Vulnerability Analysis Report

1. Introduction

This report documents the results of a vulnerability scan conducted on the target system using Nmap for port scanning and service enumeration. The goal was to identify active services and potential security weaknesses.

2. Port Scanning and Service Enumeration

The Nmap scan identified the following open ports and services:

Port	State	Service	Version
22/tcp	Open	SSH	OpenSSH 6.6.1p1 Ubuntu 2.13
80/tcp	Open	HTTP	Apache httpd 2.4.7 (Ubuntu)
9929/tcp	Open	Nping echo	Nping echo
31337/tcp	Open	Unknown service	-

Additionally, a vulnerability scan was performed, identifying potential security risks.

---

3. Identified Vulnerabilities and Risk Analysis

Vulnerability 1: Outdated OpenSSH Version (Port 22)

- **Description: The scan detected OpenSSH 6.6.1p1, which is an outdated version known to contain multiple vulnerabilities.**
- **Risk Level: High**
- **Potential Impact:**
    - **May be vulnerable to CVE-2016-0777, allowing attackers to extract private SSH keys.**
    - **May be vulnerable to CVE-2015-5600, allowing brute-force attacks on authentication.**
- **Mitigation Strategy:**
    - **Upgrade OpenSSH to the latest stable version.**
    - **Disable weak authentication methods (e.g., password-based logins).**
    - **Implement key-based authentication and fail2ban to prevent brute-force attacks.**

Vulnerability 2: Apache HTTP Server with CSRF Vulnerabilities (Port 80)

- **Description: The scan revealed an Apache 2.4.7 HTTP server, which is outdated and has potential Cross-Site Request Forgery (CSRF) vulnerabilities.**
- **Risk Level: Medium**
- **Potential Impact:**
    - **Attackers can trick users into executing unintended actions on authenticated websites.**
    - **Could lead to unauthorized modifications or privilege escalation.**
- **Mitigation Strategy:**
    - **Upgrade Apache to the latest stable version (2.4.x).**
    - **Implement CSRF protection tokens on all forms.**
    - **Use CSP (Content Security Policy) headers to prevent unauthorized script execution.**

Vulnerability 3: UDP DoS Vulnerability (CVE-2021-1002)

- **Description: The scan detected a vulnerability where an attacker can send a NULL UDP packet, potentially leading to a Denial of Service (DoS) attack.**
- **Risk Level: Medium-High**
- **Potential Impact:**
    - **Attackers can flood the service with malformed packets, leading to performance degradation or complete service unavailability.**
- **Mitigation Strategy:**

- **Apply firewall rules to filter out UDP traffic from untrusted sources.**
- **Enable rate limiting for incoming UDP packets.**
- **Update the affected service to a patched version.**

---

4. Conclusion & Recommendations

This scan identified three key vulnerabilities:

1. **Outdated OpenSSH (High risk) – Needs an immediate upgrade and security hardening.**
2. **CSRF vulnerabilities in Apache (Medium risk) – Requires security updates and web application hardening.**
3. **UDP DoS vulnerability (Medium-High risk) – Can be mitigated with firewall rules and rate limiting.**

By implementing the recommended mitigations, the security posture of the system can be significantly improved.

```
sa57@SAs-MacBook-Air-2 abi-dae % sudo nmap scanme.nmap.org
Password:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 15:49 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
sa57@SAs-MacBook-Air-2 abi-dae % sudo nmap -sS -sV -p- scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 15:50 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.076s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE    SERVICE       VERSION
22/tcp    open     ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
68/tcp    filtered dhcpc
80/tcp    open     http          Apache httpd 2.4.7 ((Ubuntu))
546/tcp   filtered dhcpv6-client
9929/tcp  open     nping-echo    Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 114.98 seconds
sa57@SAs-MacBook-Air-2 abi-dae % sudo nmap --script vuln scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 15:53 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=scanme.nmap.org
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-head-search
|     Form action: /search/
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-foot-search
|_    Form action: /search/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 542.02 seconds
```