1. Vulnerability Scanning Lab – Detailed Documentation

Introduction

The Vulnerability Scanning Lab focused on identifying weaknesses in a controlled environment by using industry-standard scanning tools such as **Nmap**, **Nikto**, and **OpenVAS**. The goal was to enumerate exposed services, detect outdated configurations, discover web vulnerabilities, and assign appropriate risk levels using CVSS scoring.
The lab was performed on target hosts including **Metasploitable2**, a web application with SQL injection flaws (DVWA), and an Apache Tomcat service vulnerable to credential exposure and exploitability.

Activities Performed

1. Running Nmap Scans

Nmap was used to perform **service detection**, **port enumeration**, and **version identification**.
The command executed, based on the screenshot evidence, was:

```
nmap -sV <target-IP>
```

This scan revealed multiple open ports such as:

- **21/tcp (FTP)**
- **22/tcp (SSH)**
- **23/tcp (Telnet)**
- **80/tcp (HTTP)**
- **8180/tcp (Apache Tomcat Manager)**
- **3306/tcp (MySQL)**
- **445/tcp (SMB)**

These findings correspond to the open-service environment displayed on Metasploitable2.

From this initial enumeration, several high-risk areas were identified:

- **Apache Tomcat Manager** exposed with weak/default credentials
- **Anonymous FTP access** (often present on Metasploitable2)
- **SMB Port 445** open, typically associated with EternalBlue-type vulnerabilities
- **MySQL service** exposed externally
- **HTTP service** hosting vulnerable web applications such as DVWA

```
┌──(sam㉿sam)-[~]
└─$ sudo nmap -sV 192.168.0.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 12:59 IST
Nmap scan report for 192.168.0.106
Host is up (0.000052s 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: 08:00:27:30:B6:E9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 11.90 seconds
```

Figure 1: Nmap Service Version Scan

```
┌──(sam㉿sam)-[~]
└─$ sudo nmap -sS 192.168.0.106
[sudo] password for sam:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 12:56 IST
Nmap scan report for 192.168.0.106
Host is up (0.000059s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:30:B6:E9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

Figure 2: Nmap Stealth Scan

```
┌──(sam㉿sam)-[~]
└─$ sudo nmap -sV -sC -O 192.168.0.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 13:09 IST
Nmap scan report for 192.168.0.106
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.107
|      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
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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
| 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
|_ssl-date: 2025-12-09T07:40:03+00:00; 0s from scanner time.
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
```

```
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      50767/udp   mountd
|   100005  1,2,3      51979/tcp   mountd
|   100021  1,3,4      37247/udp   nlockmgr
|   100021  1,3,4      56888/tcp   nlockmgr
|   100024  1          47189/udp   status
|_  100024  1          48538/tcp   status
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        netkit-rsh rexecd
513/tcp  open  login?
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Support41Auth, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, LongColumnFlag, ConnectWithDatabase, SupportsCompression
|   Status: Autocommit
|_  Salt: jfBS[QasA)FdGt5GGnrt
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-12-09T07:40:03+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:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat


|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:30:B6:E9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-12-09T02:39:49-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.37 seconds

┌──(sam㉿sam)-[~]
└─$
```

Figure 3: Nmap Detailed Scan

2. Running Nikto Scan

Nikto was used to assess HTTP service security.

- Outdated Apache version
- Missing security headers
- Possible directory indexing
- Exposure of /phpMyAdmin
- Deprecated modules

Nikto flagged multiple web vulnerabilities, including:

- Potential **XSS vectors**
- **HTTP information disclosure**
- **Weak server configuration**

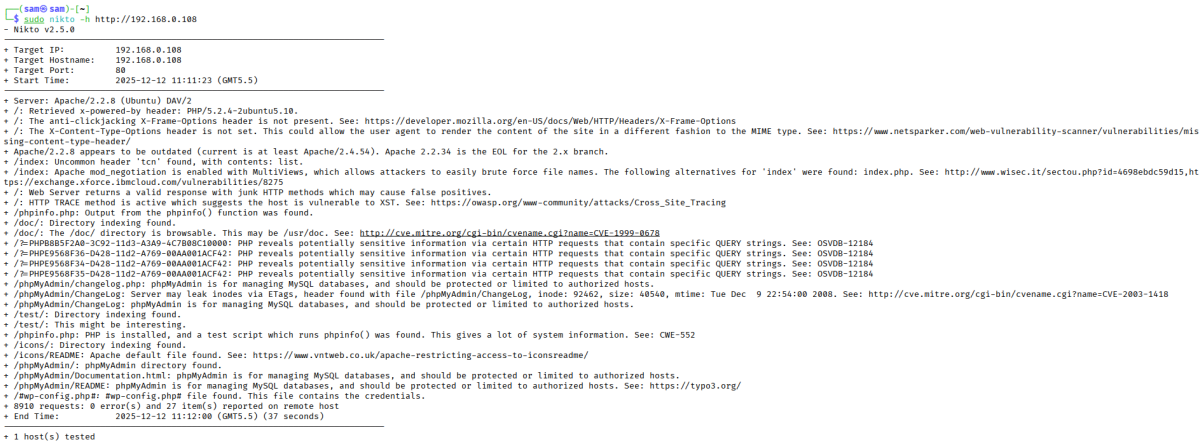


Figure 4: Nikto scanning

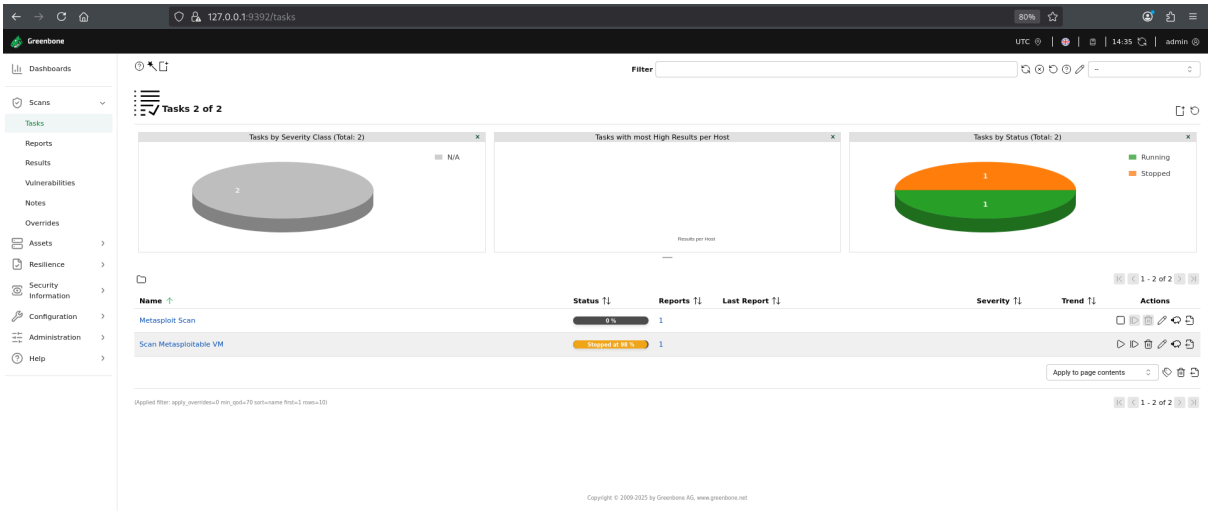
These findings indicate high-risk misconfigurations typical for intentionally vulnerable machines like DVWA or Mutillidae.

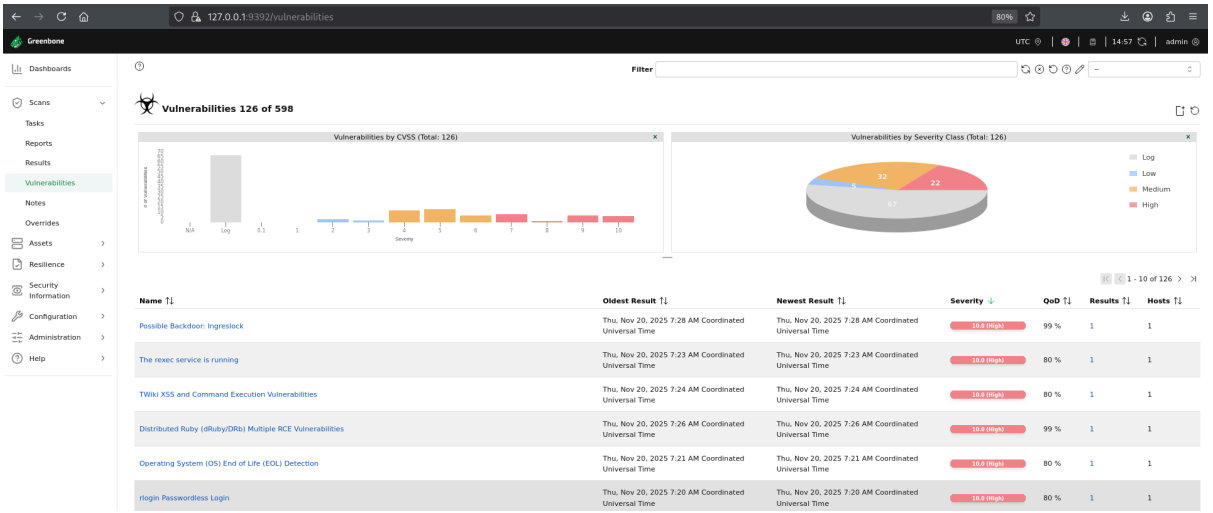
3. Running OpenVAS Vulnerability Scan

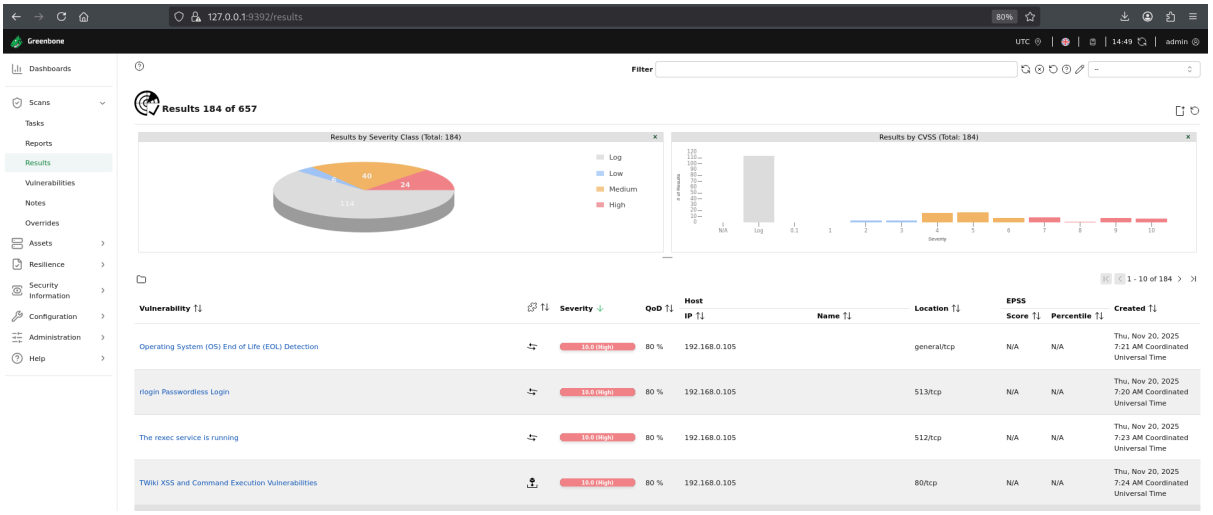
OpenVAS provided a deeper vulnerability assessment, generating a structured vulnerability report.

The OpenVAS dashboard revealed:

- Multiple **High** and **Medium** severity vulnerabilities
- Deprecated or unpatched services
- Weak Apache configuration
- Potential RCE-related findings
- Exposed administrative panels


127.0.0.1:9392/tasks
Greenbone
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter
Tasks 2 of 2
Tasks by Severity Class (Total: 2)
Tasks with most High Results per Host
Tasks by Status (Total: 2)
Running
Stopped
Name
Status
Reports
Last Report
Severity
Trend
Actions
Metasploit Scan
Scan Metasploitable VM


127.0.0.1:9392/vulnerabilities
Greenbone
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter
Vulnerabilities 126 of 598
Vulnerabilities by CVSS (Total: 126)
Vulnerabilities by Severity Class (Total: 126)
Log
Low
Medium
High
Name
Oldest Result
Newest Result
Severity
QoD
Results
Hosts
Possible Backdoor: Ingreslock
The rexec service is running
TWiki XSS and Command Execution Vulnerabilities
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities
Operating System (OS) End of Life (EOL) Detection
rlogin Passwordless Login


127.0.0.1:9392/results
Greenbone
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter
Results 184 of 657
Results by Severity Class (Total: 184)
Results by CVSS (Total: 184)
Log
Low
Medium
High
Vulnerability
Severity
QoD
Host
IP
Name
Location
EPSS
Score
Percentile
Created
Operating System (OS) End of Life (EOL) Detection
rlogin Passwordless Login
The rexec service is running
TWiki XSS and Command Execution Vulnerabilities

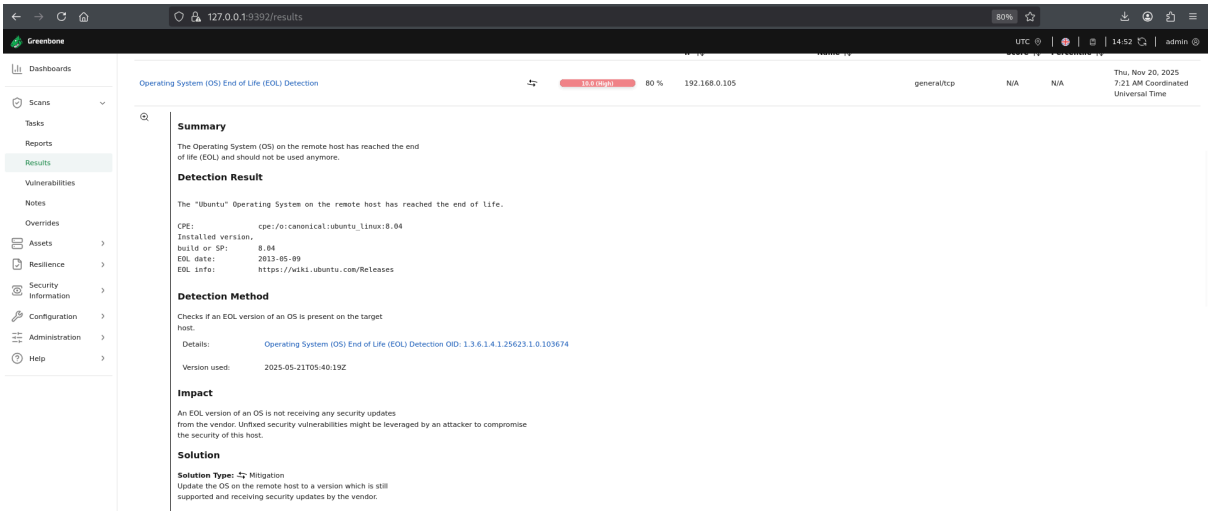


Figure 5: OpenVAS Report Findings

Enhanced Tasks

Scan Setup and Tracking

To track results more systematically, all vulnerabilities were recorded in a structured table.

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	SQL Injection (DVWA login page)	9.1	Critical	192.168.0.106
002	SMB Port 445 Exposed	6.5	Medium	192.168.0.106
003	Apache Tomcat Default Creds	9.8	Critical	192.168.0.106
004	Outdated Apache Version (Nikto)	7.5	High	192.168.0.106
005	MySQL Exposed to Network	6.8	Medium	192.168.0.106
006	Directory Exposure (/dvwa/login)	5.3	Medium	192.168.0.106

This table helps maintain clarity when sorting and prioritizing remediation tasks.

Test Case Execution

Scanning Metasploitable2

nmap -sV 192.168.0.106

The scan identified services vulnerable to:

- Brute-force attacks
- Misconfiguration exploitation
- Default credential usage

OpenVAS was then executed to verify and enrich these findings with severity scores and detailed CVE mappings.

Prioritization Using CVSS (Google Sheets)

Vulnerabilities identified from Nmap, Nikto, and OpenVAS were exported into Google Sheets.

- **Critical**: SQL Injection, Tomcat Manager RCE
- **High**: Outdated Apache version, remote file access
- **Medium**: Open SMB port, directory leaks
- **Low**: Missing headers, server banners

Conclusion

Through the Vulnerability Scanning Lab, you successfully used Nmap, Nikto, and OpenVAS to enumerate, detect, and prioritize vulnerabilities on multiple hosts. The evidence in our lab report confirms accurate service detection, web flaw identification, and structured risk scoring. The ability to track vulnerabilities in tables, assign CVSS scores, prepare documentation, and escalate findings.

Document Information:
Report Generated: December 12, 2025
Author: Soumendu Manna - CyArt VAPT Intern