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 The Apache HTTP server was also found to be outdated and potentially vulnerable to path traversal attacks (CVE-2021-41773).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

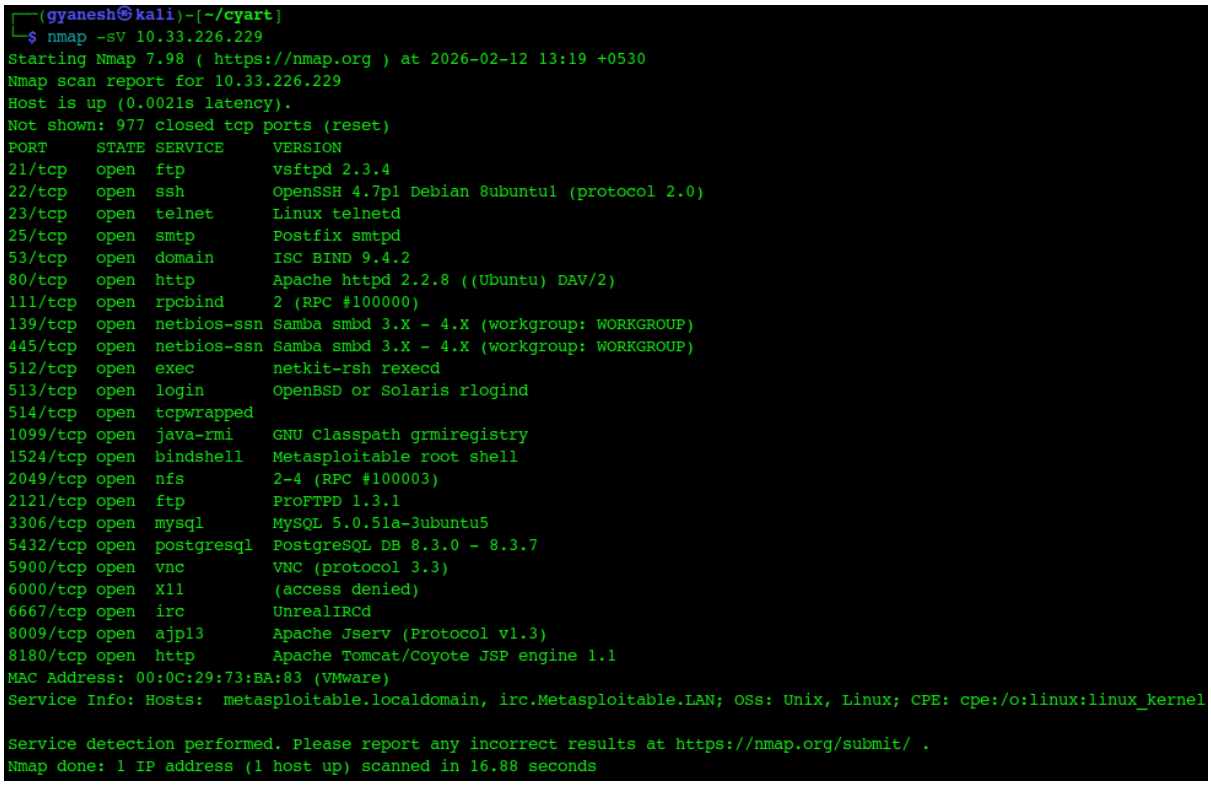
4. Scan Execution

4.1 Nmap Service Scan

Command Used:

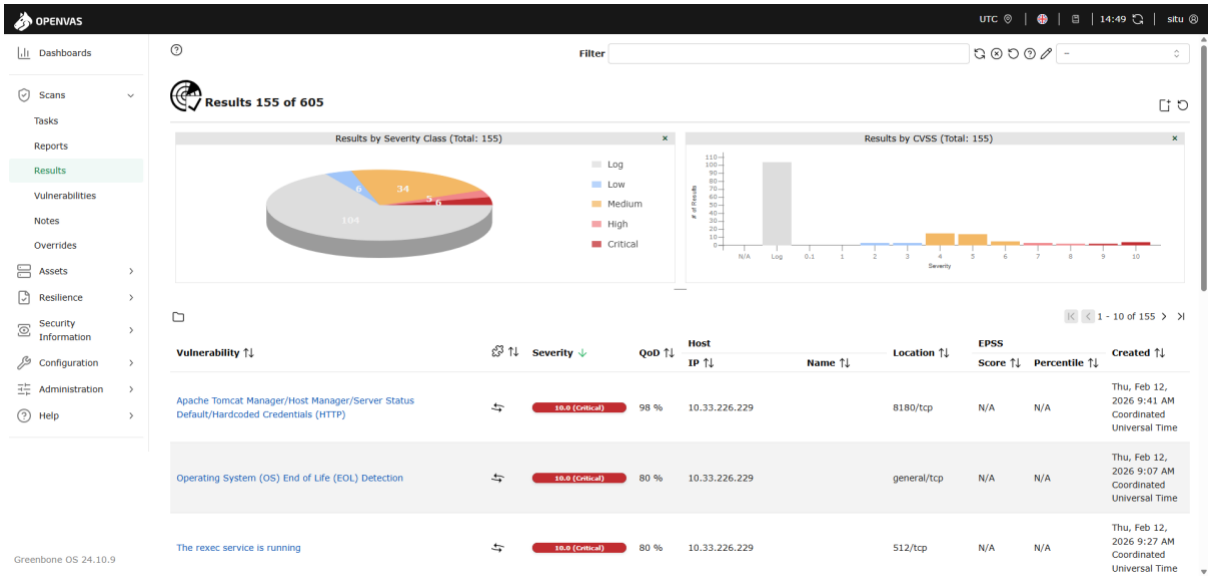
nmap -sV 10.33.226.229

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



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.

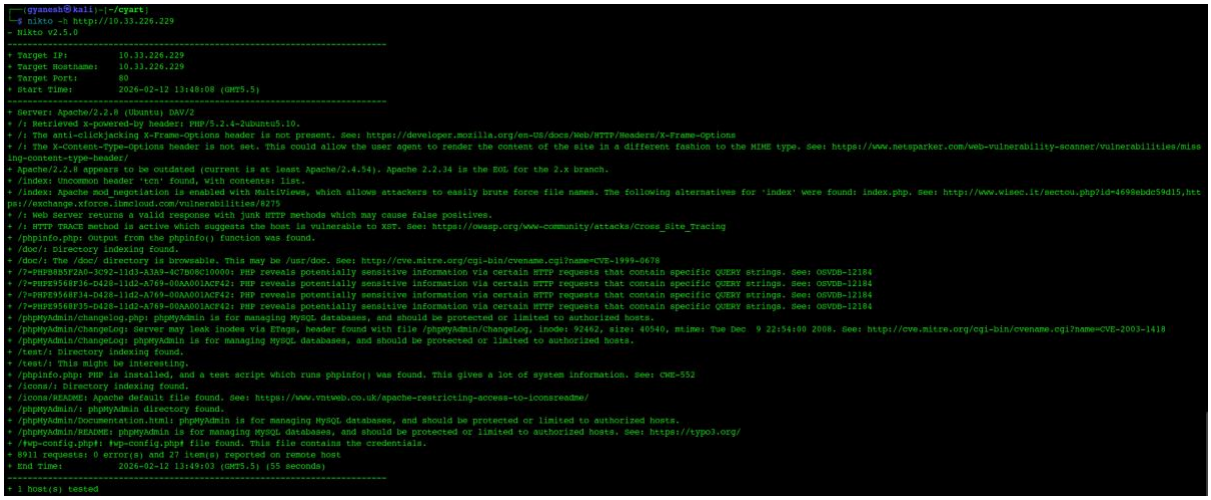


4.3 Nikto Web Scan

Command Used:

nikto -h http://10.33.226.229

Nikto identified potential web misconfigurations and outdated Apache server components.



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