OpenVAS Vulnerability Report

Target: 192.168.29.155 (Metasploitable2)
Date: 2025-09-10
Scanner: OpenVAS 22.9.0

Scan Summary:

Host Status	Up
Operating System	Linux 2.6.X (Metasploitable2)
Total Vulnerabilities Found	18
Critical	6
High	5
Medium	4
Low	3

Critical Vulnerabilities

Vulnerability	Port	CVE	CVSS	Recommendation
vsFTPd 2.3.4 Backdoor	21/tcp	CVE-2011-2523	CVSS 10.0	Upgrade or disable service.
UnrealIRCd Backdoor	6667/tcp	CVE-2010-2075	CVSS 10.0	Remove and install clean version.
Samba 3.0.20 RCE	445/tcp	CVE-2003-0201, CVE-2007-2447	CVSS 9.8	Update Samba.
Tomcat Manager Weak Auth	8180/tcp	CVE-2009-3548, CVE-2017-12615	CVSS 9.0	Upgrade and secure credentials.
PostgreSQL 8.3.x	5432/tcp	CVE-2009-3230	CVSS 9.0	Upgrade to supported version.
Default Bind Shell	1524/tcp	N/A	CVSS 10.0	Disable backdoor service.

High Severity Vulnerabilities

Vulnerability	Port	CVE	CVSS	Recommendation
Apache 2.2.8 Multiple Vulns	80/tcp	CVE-2011-3368, CVE-2017-9798, CVE-2021-41773	CVSS 8.5	Patch Apache.
ProFTPD 1.3.1	2121/tcp	CVE-2015-3306	CVSS 8.0	Update ProFTPD.
MySQL 5.0.51a	3306/tcp	CVE-2008-7247, CVE-2009-2446	CVSS 7.5	Upgrade MySQL.
OpenSSH 4.7p1	22/tcp	CVE-2008-5161	CVSS 7.4	Upgrade OpenSSH.
BIND 9.4.2	53/tcp	CVE-2009-0025	CVSS 7.8	Upgrade BIND.

Medium Severity Vulnerabilities

Vulnerability	Port	CVE	CVSS	Recommendation
SMTP VRFY User Enumeration	25/tcp	N/A	CVSS 6.5	Disable VRFY in Postfix.

SSLv2 Supported	25/tcp, 5432/tcp	N/A	CVSS 6.0	Disable SSLv2.
VNC Weak Authentication	5900/tcp	N/A	CVSS 5.8	Use stronger authentication.
NFS Shares Exposed	2049/tcp	N/A	CVSS 6.4	Restrict NFS access.

Low Severity Vulnerabilities

Vulnerability	Port	CVE	CVSS	Recommendation
X11 Server Exposed	6000/tcp	N/A	CVSS 4.0	Disable remote X11.
Outdated SSL Certificates	25/tcp, 5432/tcp	N/A	CVSS 3.5	Update SSL certs.
RPC Info Disclosure	111/tcp	N/A	CVSS 3.0	Limit RPC exposure.

Conclusion:

The target host is highly vulnerable, containing multiple critical backdoors, outdated services, and weak configurations. Exploitation of these vulnerabilities can lead to remote code execution, privilege escalation, and complete system compromise. This system should only be used for penetration testing training in a controlled lab environment.