

Basic Vulnerability Scan Report

1. Scan Information

- **Tool Used:** Nessus Essentials
 - **Scan Type:** Basic Network Scan
 - **Target System:** Metasploitable (virtual machine)
 - **Date Performed:** 17-11-2025
-

2. Summary of Findings

Severity

Count

Critical 7

High 11

Medium 36

Low 7

Informational 148

3. Detected Vulnerabilities

Critical ()

1. **SSL(MULTIPLE ISSUES)**
 2. **Bind Shell Backdoor Detection**
 3. **NFS exported share information disclosure**
 4. **Unix Operation System Unsupported Version Detection**
 5. **VNC Server Password**
-

High ()

1. **Apache TOMCAT AJP Connector Request Injection (Ghostcat).**
 2. **rlogin Service Detection**
-

Mixed ()

1. **ISC BIND (Multiple Issues)**

- 2. SSL (Multiple Issues)**
 - 3. TWIKI (Multiple Issues)**
 - 4. DNS (Multiple Issues)**
 - 5. HTTP (Multiple Issues)**
-

4. Recommendations

1. Install all pending OS security updates.
2. Disable deprecated protocols (SMBv1, TLS 1.0).
3. Remove unused services and close unnecessary ports.
4. Enable strong passwords and MFA where possible.
5. Regularly run vulnerability scans monthly.

Vulnerabilities 85			
<input type="checkbox"/> Sev	Name	Family	Count
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
MIXED	DNS (Multiple Issues)	DNS	6
MIXED	ISC Bind (Multiple Issues)	DNS	4
MIXED	Phpmysqladmin (Multiple Issues)	CGI abuses	4
MIXED	SSL (Multiple Issues)	Service detection	3
MIXED	PHP (Multiple Issues)	CGI abuses	3
MIXED	Twiki (Multiple Issues)	CGI abuses	2
HIGH	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1