**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.

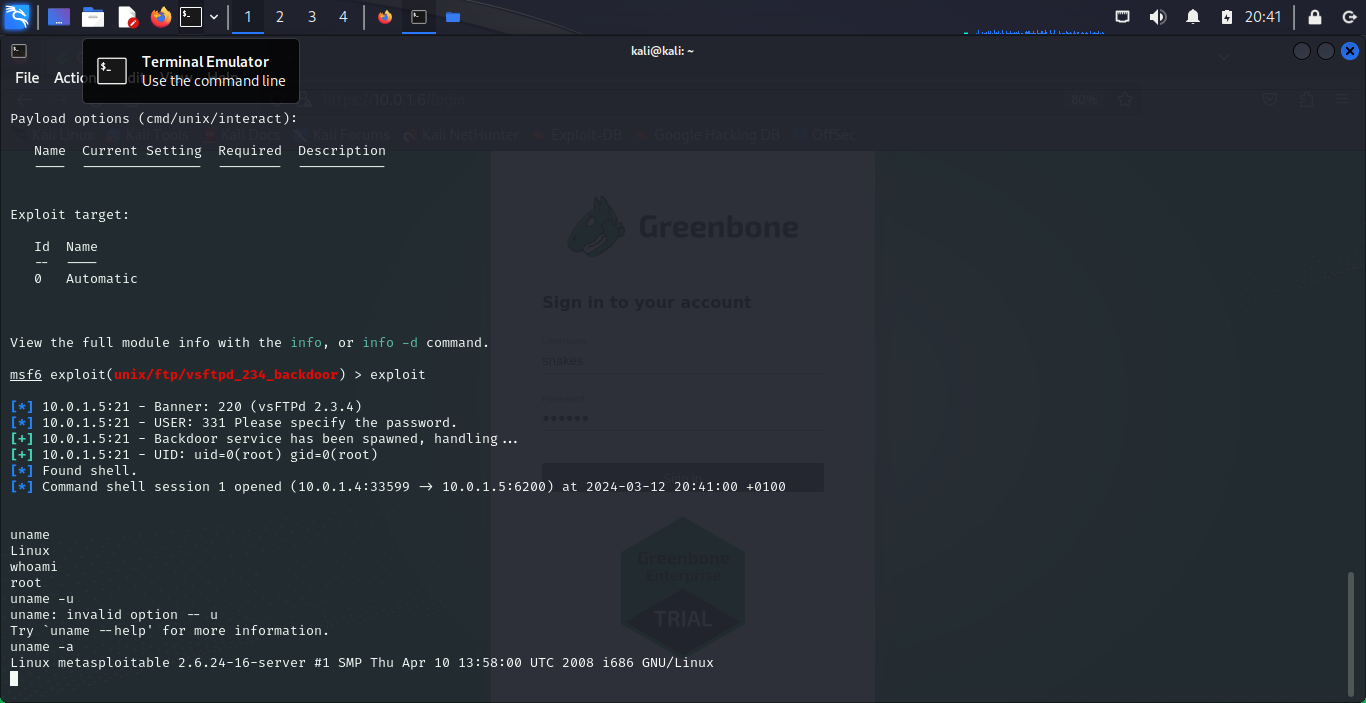


Figure 1 VSFTPD Exploit proof

## 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.

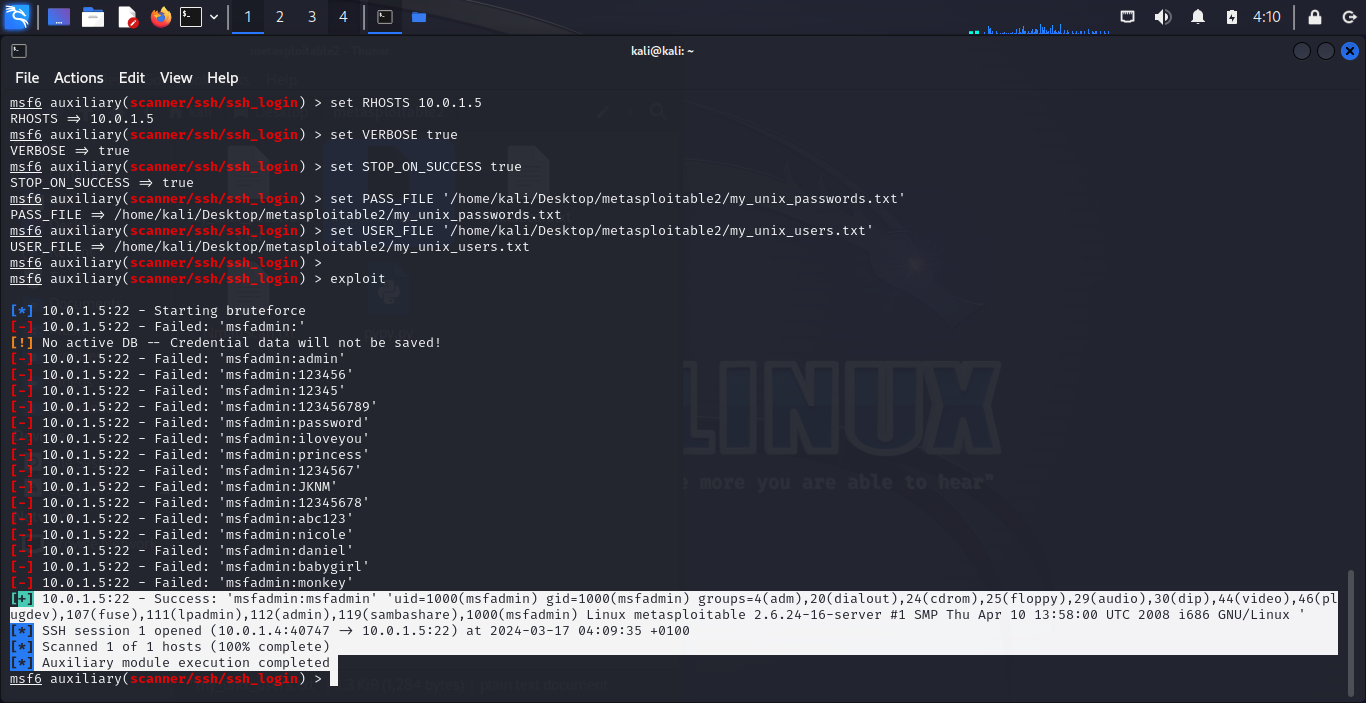


Figure 2 Brute force proof

3. Port 23 Telnet:

**Exploit Used**: Brute force attack to obtain credentials

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

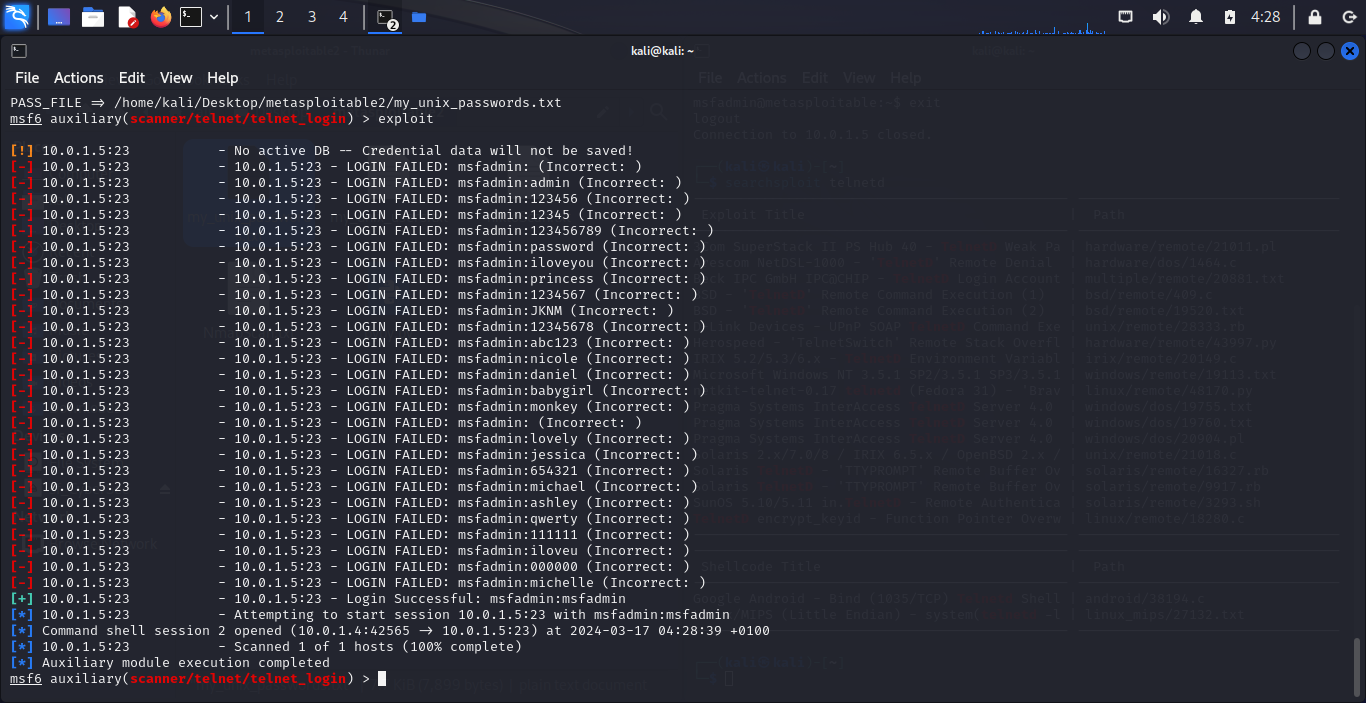


Figure 3 brute force proof

4. Port 80 HTTP:

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

**Exploit**: Utilized SQL injection.

**Result**: Successfully exploited the SQL injection vulnerability.

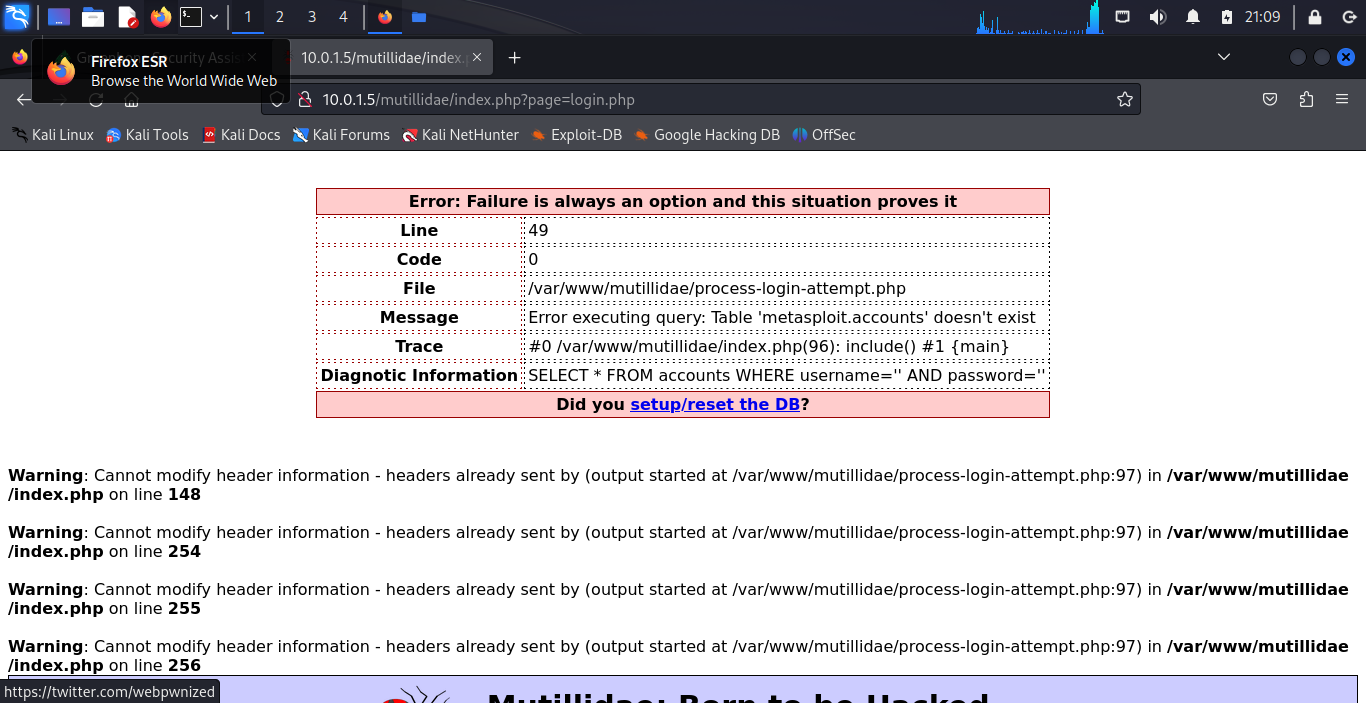


Figure 4 SQL injection error

5. Port 80 HTTP:

**Vulnerability**: Reflected Cross Site Scripting (XSS) found at `10.0.1.5/mutilidae/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.

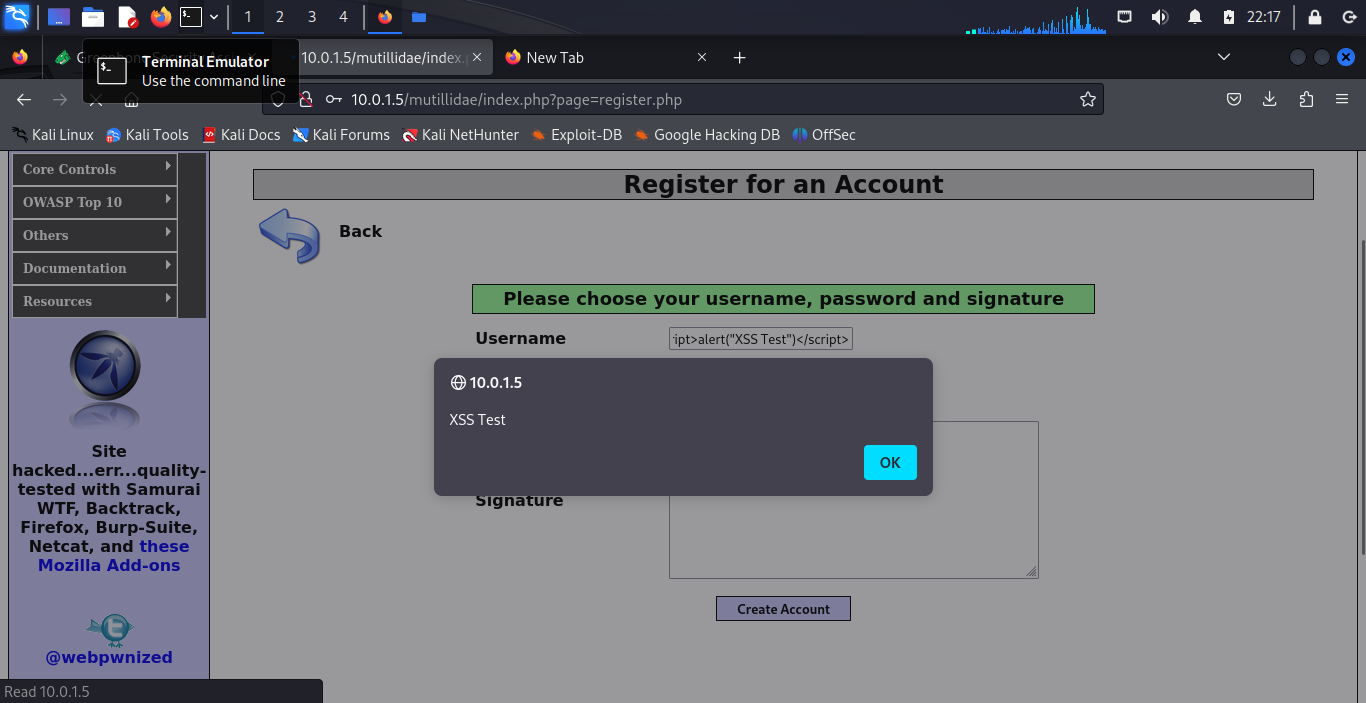
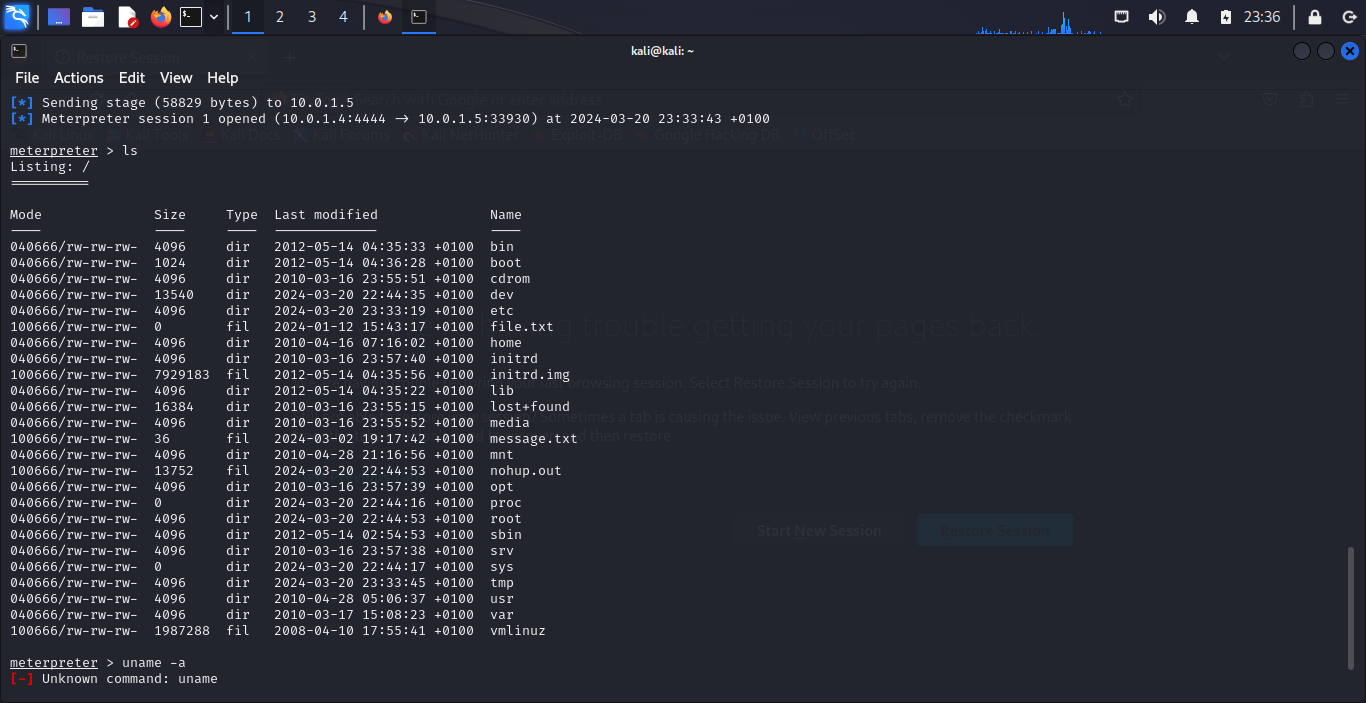


Figure 5 cross site scripting

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.

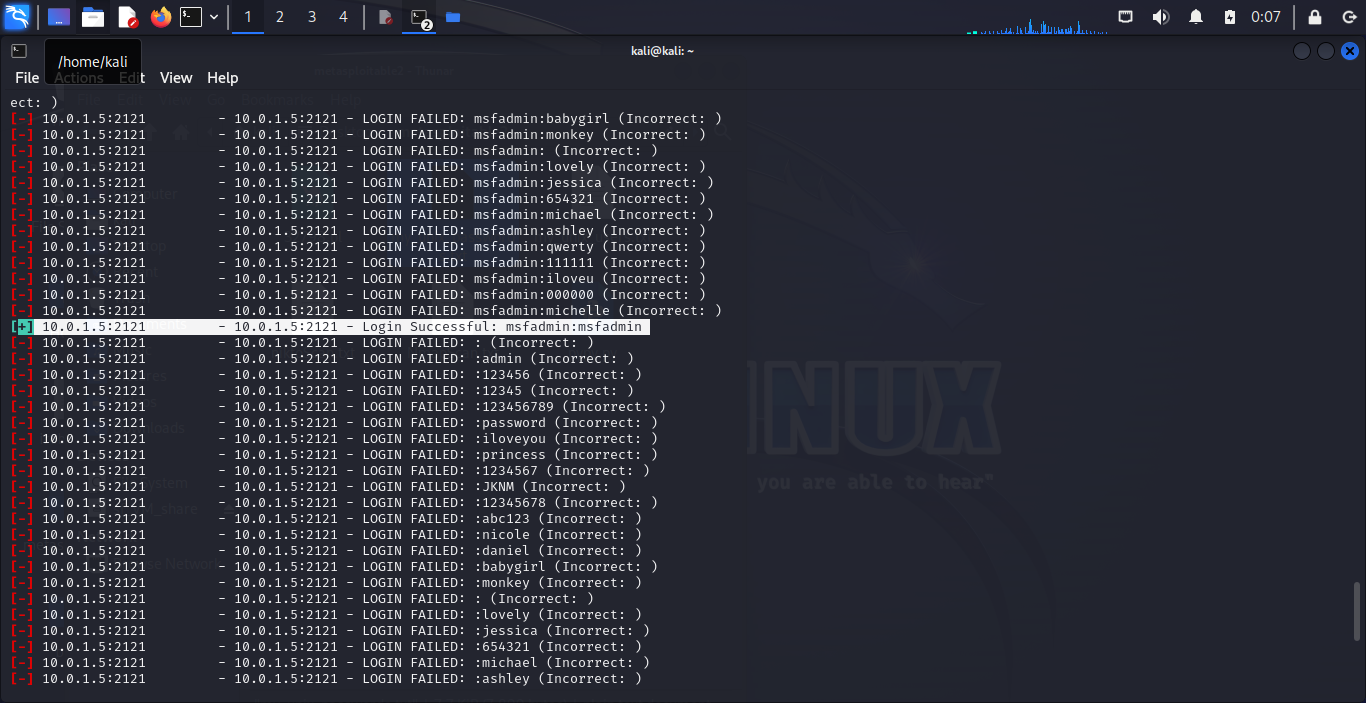
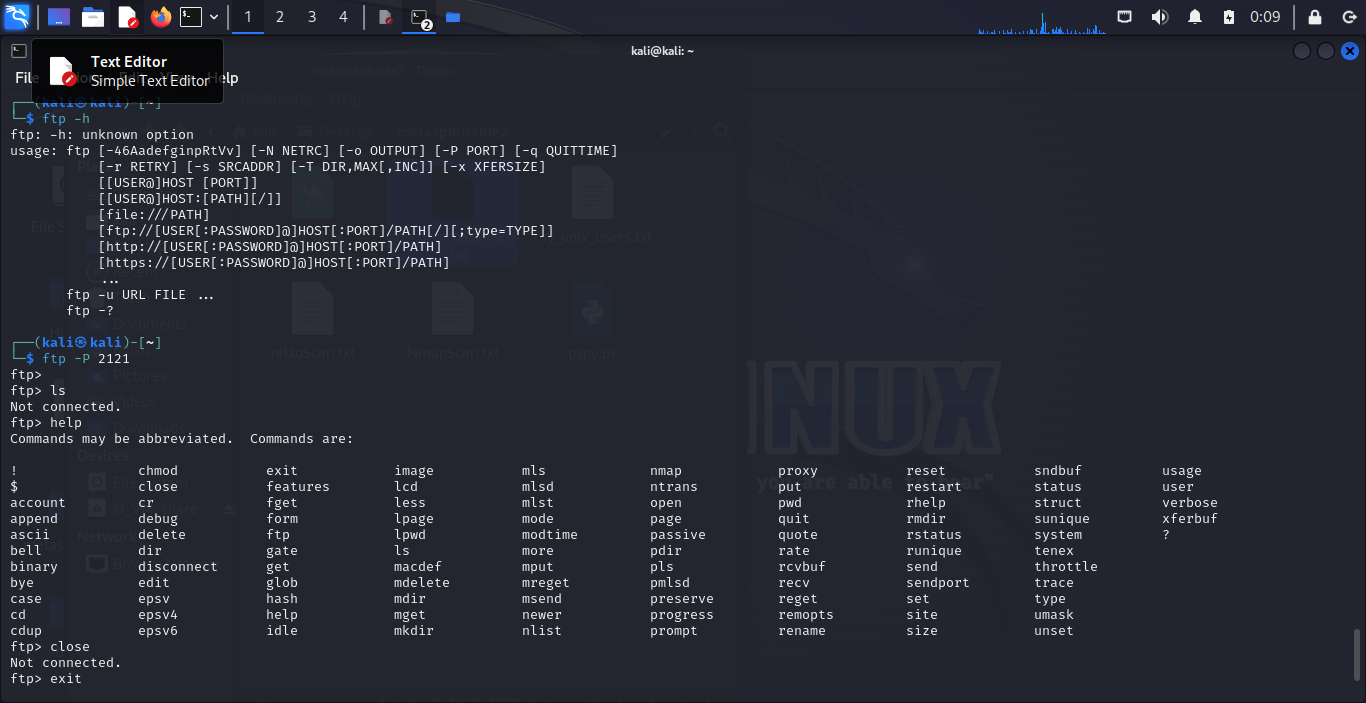


Figure 6 Brute force result



8. Port 5900 VNC:

**Exploit Used**: Brute force attack to obtain credentials

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

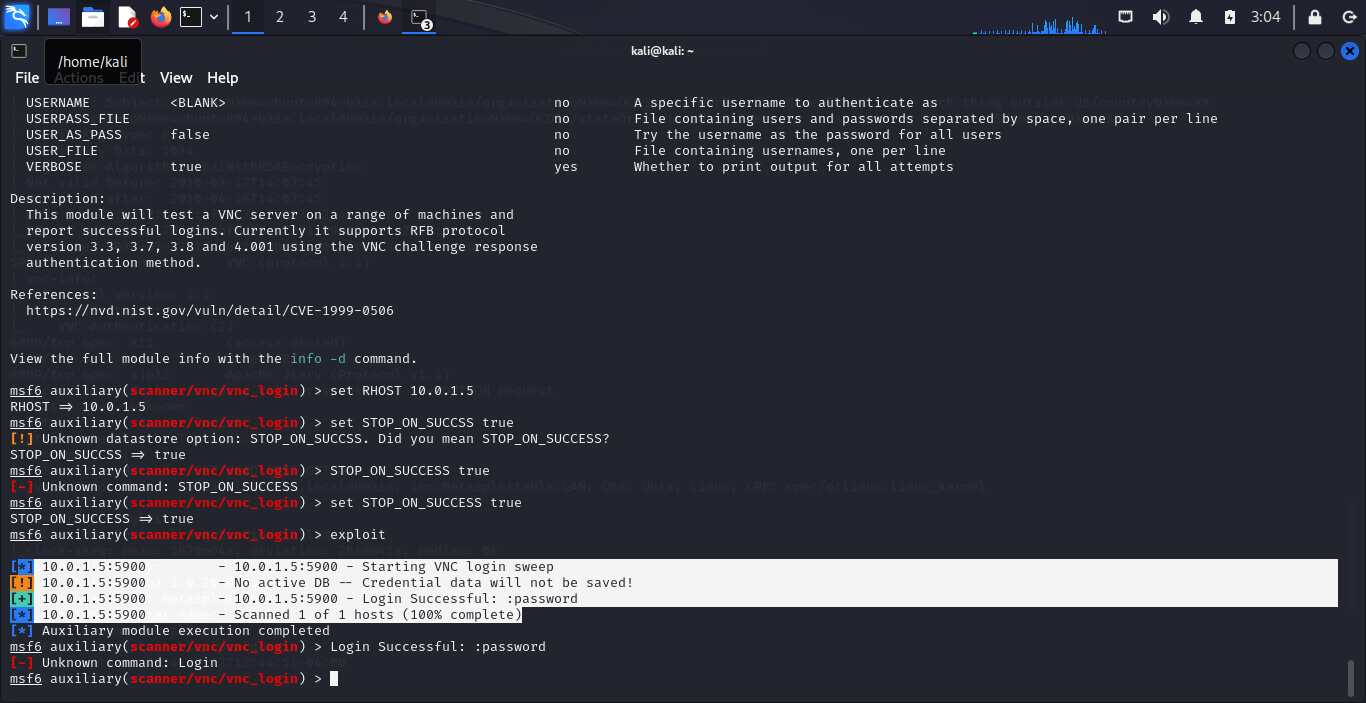


Figure 7 VNC Proof

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.

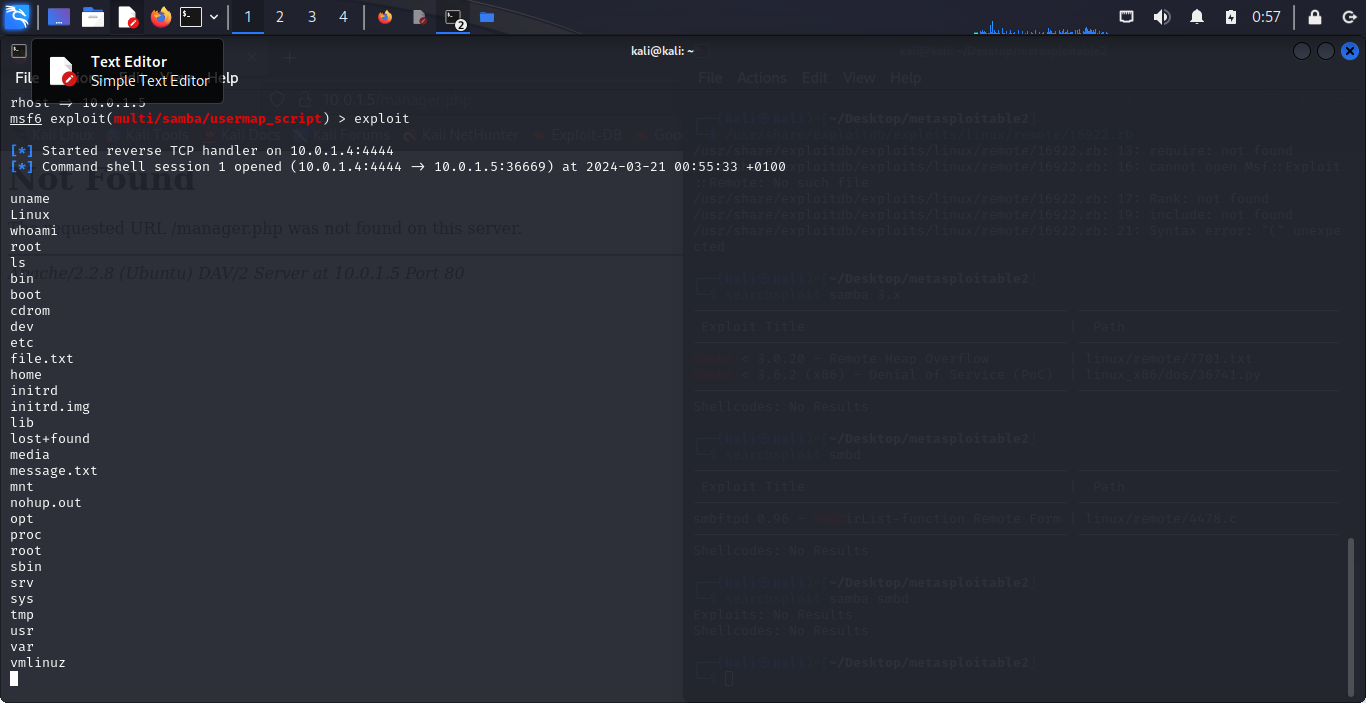


Figure 8 Samba Proof

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.