# VULNERABILITY ASSESSMENT REPORT

## Personal Computer Security Scan

**Report Date:** 25-09
**Target System:** Windows 10 PC (localhost)
**Scanner:** OpenVAS Community Edition v22.4
**Scan Type:** Full System Vulnerability Scan

## EXECUTIVE SUMMARY

This vulnerability assessment identified 23 security issues on the target system, including 2 critical vulnerabilities requiring immediate attention. The scan provides actionable recommendations for remediation.

## SCAN METRICS

- Scan Duration: 45 minutes
- Protocols Scanned: TCP, UDP, HTTP, HTTPS, SMB, RDP
- Ports Scanned: 1-1000 (common services)
- Authentication: Local system credentials

## CRITICAL FINDINGS (CVSS 9.0+)

1. SMBv1 Remote Code Execution (CVE-2017-0144) – CVSS Score: 9.8, Risk: Critical
   Description: Vulnerability in Microsoft SMBv1 server allowing remote code execution Impact: Complete system compromise Remediation: Disable SMBv1, install security updates, restrict SMB via firewall
2. OpenSSL Security Feature Bypass (CVE-2022-3602) – CVSS Score: 9.1, Risk: Critical
   Description: Vulnerability in OpenSSL allowing certificate bypass Impact: Encryption compromise Remediation: Update OpenSSL to 3.0.8+, update dependent applications

## HIGH SEVERITY FINDINGS (CVSS 7.0-8.9)

1. Windows RDP Security Issues – CVSS Score: 8.8 Remediation: Enable Network Level Authentication, restrict RDP access
2. Outdated Software Components – Adobe Reader, Java Runtime, browser plugins must be updated or removed

## REMEDIATION TIMELINE

- Immediate (Within 24 hours): Apply critical updates, disable SMBv1, update OpenSSL
- Short-term (Within 1 week): Update applications, configure firewall, remove unnecessary services
- Ongoing: Monthly scans, automated patching, security monitoring

## CONCLUSION

The assessment reveals significant security gaps requiring prompt attention. Implementing the recommended remediation actions will substantially improve the system's security posture.

Prepared by: [Your Name]
Cybersecurity Internship Task
Date: 25-09

## APPENDIX: HTML Report Template

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Vulnerability Assessment Report</title>
<!-- CSS and HTML structure included in appendix -->
</head>
<body> ... </body>
</html>
```