

Vulnerablility Asessment Scan Report on a Unix Server Using Nmap

IP Address: 192.168.0.170

Prepared by: Oluwafemi A. Ojo

Date: 3rd March, 2025

Table of Contents

Introduction	3
Objective	4
Nmap Scan Report	5
Findings from Nmap Scan on 192.168.0.170	5
Analysis & Recommendation	10
Conclusion	10

Introduction

This report presents the findings of a penetration testing scan performed on a Unix machine with the IP address 192.168.0.170. The assessment was conducted using three security reconnaissance tools: Nmap, SpiderFoot, and Recon-ng. Each tool was used to gather different security-related information about the target system.

The goal of this scan is to identify open ports, services, vulnerabilities, and possible security risks that could be exploited by attackers. This document provides detailed results from each tool, along with relevant screenshots and findings.

Objective

Nmap (Network Mapper) was used to scan the Unix machine to detect open ports, running services, and vulnerabilities.

Nmap Scan Report

Scan Command Used

nmap -A -p- 192.168.0.170

This is a powerful Nmap scan that provides detailed information about a target machine (192.168.0.170). Here's what each flag does:

Breaking it Down:

- **nmap** → Calls the Nmap tool, which is used for network scanning and security auditing.
- **-A (Aggressive Scan)** → Enables multiple advanced features, including:
 - OS detection
 - Version detection
 - Script scanning
 - Traceroute
- **-p- (Scan All Ports)** → Scan all **65,535 TCP** ports instead of just the default 1,000.

- **192.168.0.170** → The target IP address being scanned.

How It Helps in a Vulnerability Scan:

- **Identifies Open Ports** → Shows which services are running and where vulnerabilities might exist.
- **Detects Running Services & Versions** → Helps find outdated or misconfigured services.
- **Finds OS & System Info** → Useful for fingerprinting a system to tailor attacks or defenses.
- **Performs Traceroute** → Helps map out the network for possible attack paths.

Findings from Nmap Scan on 192.168.0.170

General Information:

- **Target IP:** 192.168.0.170
- **Host is up:** 0.0012s latency
- **Operating System:** Linux 2.6.9 - 2.6.33
- **Network Distance:** 1 hop
- **MAC Address:** 08:00:27:3A:27:F4 (Oracle VirtualBox virtual NIC)
- **Hostname:** metasploitable.localdomain

```
(kali㉿kali)-[~]  
$ nmap -A -p- 192.168.0.170  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-03 13:08 EST  
Nmap scan report for 192.168.0.170  
Host is up (0.0012s latency).  
Not shown: 65505 closed tcp ports (conn-refused)
```

Open Ports and Services:

- **FTP (Port 21)**
 - **Service:** vsftpd 2.3.4
 - **Anonymous Login:** Enabled
 - **Vulnerability:** This version is known to have a backdoor vulnerability (CVE-2011-2523).

```

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|       Connected to 192.168.0.179
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       vsFTPd 2.3.4 - secure, fast, stable
|_End of status

```

- **SSH (Port 22)**
 - **Service:** OpenSSH 4.7p1 Debian 8ubuntu1
 - **Vulnerability:** Outdated version, possibly vulnerable to multiple known exploits.

```

22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2025-03-03T18:11:34+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|       SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|       SSL2_DES_192_EDE3_CBC_WITH_MD5
|       SSL2_RC2_128_CBC_WITH_MD5
|       SSL2_RC4_128_WITH_MD5
|       SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5

```

- **Telnet (Port 23)**
 - **Service:** Linux telnetd
 - **Vulnerability:** Unencrypted transmission, prone to credential sniffing.

- **SMTP (Port 25)**
 - **Service:** Postfix smtpd
 - **STARTTLS Enabled:** Yes
 - **Vulnerability:** Could allow enumeration of valid users through VRFY.
- **DNS (Port 53)**
 - **Service:** ISC BIND 9.4.2
 - **Vulnerability:** Older version, may be susceptible to cache poisoning attacks.

```

53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2             111/tcp    rpcbind
|   100000   2             111/udp    rpcbind
|   100003   2,3,4         2049/tcp   nfs
|   100003   2,3,4         2049/udp   nfs
|   100005   1,2,3         51238/tcp  mountd
|   100005   1,2,3         55340/udp  mountd
|   100021   1,3,4         49084/udp  nlockmgr
|   100021   1,3,4         59046/tcp  nlockmgr
|   100024   1             56247/udp  status
|   100024   1             59659/tcp  status

```

- **HTTP (Port 80)**
 - **Service:** Apache 2.2.8 (Ubuntu)
 - **Vulnerability:** Version may be affected by several known exploits, including directory traversal and remote code execution.
- **Samba (Ports 139 & 445)**
 - **Service:** Samba smbd 3.0.20-Debian
 - **Workgroup:** WORKGROUP
 - **Vulnerability:** Susceptible to SMB exploits such as EternalBlue.

```

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec?
513/tcp open login      OpenBSD or Solaris rlogind
514/tcp open shell?
| fingerprint-strings:
|   NULL:
|_   Couldn't get address for your host (kali)
1099/tcp open java-rmi    GNU Classpath grmiregistry
1524/tcp open bindshell  Metasploitable root shell
2049/tcp open nfs       2-4 (RPC #100003)
2121/tcp open ftp       ProFTPD 1.3.1
3306/tcp open mysql     MySQL 5.0.51a-3ubuntu5

```

- **MySQL (Port 3306)**

- **Service:** MySQL 5.0.51a-3ubuntu5
- **Vulnerability:** May be vulnerable to authentication bypass exploits.

```

3306/tcp open mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, SupportsCompression, SupportsTransactions, Speaks41P
|   rotocolNew, ConnectWithDatabase, Support41Auth, LongColumnFlag
|   Status: Autocommit
|_  Salt: ^3#RV7QpatD8)eAVm@89
3632/tcp open distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-date: 2025-03-03T18:11:34+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=
| There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
5900/tcp open vnc        VNC (protocol 3.3)
| vnc-info:

```

- **PostgreSQL (Port 5432)**

- **Service:** PostgreSQL 8.3.0 - 8.3.7
- **Vulnerability:** Older version, may be susceptible to SQL injection attacks.

- **VNC (Port 5900)**

- **Service:** VNC (protocol 3.3)
- **Vulnerability:** If no password is set, attackers could gain unauthorized remote access.

- **Apache Tomcat (Port 8180)**

- **Service:** Apache Tomcat/Coyote JSP engine 1.1
- **Vulnerability:** Tomcat default credentials might be used for unauthorized access.

- **DistCC (Port 3632)**
 - **Service:** distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
 - **Vulnerability:** Open access can allow remote code execution (CVE-2004-2687).

Analysis & Recommendations:

- Disable anonymous FTP access or upgrade vsftpd to a secure version.
- Upgrade OpenSSH to the latest version to patch known vulnerabilities.
- Disable Telnet and use SSH for secure remote access.
- Upgrade SMTP service and restrict VRFY to prevent user enumeration.
- Upgrade BIND DNS to the latest secure version to mitigate cache poisoning risks.
- Update Apache HTTP Server to avoid known exploits.
- Harden Samba configuration and ensure the latest security patches are applied.
- Upgrade MySQL and PostgreSQL to mitigate SQL injection risks.
- Secure VNC with strong authentication or disable it if not needed.
- Update Apache Tomcat and remove default credentials.
- Disable or restrict distccd to prevent remote code execution vulnerabilities.

Conclusion:

This scan indicates that the target system is highly vulnerable, running several outdated services with known exploits. Immediate security patches and mitigations are recommended to secure the system from potential attacks.