# Penetration Testing Lab

## Objective

The Penetration Testing Lab project aimed to establish a virtual environment for conducting controlled penetration tests using Kali Linux and Metasploitable. The primary focus was to identify, exploit, and analyze vulnerabilities within a simulated network environment. This hands-on experience provided practical skills in network security, vulnerability assessment, and exploitation, enhancing understanding of offensive and defensive cybersecurity techniques.

## Skills Learned

Penetration Testing Fundamentals: Practical understanding of penetration testing methods and tools.  
Network Scanning and Enumeration: Ability to identify open ports and running services on target machines.  
Exploitation and Vulnerability Analysis: Proficiency in discovering and exploiting system vulnerabilities.  
Security Recommendations: Developing strategies to improve system security based on identified vulnerabilities.  
Documentation and Reporting: Learning to document findings and communicate them clearly.

## Tools Used

Kali Linux: As the primary penetration testing operating system.  
Metasploitable: A vulnerable virtual machine used as the target for exploitation.  
Metasploit Framework: For exploiting vulnerabilities and conducting penetration tests.  
Nmap: For network discovery and scanning open ports on the target.  
Telnet: To remotely access the Metasploitable machine for further investigation.  
Wireshark: For analyzing captured network traffic (optional, for deeper analysis).

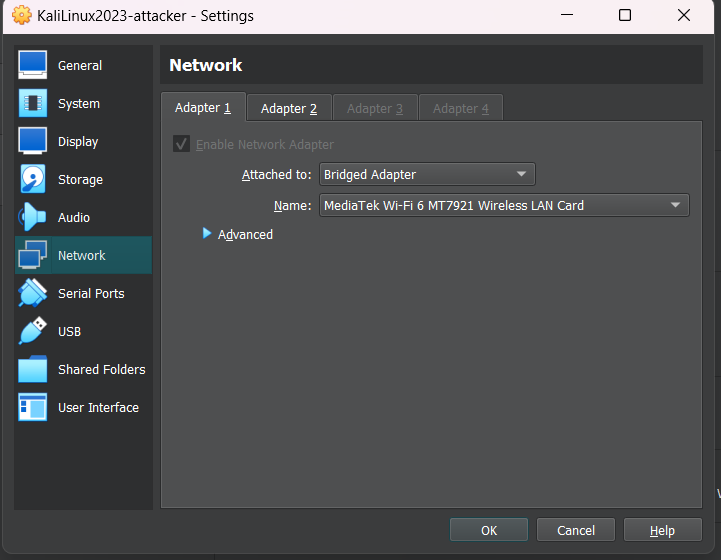
## Steps

### 1. Network Configuration

Objective: Set up the virtual network to allow communication between the Kali Linux (attacker) and Metasploitable (victim) virtual machines.

- Adapter Settings:  
 - Kali Linux: Set Adapter 1 to Bridged Adapter and Adapter 2 to Internal Network.  
 - Metasploitable: Set Adapter 1 to Bridged Adapter.

Screenshot:



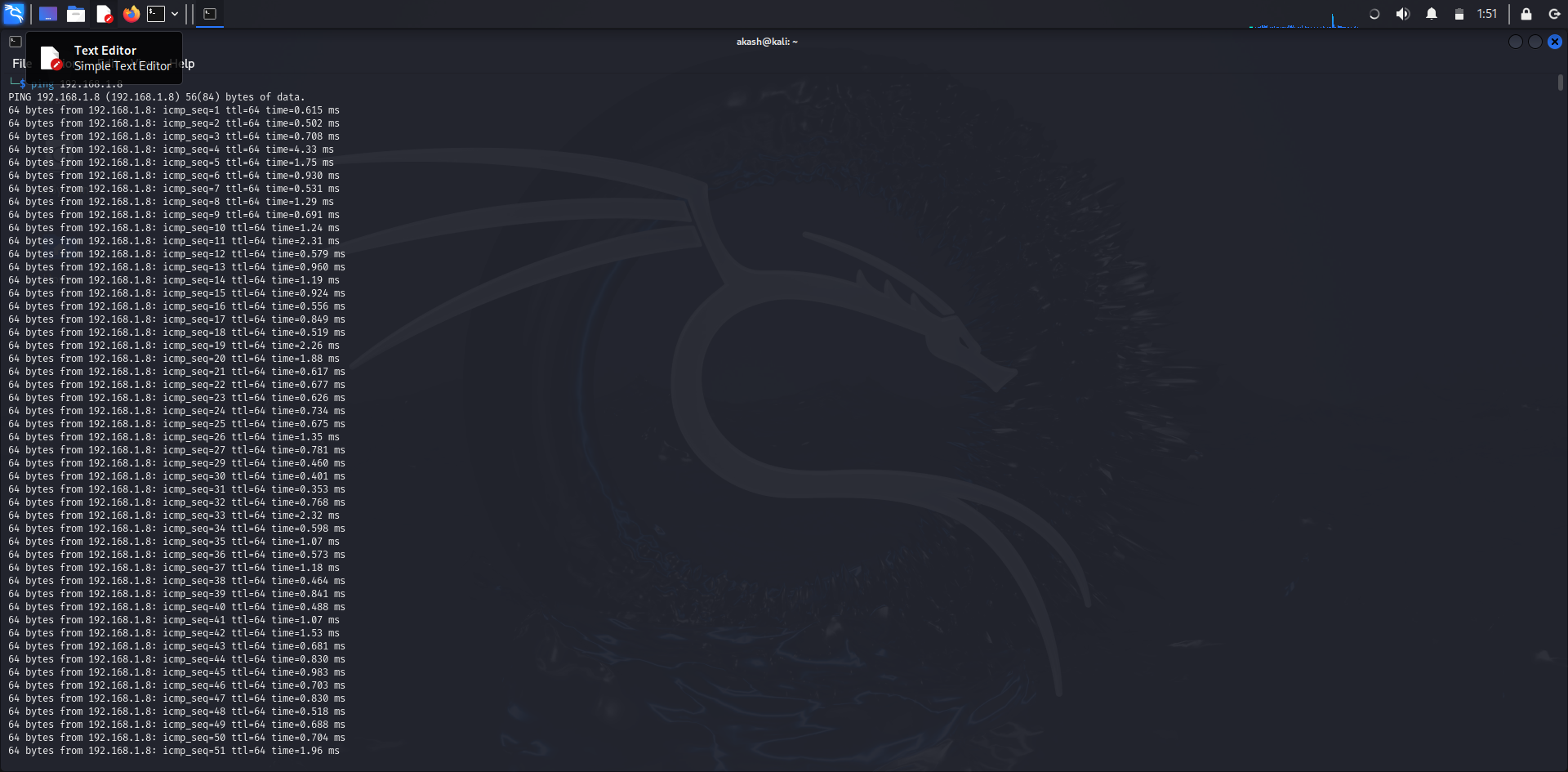
### 2. Testing Network Connectivity

Objective: Verify network connectivity between Kali and Metasploitable by pinging the Metasploitable IP from Kali.

- Command:  
 ```bash  
 ping <Metasploitable IP>  
 ```

Expected Result: Successful response from the Metasploitable IP, indicating connectivity.

Screenshot:

 Ping Response

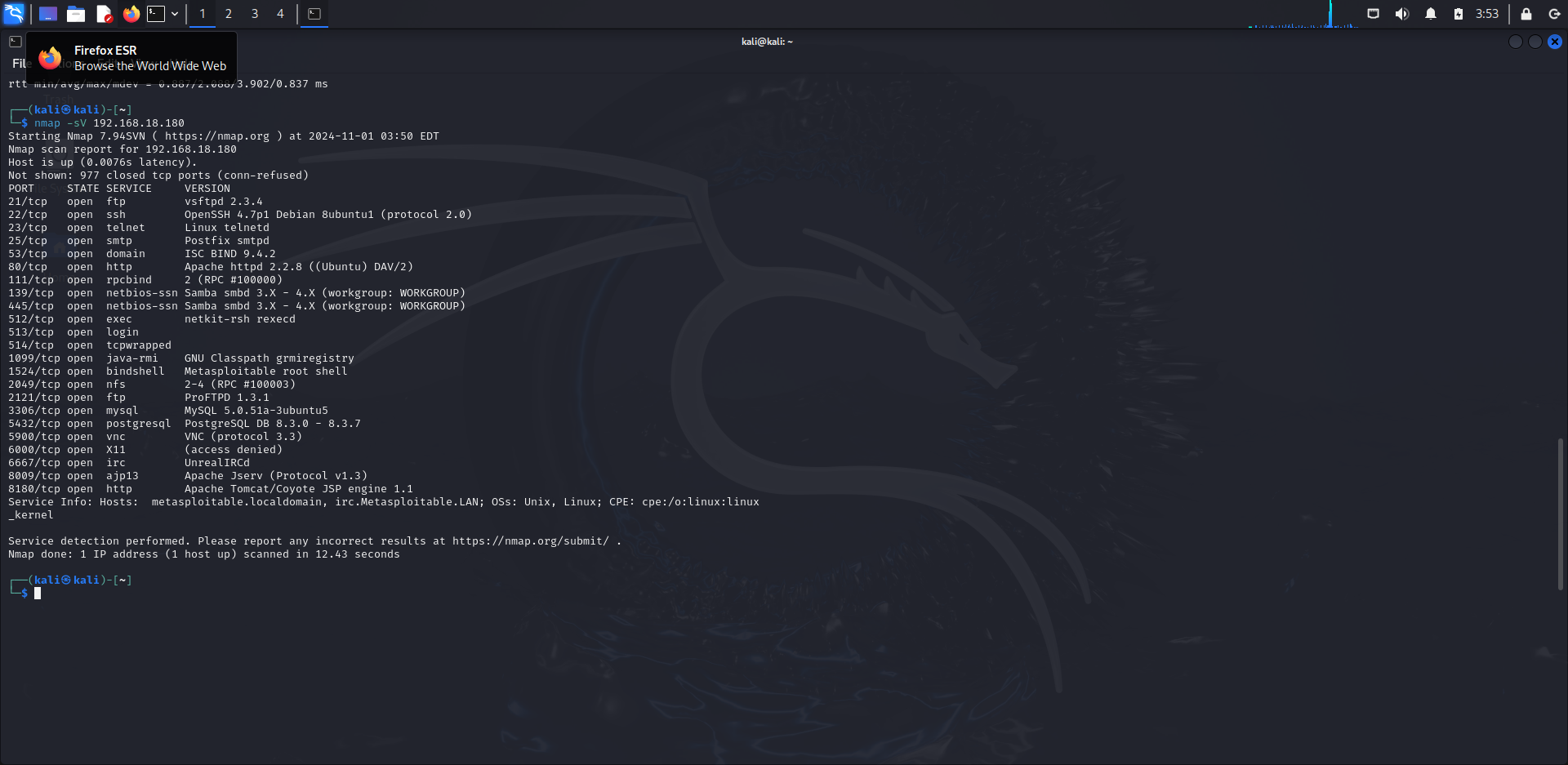
### 3. Initial Nmap Scan

Objective: Identify open ports and services running on the Metasploitable machine.

- Command:  
 ```bash  
 nmap -sS -A <Metasploitable IP>  
 ```

Expected Result: List of open ports and services, such as FTP, SSH, and Telnet, indicating potential entry points for exploitation.

Screenshot:

Nmap Results

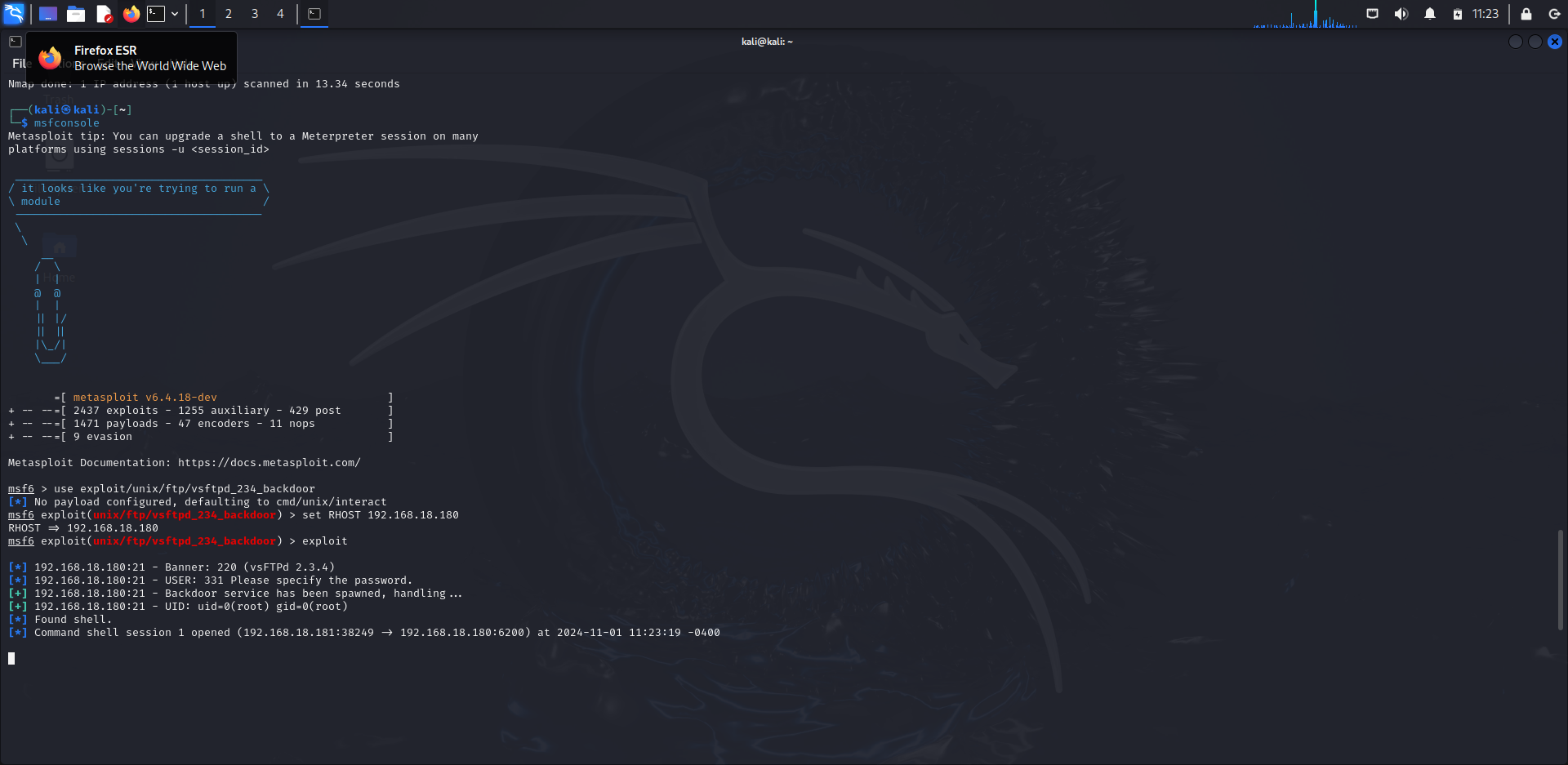
### 4. Exploiting the vsftpd 2.3.4 Vulnerability

Objective: Use Metasploit to exploit a known vulnerability in the vsftpd service to gain access to the target.

- Command Sequence:  
 ```bash  
 msfconsole  
 use exploit/unix/ftp/vsftpd\_234\_backdoor  
 set RHOST <Metasploitable IP>  
 exploit  
 ```

Expected Result: A successful session indicating that access was gained via the vsftpd vulnerability.

Screenshot:

 Metasploit Exploit

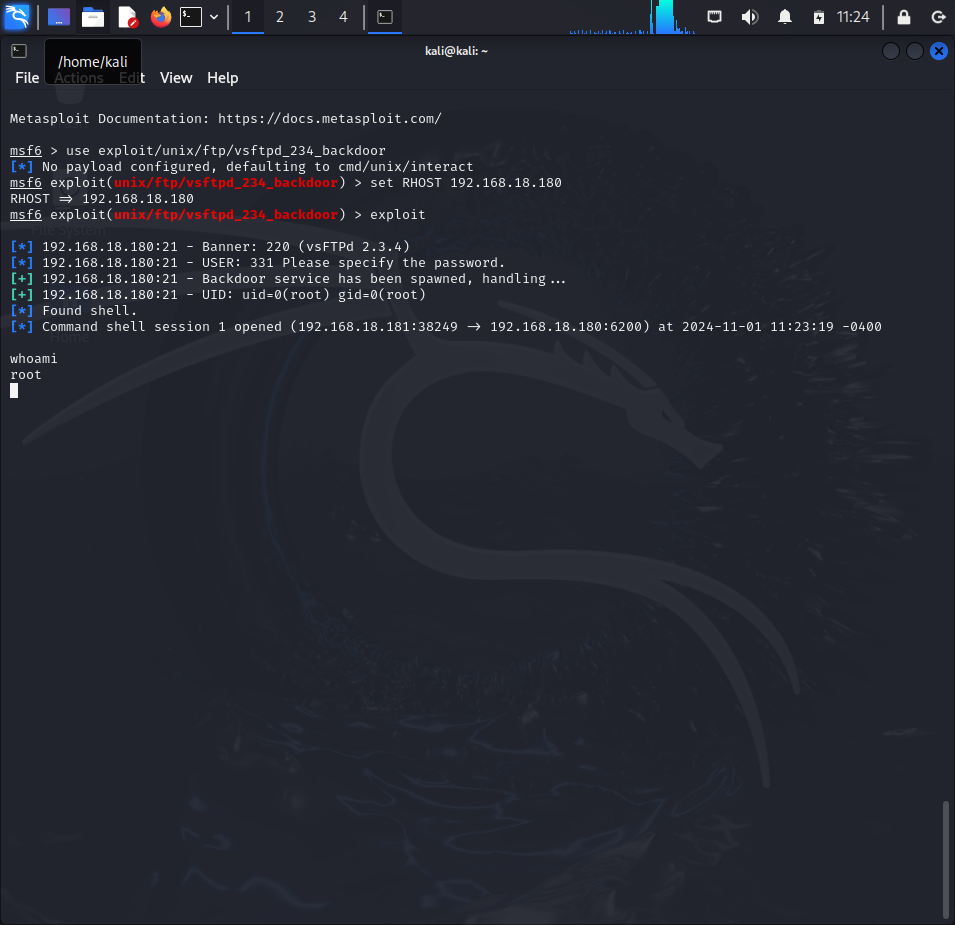
### 5. Checking Access Privileges

Objective: Verify access level on the Metasploitable system using `whoami`.

- Command:  
 ```bash  
 whoami  
 ```

Expected Result: Display the username of the current session, confirming whether access was gained as `msfadmin` or `root`.

Screenshot:

 whoami Command

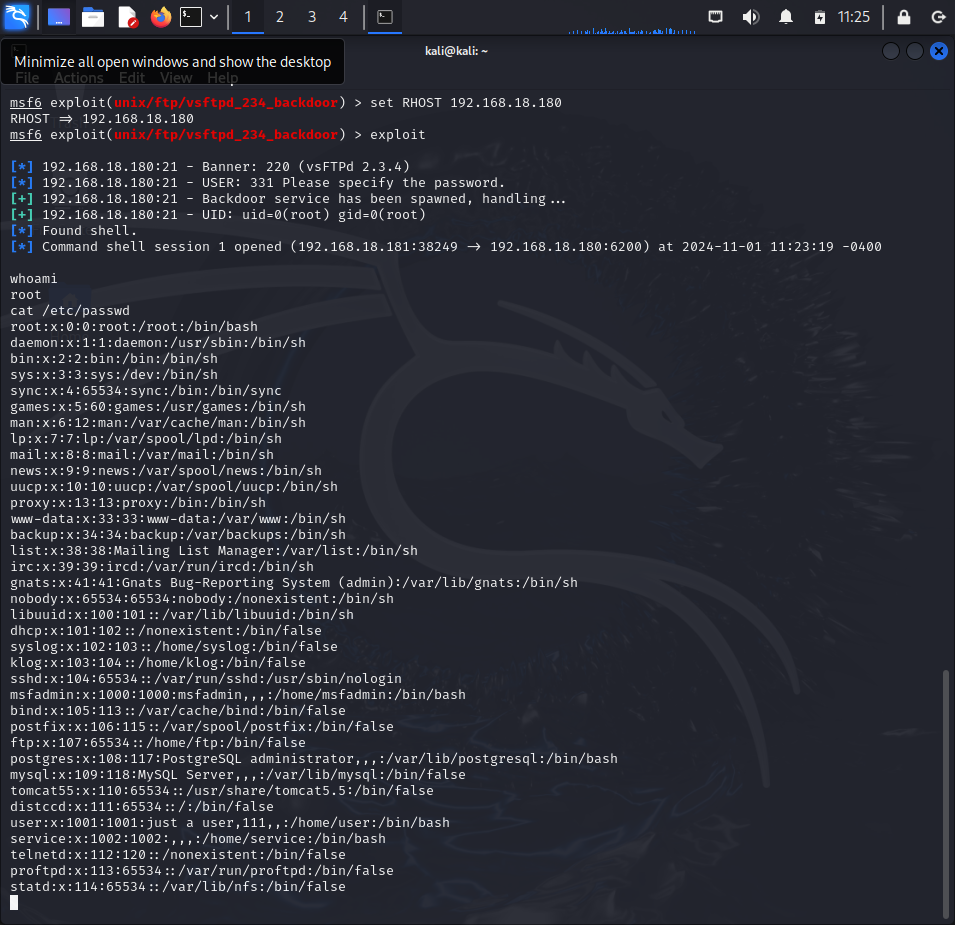
### 6. Listing User Accounts

Objective: Identify user accounts configured on the system to determine possible points of privilege escalation.

- Command:  
 ```bash  
 cat /etc/passwd  
 ```

Expected Result: List of user accounts on the system.

Screenshot:

 User Accounts

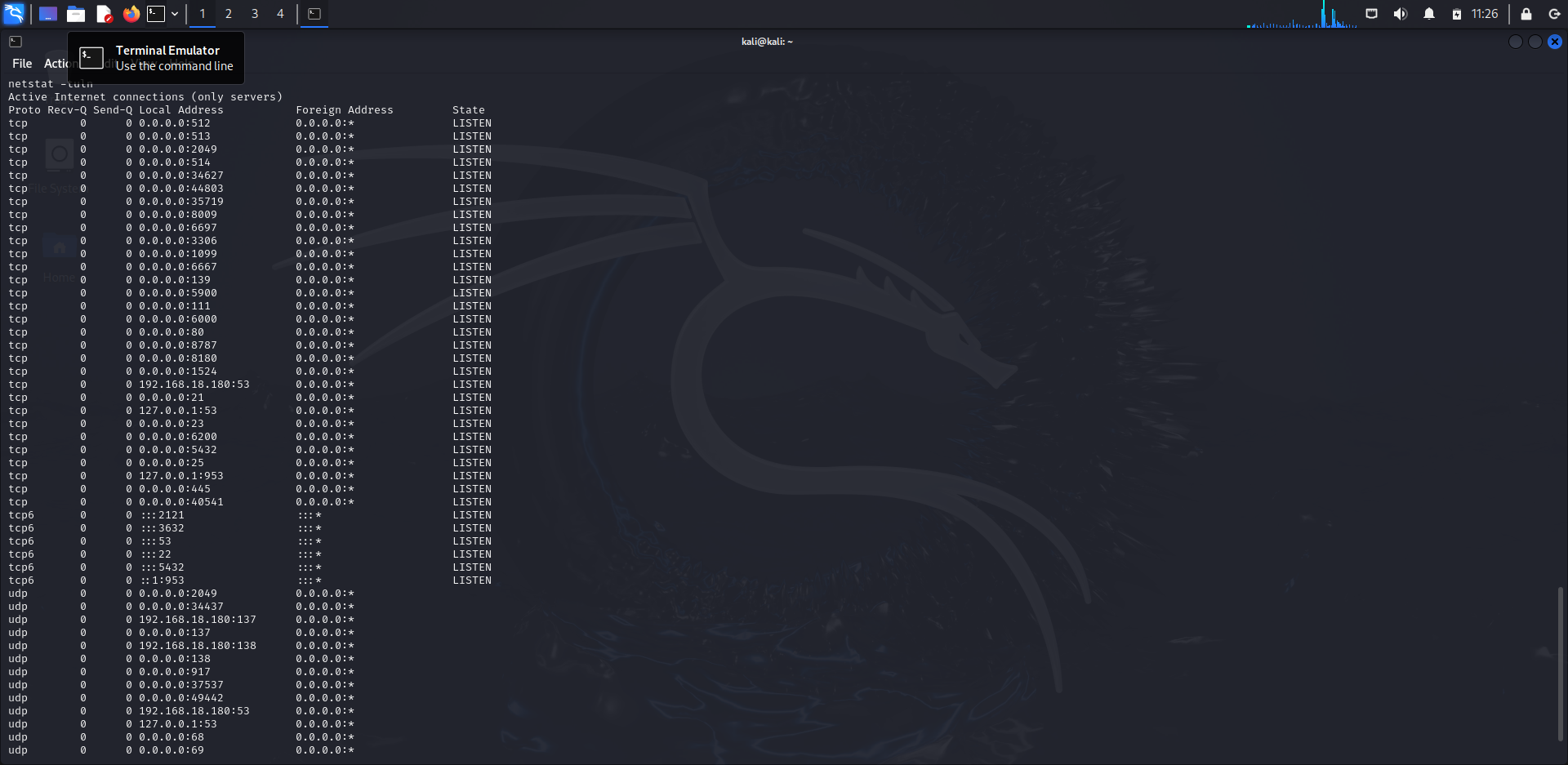
### 7. Checking Running Services

Objective: Identify active services to look for additional potential vulnerabilities.

- Command:  
 ```bash  
 netstat -tuln  
 ```

Expected Result: List of listening services and their respective ports.

Screenshot:

 Running Services

# 8. Documenting Findings

## 1. Network Configuration and Connectivity

Network Setup: The virtual machines were set up with Kali Linux as the attacker machine and Metasploitable as the target machine.

Network Settings: Both machines were connected via an Internal Network to allow direct communication.

Connectivity Verification: The connection was verified by successfully pinging the Metasploitable machine from Kali.

## 2. Initial Nmap Scan Results

Objective: To enumerate open ports and services on the Metasploitable machine to identify potential entry points.

Scan Command:  
nmap -sS -A <Metasploitable IP>

Findings:  
- Open Ports: Ports 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), and 80 (HTTP) were found open.  
- Service Information: The scan identified various services, including vsftpd on port 21, which indicated a potentially vulnerable version (2.3.4).  
- Vulnerable Services: The presence of vsftpd 2.3.4 was notable as it is known to have a backdoor vulnerability, making it a prime candidate for exploitation.

## 3. Exploitation of vsftpd Vulnerability

Exploit Used: vsftpd 2.3.4 backdoor exploit in Metasploit.

Command Sequence:  
msfconsole  
use exploit/unix/ftp/vsftpd\_234\_backdoor  
set RHOST <Metasploitable IP>  
exploit

Outcome: After executing the exploit, a new session was opened, indicating successful access to the Metasploitable machine through the vsftpd backdoor.

## 4. Privilege Level and User Verification

Objective: Verify the access level achieved on the target system.

Verification Command:  
whoami

Result: The command confirmed access as root, providing full privileges on the Metasploitable system.

## 5. Enumeration of User Accounts

Objective: Identify existing user accounts to assess privilege escalation opportunities and potential targets.

Command:  
cat /etc/passwd

Result: The file /etc/passwd listed multiple users, including standard system accounts.

## 6. Running Services and Open Ports Analysis

Objective: Check for any services currently active on the machine, which could be used to expand the scope of penetration testing.

Command:  
netstat -tuln

Findings: Displayed various open ports and services, which were reviewed for potential further exploitation.

## 7. Potential Vulnerabilities and Security Recommendations

Vulnerabilities Identified:  
- FTP Service: The vsftpd 2.3.4 vulnerability provides unauthorized access via a backdoor.  
- Telnet: Telnet is insecure as it transmits data in plain text.

Security Recommendations:  
- Service Hardening: Disable unnecessary services like Telnet and FTP on production systems.  
- Regular Updates: Keep services up-to-date to avoid known vulnerabilities.  
- Access Control: Limit access to sensitive services and ports.  
- Monitoring and Logging: Implement logging and alerting for unauthorized access attempts.