1 via Windows Features or registry | High |
| Apache RCE | Update Apache to the latest version | High |
| Weak Passwords | Implement strong password policies and enforce MFA | High |
| Weak SSH Ciphers | Update SSH config to use strong ciphers only | Medium |
| Outdated Software | Implement patch management | Medium |