SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2017-18

Práctica [1]. Administración de la seguridad en Linux

Sesión [2]. Herramientas básicas de seguridad

Autor[1]: Rubén Calvo Villazán

Ejercicio 1.

1º

Actividad de la red con lsof -i:

```
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
dhclient 772 root    6u  IPv4  19677      0t0  UDP *:bootpc
megasync 995 root   25u  IPv4  20767      0t0  TCP localhost:6342 (LISTEN)
megasync 995 root   31u  IPv4  45858      0t0  TCP cvi042030.ugr.es:60298->lu5.api.mega.nz:https (ESTABLISHED)
megasync 995 root   34u  IPv4  47830      0t0  TCP cvi042030.ugr.es:57024->lu7.api.mega.nz:http (ESTABLISHED)
```

2º

Para ver si hay un servicio ssh (se está escuchando en el puerto 22):

```
$> lsof -i :22
```

Si hay tráfico saliente ssh:

Si hay una conexión establecida a nuestra máquina por medio de ssh, basta con mirar el

fichero: /var/log/auth.log y ver los registros correspondientes a ssh.

3º

```
$> lsof -c init -uroot
```

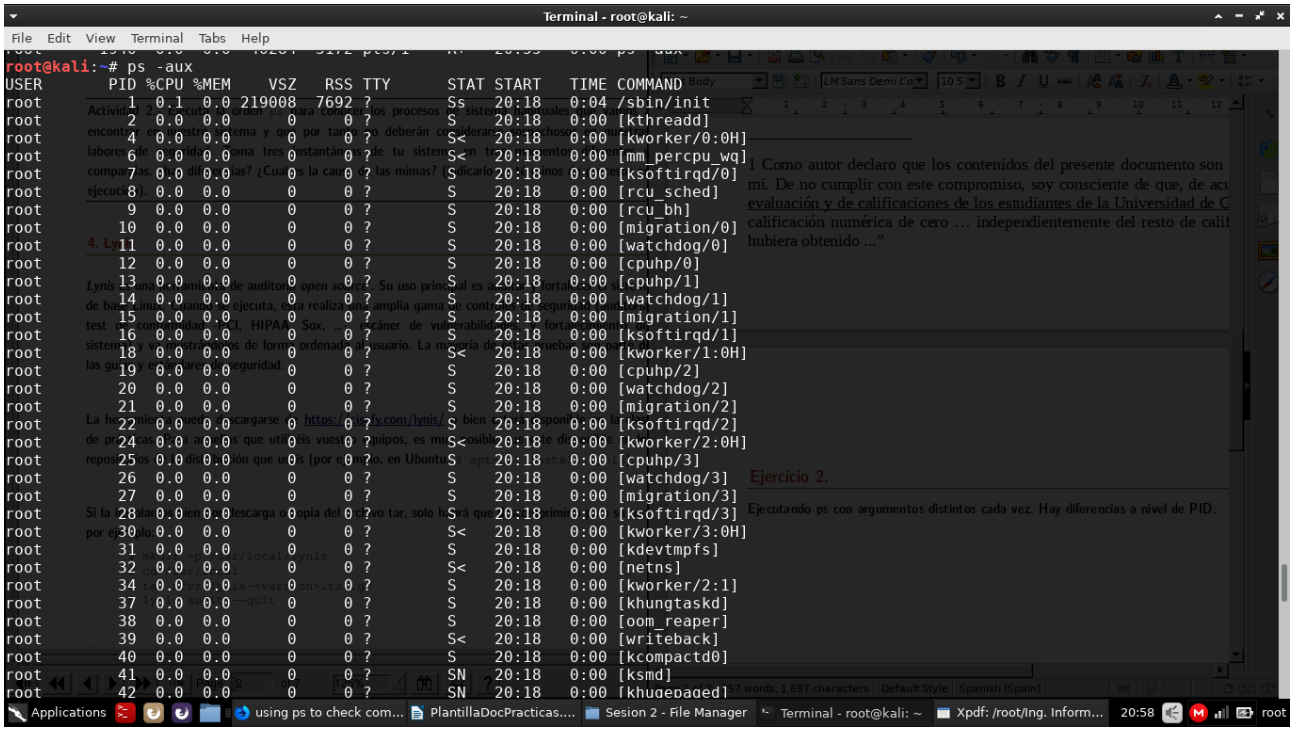
Usando el comando lsof nos muestra los archivos abiertos por algun proceso, con -c init especificamos que queremos los del proceso init y con -uroot especificamos que queremos todos los correspondientes al usuario root

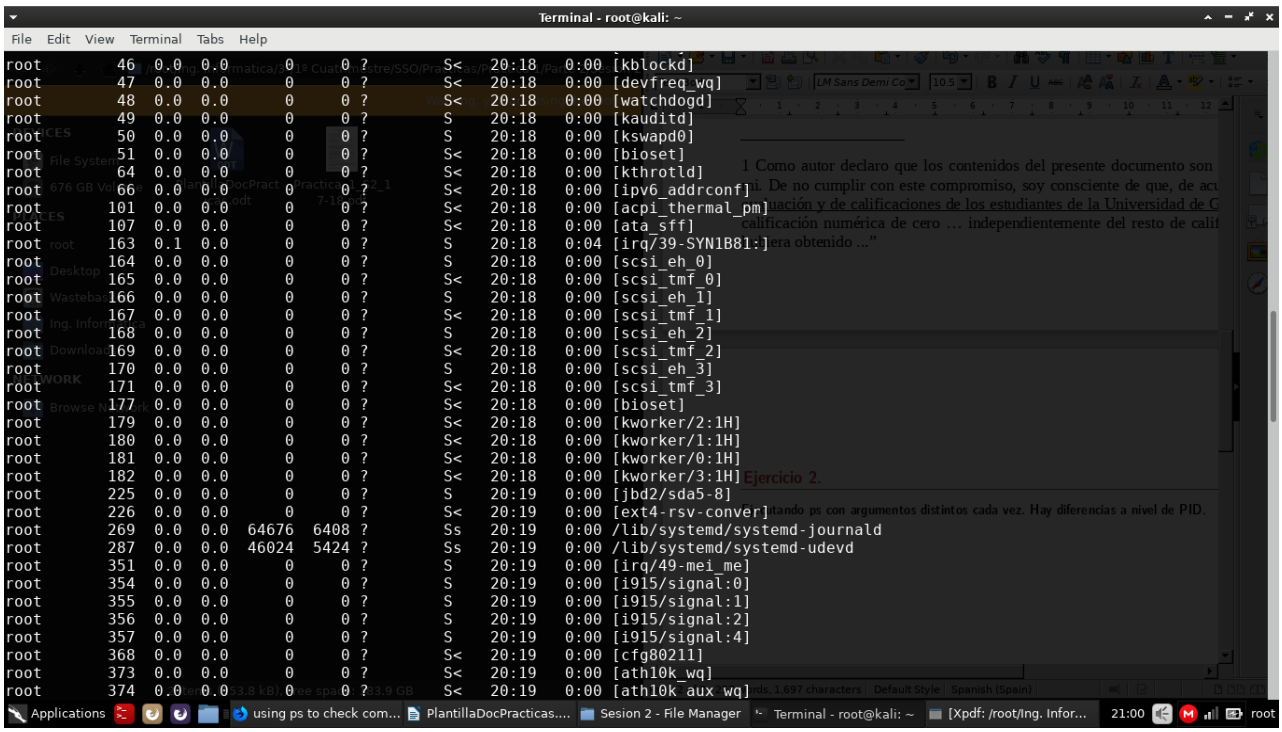
---

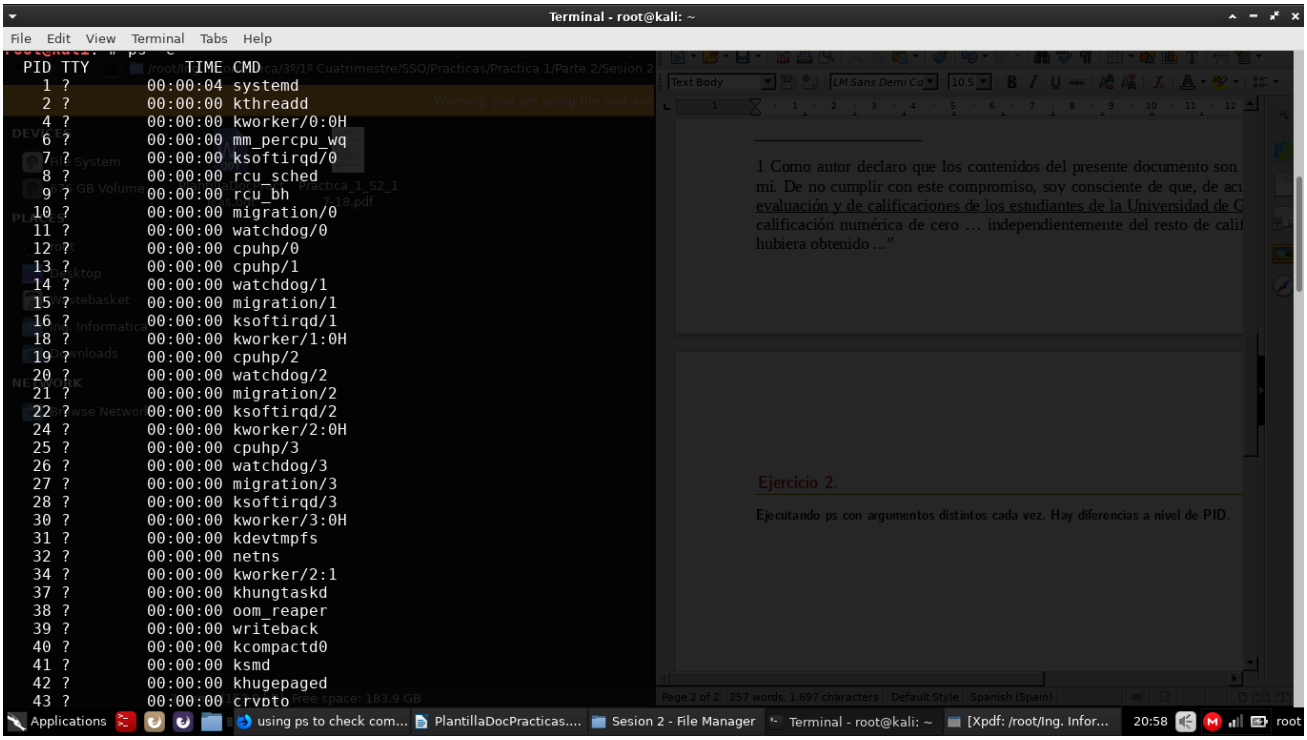
1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la "Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada" esto "conllevará la calificación numérica de cero … independientemente del resto de calificaciones que el estudiante hubiera obtenido ..."

Ejercicio 2.

Ejecutando ps con argumentos distintos cada vez. Hay diferencias a nivel de PID.







Ejercicio 3.

1º

Las vulnerabilidades encontradas son:

! No password set for single mode [AUTH-9308]

! Can't find any security repository in /etc/apt/sources.list or sources.list.d directory [PKGS-7388]

! iptables module(s) loaded, but no rules active [FIRE-4512]

El grado de severidad es medio, algunas sugerencias para solucionarlas son:

Asignar una contraseña al GRUB bootloader y a singlemode.

Separar en particiones /tmp y /var.

Establecer reglas para iptables.

Asignar repositorios seguros en /etc/apt/sources.list para apt.

2º

La vulnerabilidad shellshock tiene de código SHLL-6290, tras ejecutar un analisis con Lynis hacemos:

cat /var/log/lynis.log | grep SHLL-6290

Si no aparece registro, no tenemos la vulnerabilidad. Para ver otras vulnerabilidades relacionadas con la shell:

cat /var/log/lynis.log | grep SHLL

2017-10-20 21:25:55 Skipped test SHLL-6202 (Check console TTYs)

2017-10-20 21:25:55 Performing test ID SHLL-6211 (Checking available and valid shells)

2017-10-20 21:25:55 Performing test ID SHLL-6220 (Checking available and valid shells)

2017-10-20 21:25:55 Performing test ID SHLL-6230 (Perform umask check for shell configurations)

3º

Si tenemos un antivirus instalado, Lynis lo detectará. Podemos ver el resultado del análisis relativo al antivirus con:

cat /var/log/lynis.log | grep anti

2017-10-20 21:51:58 Performing test ID MALW-3280 (Check if anti-virus tool is installed)

2017-10-20 21:51:58 Test: checking process TmccMac to test for Trend Micro anti-virus (macOS)

2017-10-20 21:51:58 Result: no commercial anti-virus tools found

Ejercicio 4.

1º

Tras realizar un análisis con rkhunter: rkhunter –check

Aparece todo correcto salvo en las siguientes advertencias.

/usr/bin/lwp-request

Se soluciona creando o editando `/etc/rkhunter.conf.local`

y añadiendo PKGMGR=DPKG

Checking for suspicious shared memory segments

Se soluciona añadiendo a whitelist los procesos que usen memoria compartida

```
ALLOWIPCPROC=path/to/service
```

Checking if SSH root access is allowed

Se soluciona editando el fichero rkhunter:

```
cat /etc/rkhunter.conf | grep ALLOW_SSH_ROOT_USER
```

Cambiando:

```
ALLOW_SSH_ROOT_USER=no
```

Y cambiando en ssh:

```
cat /etc/ssh/sshd_config | grep PermitRootLogin
```

Editando:

```
PermitRootLogin no
```