Simulated Nessus Vulnerability Scan Report

Generated on: 2025-09-25 11:08 UTC
Scanner: Nessus (simulated)
Scanned targets: 127.0.0.1 (localhost)

Executive Summary

This document is a simulated Nessus-style vulnerability scan report generated for coursework/demo purposes. The scan target is a localhost system (127.0.0.1). Findings are realistic in style but are NOT based on a live scan. Use this report only as an example to include in deliverables where a simulated report is acceptable.

Total Findings (simulated)	**8**
Critical	1
High	2
Medium	3
Low	2

Findings Summary (Top entries)

ID	Title	Port	Risk	CVSS	CVE
1	OpenSSL Heartbleed-like Vulnerability (Simulat	ed)443/tcp (https)	High	7.5	
2	SMBv1 Server Enabled	445/tcp (microso	ft-dsCritical)	9.1	
3	Outdated Apache HTTP Server (Directory Trave	rsal Risk)80/tcp (http)	Medium	6.8	
4	Weak SSH Ciphers and MAC Algorithms	22/tcp (ssh)	Medium	5.3	N/A (configuratio
5	Default Credentials — Web Management Interfa	ce8080/tcp (http-pr	oxy)High	8.0	N/A (auth issue)
6	Insecure HTTP (Missing HSTS and TLS Weakn	esses)80/tcp http)	Low	4.3	N/A (configuratio
7	Outdated SMB Client Signing Not Required	445/tcp (microso	ft-dsMedium)	6.5	N/A (configuratio
8	Localhost Unnecessary Service: FTP Running	21/tcp (ftp)	Low	3.7	

CVE
2014
0160
(example

N/A

(configuration issue)

CVE-2017-9798 (example

N/A (insecure service)

Finding 1: OpenSSL Heartbleed-like Vulnerability (Simulated)

Finding 2: SMBv1 Server Enabled

Risk	High
CVSS (simulated)	7.5
CVE	CVE-2014-0160 (example)
Port / Service	443/tcp (https)
Evidence	OpenSSL 1.0.1f detected in service banner (simulated)
Description	A simulated Heartbleed-like memory disclosure vulnerability allowing remote attackers to read s
Remediation	Upgrade OpenSSL to a version without the heartbeat vulnerability (e.g., >=1.0.1g). Apply vendo
Risk	Critical
CVSS (simulated)	9.1
CVE	N/A (configuration issue)
Port / Service	445/tcp (microsoft-ds)
Evidence	SMBv1 protocol detected via banner (simulated)
Description	SMBv1 is insecure and has known critical vulnerabilities (e.g., WannaCry).
Remediation	Disable SMBv1 on the host and enable SMBv2/SMBv3. Apply all OS security updates.

Finding 3: Outdated Apache HTTP Server (Directory Traversal Risk)

Finding 4: Weak SSH Ciphers and MAC Algorithms

Risk	Medium
CVSS (simulated)	6.8
CVE	CVE-2017-9798 (example)
Port / Service	80/tcp (http)
Evidence	Apache/2.2.15 detected in server header (simulated)
Description	Older Apache versions may be susceptible to directory traversal and other issues.
Remediation	Update Apache to the latest stable release, review document root permissions, and disable moc

Finding 5: Default Credentials — Web Management Interface

Risk	High
Risk	Medium
CVSS (simulated)	5.3
CVE	N/A (configuration)
Port / Service	22/tcp (ssh)
Evidence	Server supports 3des-cbc, hmac-sha1 (simulated)
Description	The SSH service is allowing weak ciphers and MACs which can be susceptible to cryptographic
Remediation	Reconfigure SSH to use strong ciphers (e.g., aes256-gcm@openssh.com) and strong MACs. R

Finding 6: Insecure HTTP (Missing HSTS and TLS Weaknesses)

CVSS (simulated)	8.0
CVE	N/A (auth issue)
Port / Service	8080/tcp (http-proxy)
Evidence	Default admin:admin credentials accepted on /admin (simulated)
Description	Web management interface accessible with default credentials allowing administrative access.
Remediation	Change default passwords, enforce strong password policy, restrict management interface to tru

Finding 7: Outdated SMB Client Signing Not Required

Risk	Low
CVSS (simulated)	4.3
CVE	N/A (configuration)
Port / Service	80/tcp (http)
Evidence	No HSTS header; TLS 1.0 supported (simulated)
Description	HTTP connections and weak TLS versions expose traffic to interception and downgrade attacks
Remediation	Redirect HTTP to HTTPS, enable HSTS, and disable TLS 1.0/1.1. Use TLS 1.2+ and modern ci
Risk	Medium
CVSS (simulated)	6.5
CVE	N/A (configuration)
Port / Service	445/tcp (microsoft-ds)
Evidence	SMB signing not required (simulated)
Description	SMB client signing not required may allow man-in-the-middle attacks on SMB sessions.
Remediation	Require SMB signing via group policy or system config and ensure clients are updated.

Finding 8: Localhost Unnecessary Service: FTP Running

Risk	Low
CVSS (simulated)	3.7
CVE	N/A (insecure service)
Port / Service	21/tcp (ftp)
Evidence	FTP service banner: vsftpd 2.0.5 (simulated)
Description	FTP transmits credentials in cleartext. Unnecessary services increase attack surface.
Remediation	Disable FTP if not required or replace with SFTP (SSH-based). Enforce secure file transfer meth