Metasploitable2 VM - Nmap Scan Report

Target Information

- **IP Address**: 192.168.56.102
- **MAC Address**: 08:00:27:79:B8:59 (Oracle VirtualBox virtual NIC)
- **Hostname**: metasploitable.localdomain
- **Operating System**: Linux 2.6.9 - 2.6.33 (Ubuntu)
- **Network Distance**: 1 hop

Scan Summary

- **Scanner**: Nmap 7.95
- **Scan Date**: September 6, 2025, 03:00-03:33 EDT
- **Host Status**: Up (latency: 0.0012-0.0033s)
- **Total Open TCP Ports**: 23
- **Total Open UDP Ports**: 4

TCP Port Scan Results (-sV Service Detection)

Port	State	Service	Version	Notes
21	Open	FTP	vsftpd 2.3.4	Known vulnerable version
22	Open	SSH	OpenSSH 4.7p1 Debian 8ubuntu1	Older version
23	Open	Telnet	Linux telnetd	Unencrypted protocol
25	Open	SMTP	Postfix smtpd	Mail server
53	Open	DNS	ISC BIND 9.4.2	Domain name server
80	Open	HTTP	Apache httpd 2.2.8 (Ubuntu) DAV/2	Web server
111	Open	RPC	rpcbind 2 (RPC ● #100000)	Remote procedure call
139	Open	NetBIOS	Samba smbd 3.X - 4.X (WORKGROUP)	File sharing
445	Open	SMB	Samba smbd 3.X - 4.X (WORKGROUP)	File sharing
512	Open	rexec	netkit-rsh rexecd	Remote execution
513	Open	rlogin	login?	Remote login
514	Open	rsh	shell?	Remote shell
1099	Open	Java RMI	GNU Classpath grmiregistry	Java remote method invocation
1524	Open	Backdoor	Metasploitable root shell	**CRITICAL: Backdoor**
2049	Open	NFS	NFS 2-4 (RPC ● #100003)	Network file system
2121	Open	FTP	ProFTPD 1.3.1	Alternative FTP server
3306	Open	MySQL	MySQL 5.0.51a-3ubuntu5	Database server
5432	Open	PostgreSQL	PostgreSQL DB 8.3.0 - 8.3.7	Database server
5900	Open	VNC	VNC (protocol 3.3)	Remote desktop
6000	Open	X11	X11 (access denied)	X Window System
6667	Open	IRC	UnrealIRCd	Internet Relay Chat
8009	Open	AJP	Apache Jserv (Protocol v1.3)	Apache JServ Protocol
8180	Open	HTTP	Apache Tomcat/Coyote JSP engine 1.1	Java web server

UDP Port Scan Results (-sU)

Port	State	Service	Notes
53	Open	DNS	Domain name server
68	Open/Filtered	DHCP Client	Dynamic host configuration
69	Open/Filtered	TFTP	Trivial file transfer
111	Open	RPC	Remote procedure call
137	Open	NetBIOS-NS	NetBIOS name service
138	Open/Filtered	NetBIOS-DGM	NetBIOS datagram service
2049	Open	NFS	Network file system

Operating System Detection (-O)

Detected OS: Linux 2.6.X

OS Details: Linux 2.6.9 - 2.6.33

Device Type: General purpose

CPE: cpe:/o:linux:linux_kernel:2.6

Critical Security Findings

🔴 CRITICAL Vulnerabilities

1. **Backdoor Shell (Port 1524)**
   - Direct root shell access
   - No authentication required
   - **Risk Level**: CRITICAL
2. **vsftpd 2.3.4 (Port 21)**
   - Known backdoor vulnerability (CVE-2011-2523)
   - **Risk Level**: CRITICAL

🟠 HIGH Risk Services

3. **Unencrypted Protocols**
   - Telnet (Port 23) - plaintext authentication
   - FTP (Ports 21, 2121) - plaintext credentials
   - VNC (Port 5900) - often weak/no authentication
4. **Legacy Services**
   - rexec, rlogin, rsh (Ports 512-514) - deprecated remote access
   - UnrealIRCd (Port 6667) - known vulnerabilities
5. **Database Exposure**
   - MySQL (Port 3306) - externally accessible
   - PostgreSQL (Port 5432) - externally accessible

🟡 MEDIUM Risk Services

6. **File Sharing**
   - Samba/SMB (Ports 139, 445) - potential for anonymous access
   - NFS (Port 2049) - network file sharing
7. **Web Services**
   - Apache 2.2.8 (Port 80) - older version
   - Tomcat (Port 8180) - Java application server

Recommendations

Immediate Actions Required

1. **Disable backdoor shell** on port 1524 immediately
2. **Update vsftpd** to latest version or disable FTP
3. **Disable unnecessary services**:
    - Telnet (use SSH instead)
    - rexec, rlogin, rsh (legacy remote access)
    - IRC server (if not needed)

Security Hardening

1. **Network Segmentation**: Isolate this system from production networks
2. **Firewall Rules**: Block unnecessary external access
3. **Service Hardening**:
    - Configure strong authentication for VNC
    - Secure database access (bind to localhost only)
    - Update all software to latest versions
4. **Monitoring**: Implement logging and monitoring for all services

Penetration Testing Notes

This system appears to be **Metasploitable2**, a deliberately vulnerable Linux system designed for security training and penetration testing. It contains multiple known vulnerabilities and should:

- **Never be connected to production networks**
- **Only be used in isolated lab environments**
- **Be used for authorized security training only**

Scan Command Reference

```bash
# Service version detection
nmap -sV 192.168.56.102

# TCP SYN scan
nmap -sS 192.168.56.102

# UDP scan (verbose)
nmap -sU -v 192.168.56.102

# OS detection
nmap -O 192.168.56.102
```

Report Generated: September 6, 2025

Scanner: Nmap 7.95

Scan Duration: ~30 minutes total

Classification: TRAINING ENVIRONMENT - DELIBERATELY VULNERABLE