



Vulnerability Scanning Lab

1. Executive Summary

A vulnerability assessment was conducted on the target system (10.33.226.229) using Nmap, OpenVAS, and Nikto to identify exposed services and potential security weaknesses. The objective was to evaluate the system's security posture, prioritize risks using CVSS scoring, and recommend appropriate remediation measures.

The scan identified multiple critical vulnerabilities, including a backdoored VSFTPD service (CVE-2011-2523), vulnerable Samba services, and exposed remote access services such as Telnet and SMB (Port 445). The Apache HTTP server was also found to be outdated and potentially vulnerable to path traversal attacks (CVE-2021-41773). Additionally, a bind shell service was detected, which poses a severe risk of unauthorized remote access.

If exploited, these vulnerabilities could allow attackers to gain remote system access, execute arbitrary commands, or fully compromise the host. Immediate remediation is strongly recommended for all critical and high-severity findings.

2. Tools

Tool	Purpose
Nmap	Port scanning and service enumeration
OpenVAS	Automated vulnerability detection
Nikto	Web server vulnerability scanning

3. Methodology

The assessment followed these steps:

1. Network Discovery using Nmap
2. Vulnerability Detection using OpenVAS



3. Web Server Analysis using Nikto
4. Risk Prioritization using CVSS
5. Documentation and Reporting

4. Scan Execution

4.1 Nmap Service Scan

Command Used:

```
nmap -sV 10.33.226.229
```

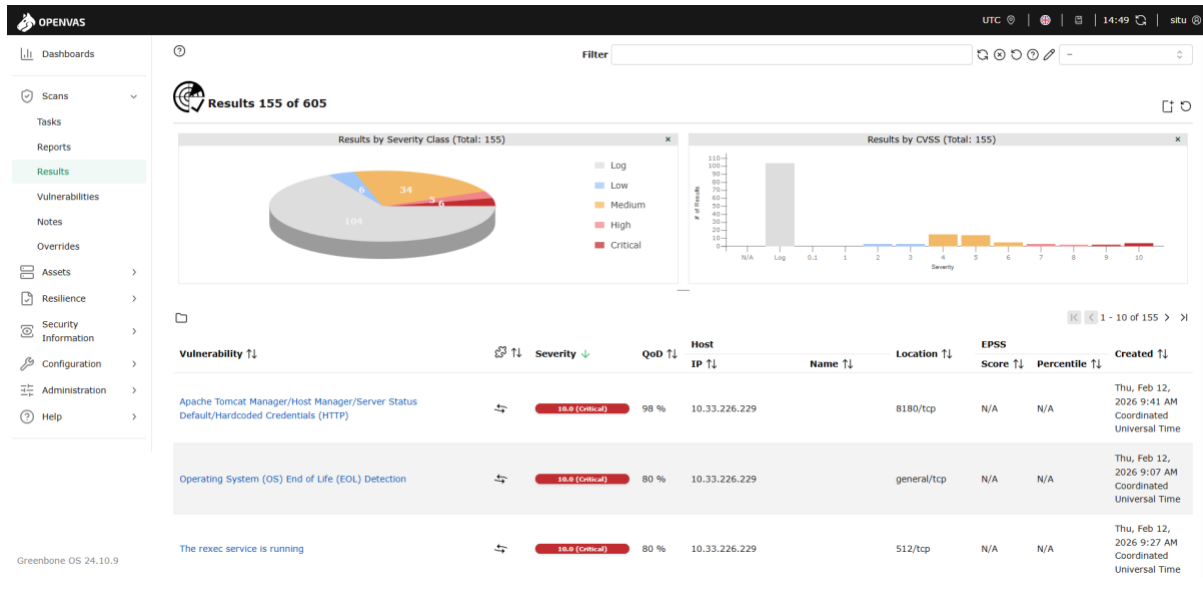
The scan revealed multiple open ports including 21 (FTP), 22 (SSH), 80 (HTTP), and 445 (SMB).

```
(gyanesh@kali)-[~/cyart]
$ nmap -sV 10.33.226.229
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 13:19 +0530
Nmap scan report for 10.33.226.229
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:73:BA:83 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 16.88 seconds
```

4.2 OpenVAS Vulnerability Scan

An unauthenticated “Full and Fast” scan was performed on the target host. The scan detected multiple vulnerabilities with CVSS scores ranging from Medium to Critical.



4.3 Nikto Web Scan

Command Used:

```
nikto -h http://10.33.226.229
```

Nikto identified potential web misconfigurations and outdated Apache server components.



```
(green08@kali:~/cyart)
$ nikto -h https://10.33.226.229
- Nikto v2.5.0

-----
+ Target IP: 10.33.226.229
+ Target Hostname: 10.33.226.229
+ Target Port: 80
+ Start time: 2026-02-12 13:48:08 (GMT+5)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Detected x-powered-by header: PHP/5.2.4-6ubuntu0.19.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis-
  x-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'ton' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698&id=59d15,ht
  tp://seahorse.afnsw.gov.au/learnload.com/vulnerabilities/423/
+ /: Web server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0478
+ /?PHPBB35F2B-3C92-11d3-A3A3-6C7D08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPBB35F2B-0428-11d3-A768-00A001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPBB35F2B-0428-11d3-A768-00A001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHPBB35F2B-0428-11d3-A768-00A001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpmyadmin/changepw.php: phpmyadmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/changelang.php: phpmyadmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/changelang.php: phpmyadmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/changelang.php: phpmyadmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CVE-952
+ /icons/: Directory indexing found.
+ /icons/: Apache details file found. See: https://www.vuxweb.co.uk/apache-restricting-access-to-icons/
+ /phpmyadmin/: phpmyadmin directory found.
+ /phpmyadmin/documentation.html: phpmyadmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/README: phpmyadmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /php-config.php: php-config.php file found. This file contains the credentials.
+ 8/11 requests: 8 error(s) and 27 item(s) reported on remote host
+ End time: 2026-02-12 13:49:03 (GMT+5) (55 seconds)
-----
+ 1 host(s) tested
```

5. Detailed Findings

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	VSFTPD 2.3.4 Backdoor (CVE-2011-2523)	10.0	Critical	10.33.226.229
002	Samba 3.x Remote Code Execution	9.8	Critical	10.33.226.229
003	Apache 2.2.8 Outdated Version	8.1	High	10.33.226.229
004	MySQL 5.0.51a Weak Configuration	7.5	High	10.33.226.229
005	Tomcat Manager Exposure (Port 8180)	8.8	High	10.33.226.229
006	Telnet Service Enabled (Port 23)	6.5	Medium	10.33.226.229
007	rlogin Service Enabled (Port 513)	6.0	Medium	10.33.226.229
008	UnrealIRCd Backdoor Vulnerability	10.0	Critical	10.33.226.229
009	Bind Shell Backdoor (Port 1524)	10.0	Critical	10.33.226.229
010	NFS Service Exposure (Port 2049)	7.5	High	10.33.226.229



Title: Apache Path Traversal

Findings: [CVE-2021-41773], [Host: 10.33.226.229]

Remediation: Restrict directory permissions

Title: VSFTPD Backdoor

Findings: [CVE-2011-2523]

Remediation: Remove vulnerable FTP version

Title: Samba Remote Code Execution

Severity: Critical (CVSS 9.8)

Remediation: Upgrade Samba, Restrict SMB ports (139, 445)

6. Escalation Email to developers

Critical Web Vulnerability Identified on 10.33.226.229

Draft saved at 03:12 PM

Dear Development Team,

During a recent vulnerability assessment of host 10.33.226.229, a critical issue was identified in the Apache HTTP Server (CVE-2021-41773). The server is running a vulnerable version that is susceptible to path traversal attacks. Proof-of-Concept testing confirmed that restricted files could potentially be accessed through crafted HTTP requests. Additionally, multiple unnecessary services are exposed, increasing the attack surface. We strongly recommend upgrading Apache to the latest secure version and disabling unused ports and services immediately to mitigate exploitation risks.

Regards,
VAPT Analyst

Gyanesh Chand