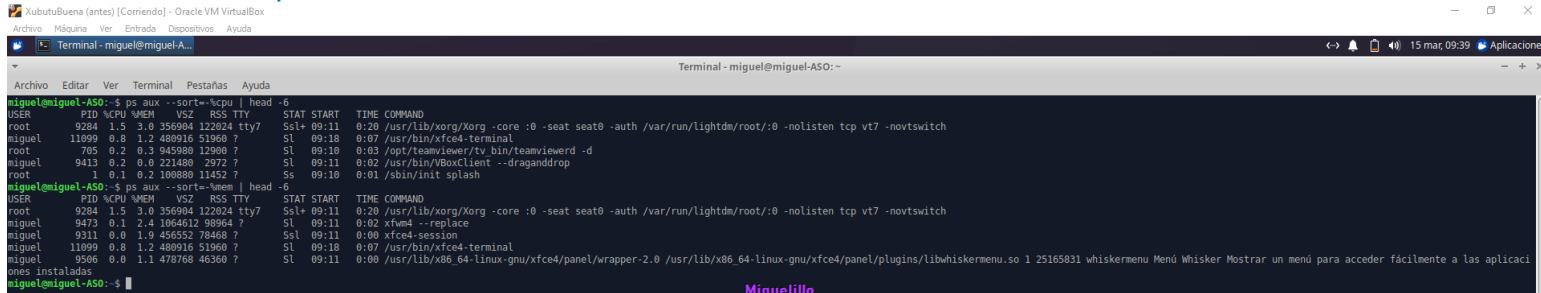


UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

En la UD 07 hay un criterio de evaluación que dice lo siguiente: “Se han tomado medidas de seguridad ante la aparición de procesos no identificados”

¿Qué harías en tu servidor Linux?

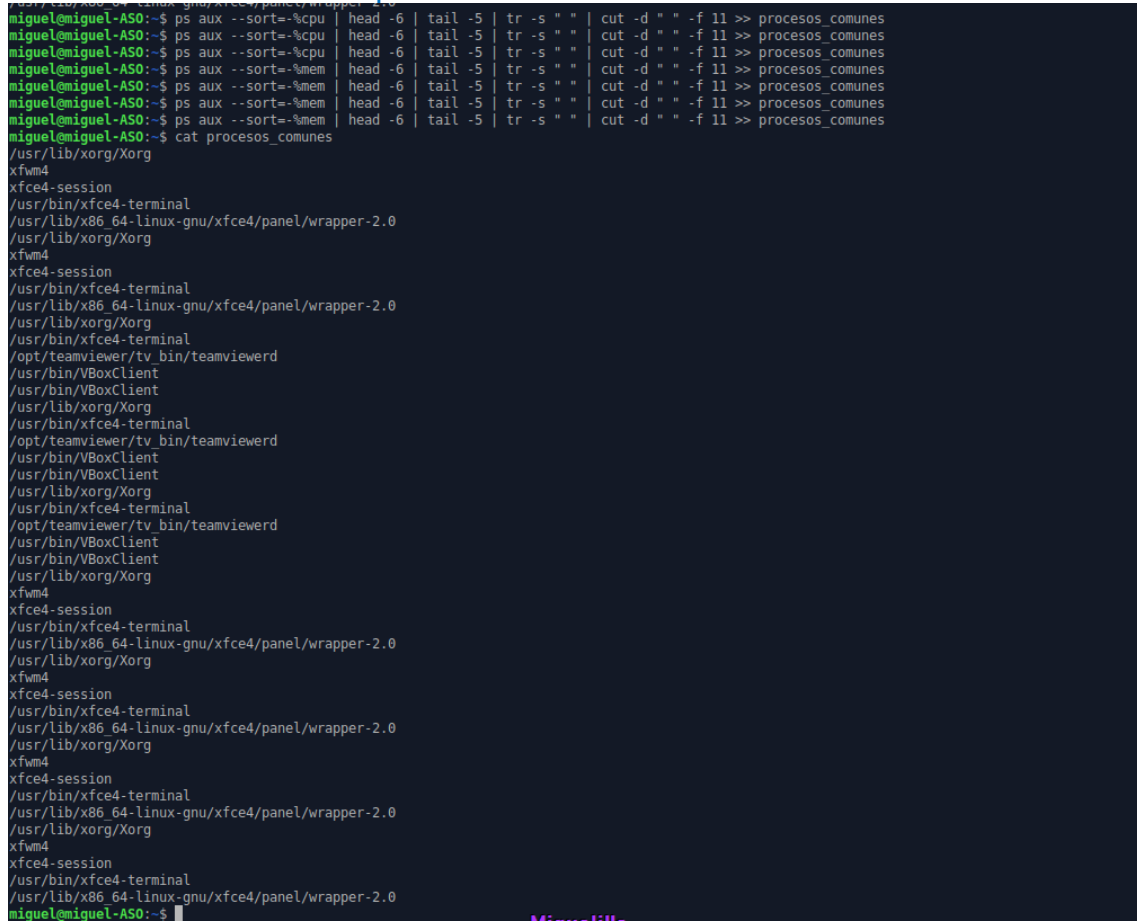
Para poder encontrar procesos sin identificar maliciosos, podemos monitorizar los procesos del equipo por uso de la CPU o de RAM en mi caso cojo solamente los 6 primeros. Podemos hacer un script donde pongamos los procesos más usuales que consuman más memoria y más CPU. En caso que no aparezcan nos aparezca un aviso.



```
miguel@miguel-ASO:~$ ps aux --sort=-%cpu | head -6
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         9284  1.5  3.0 356904 122024 tty7    Ssl+ 09:11   0:20 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswi
root      11099  0.8  1.2 480916 51968 ?        Sl   09:18   0:07 /usr/bin/xfce4-terminal
root         705  0.2  0.3 945988 12908 ?        Sl   09:10   0:03 /opt/teamviewer/tv_bin/teamviewer -d
miguel      9413  0.2  0.0 221488 2972 ?        Sl   09:11   0:02 /usr/bin/VBoxClient --draganddrop
root          1  0.1  0.2 108888 11452 ?        Ss   09:10   0:01 /sbin/init splash

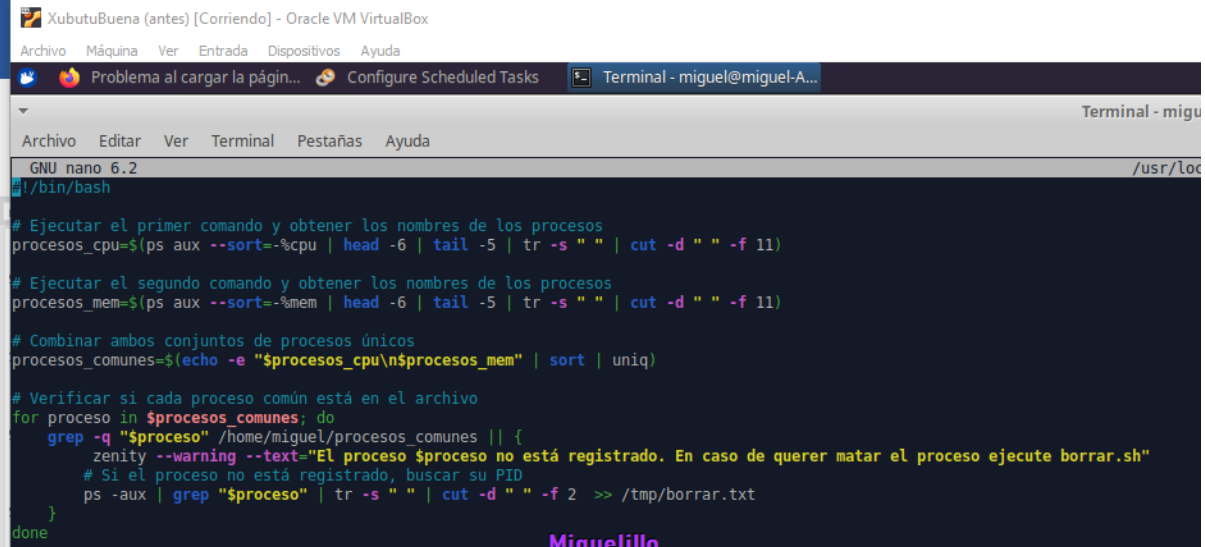
miguel@miguel-ASO:~$ ps aux --sort=-%mem | head -6
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         9284  1.5  3.0 356904 122024 tty7    Ssl+ 09:11   0:20 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswi
miguel      9473  0.1  2.4 1064612 98964 ?        Sl   09:11   0:02 xfwm4 --replace
miguel      9311  0.0  1.9 456552 78468 ?        Ssl 09:11   0:00 xfce4-session
miguel      11099  0.8  1.2 480916 51968 ?        Sl   09:18   0:07 /usr/bin/xfce4-terminal
miguel      9506  0.0  1.1 478768 46360 ?        Sl   09:11   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libwhiskermenu.so 1 25165831 whiskermenu Menú Whisker Mostrar un menú para acceder fácilmente a las aplicac
iones instaladas
miguel@miguel-ASO:~$
```

Relleno el fichero con los procesos comunes del sistema



```
miguel@miguel-ASO:~$ ps aux --sort=-%cpu | head -6 | tail -5 | tr -s " " | cut -d " " -f 11 >> procesos_comunes
miguel@miguel-ASO:~$ ps aux --sort=-%cpu | head -6 | tail -5 | tr -s " " | cut -d " " -f 11 >> procesos_comunes
miguel@miguel-ASO:~$ ps aux --sort=-%cpu | head -6 | tail -5 | tr -s " " | cut -d " " -f 11 >> procesos_comunes
miguel@miguel-ASO:~$ ps aux --sort=-%mem | head -6 | tail -5 | tr -s " " | cut -d " " -f 11 >> procesos_comunes
miguel@miguel-ASO:~$ ps aux --sort=-%mem | head -6 | tail -5 | tr -s " " | cut -d " " -f 11 >> procesos_comunes
miguel@miguel-ASO:~$ ps aux --sort=-%mem | head -6 | tail -5 | tr -s " " | cut -d " " -f 11 >> procesos_comunes
miguel@miguel-ASO:~$ cat procesos_comunes
/usr/lib/xorg/Xorg
xfwm4
xfce4-session
/usr/bin/xfce4-terminal
/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
/usr/lib/xorg/Xorg
xfwm4
xfce4-session
/usr/bin/xfce4-terminal
/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
/usr/lib/xorg/Xorg
/usr/bin/xfce4-terminal
/opt/teamviewer/tv_bin/teamviewer
/usr/bin/VBoxClient
/usr/bin/VBoxClient
/usr/lib/xorg/Xorg
/usr/bin/xfce4-terminal
/opt/teamviewer/tv_bin/teamviewer
/usr/bin/VBoxClient
/usr/bin/VBoxClient
/usr/lib/xorg/Xorg
/usr/bin/xfce4-terminal
/opt/teamviewer/tv_bin/teamviewer
/usr/bin/VBoxClient
/usr/bin/VBoxClient
/usr/lib/xorg/Xorg
/usr/bin/xfce4-terminal
/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
/usr/lib/xorg/Xorg
xfwm4
xfce4-session
/usr/bin/xfce4-terminal
/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
/usr/lib/xorg/Xorg
xfwm4
xfce4-session
/usr/bin/xfce4-terminal
/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
/usr/lib/xorg/Xorg
xfwm4
xfce4-session
/usr/bin/xfce4-terminal
/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
miguel@miguel-ASO:~$
```

Creo un script que cuando detecta un proceso que no está añadido lo detecta este saca un mensaje de error



```

XubutuBuena (antes) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Problema al cargar la página... Configure Scheduled Tasks Terminal - miguel@miguel-A...

GNU nano 6.2 /usr/local/bin/procesos.sh
#!/bin/bash

# Ejecutar el primer comando y obtener los nombres de los procesos
procesos_cpu=$(ps aux --sort=-%cpu | head -6 | tail -5 | tr -s " " | cut -d " " -f 11)

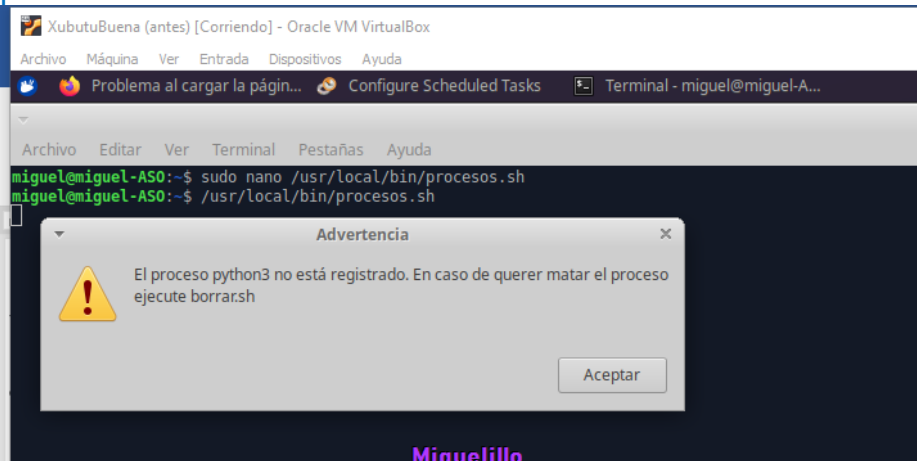
# Ejecutar el segundo comando y obtener los nombres de los procesos
procesos_mem=$(ps aux --sort=-%mem | head -6 | tail -5 | tr -s " " | cut -d " " -f 11)

# Combinar ambos conjuntos de procesos únicos
procesos_comunes=$(echo -e "$procesos_cpu\n$procesos_mem" | sort | uniq)

# Verificar si cada proceso común está en el archivo
for proceso in $procesos_comunes; do
    grep -q "$proceso" /home/miguel/procesos_comunes || {
        zenity --warning --text="El proceso $proceso no está registrado. En caso de querer matar el proceso ejecute borrar.sh"
        # Si el proceso no está registrado, buscar su PID
        ps -aux | grep "$proceso" | tr -s " " | cut -d " " -f 2 >> /tmp/borrar.txt
    }
done
Miguelillo

```

Lo pruebo y funciona, el “fallo de este script es que debemos añadir todos los procesos pesados que utilicemos habitualmente” una vez detenta el proceso podemos borrarlos



```

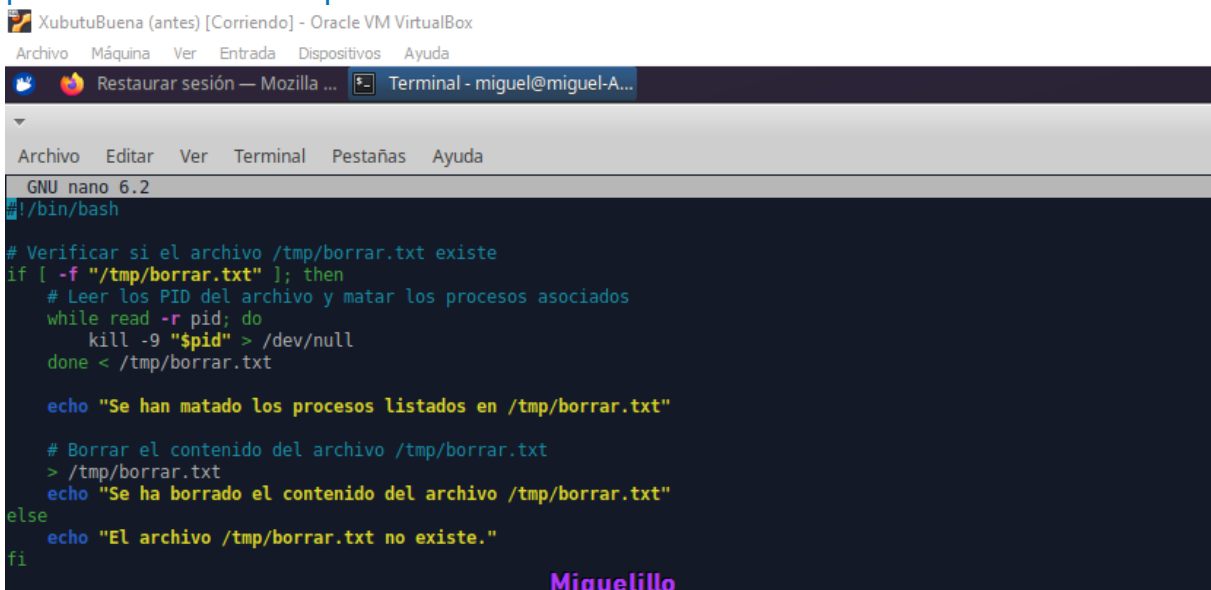
XubutuBuena (antes) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Problema al cargar la página... Configure Scheduled Tasks Terminal - miguel@miguel-A...

miguel@miguel-A50:~$ sudo nano /usr/local/bin/procesos.sh
miguel@miguel-A50:~$ /usr/local/bin/procesos.sh

Advertencia
El proceso python3 no está registrado. En caso de querer matar el proceso ejecute borrar.sh
Aceptar
Miguelillo

```

Para borrarlos manda los PID a un fichero temporal el cual podemos matar los procesos con este script



```

XubutuBuena (antes) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Restaurar sesión — Mozilla ... Terminal - miguel@miguel-A...

GNU nano 6.2 /usr/local/bin/borrar.sh
#!/bin/bash

# Verificar si el archivo /tmp/borrar.txt existe
if [ -f "/tmp/borrar.txt" ]; then
    # Leer los PID del archivo y matar los procesos asociados
    while read -r pid; do
        kill -9 "$pid" > /dev/null
    done < /tmp/borrar.txt

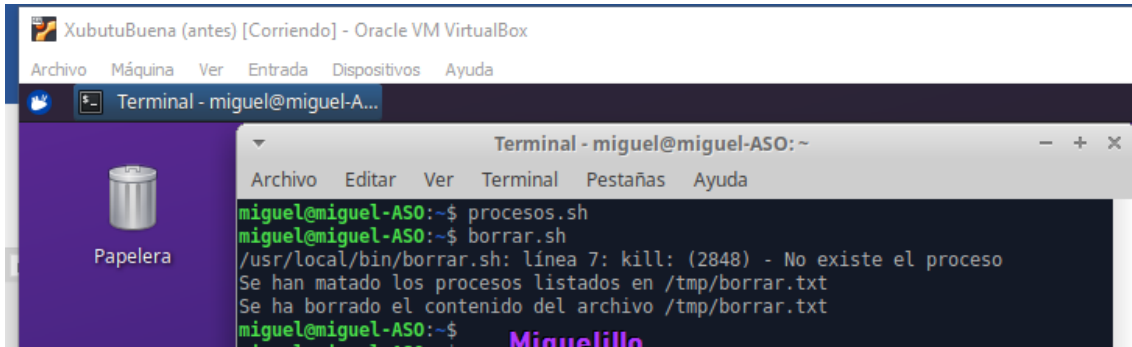
    echo "Se han matado los procesos listados en /tmp/borrar.txt"

    # Borrar el contenido del archivo /tmp/borrar.txt
    > /tmp/borrar.txt
    echo "Se ha borrado el contenido del archivo /tmp/borrar.txt"
else
    echo "El archivo /tmp/borrar.txt no existe."
fi
Miguelillo

```

UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

Lo probamos y los mata una vez ejecutado mata el proceso y borra los PID de los servicios del fichero



```
miguel@miguel-ASO:~$ procesos.sh
miguel@miguel-ASO:~$ borrar.sh
/usr/local/bin/borrar.sh: línea 7: kill: (2848) - No existe el proceso
Se han matado los procesos listados en /tmp/borrar.txt
Se ha borrado el contenido del archivo /tmp/borrar.txt
miguel@miguel-ASO:~$
```

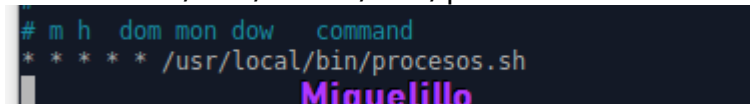
Para que la detección sea activa podemos añadirlo a un programador de tareas como crontab

Con

`crontab -e`

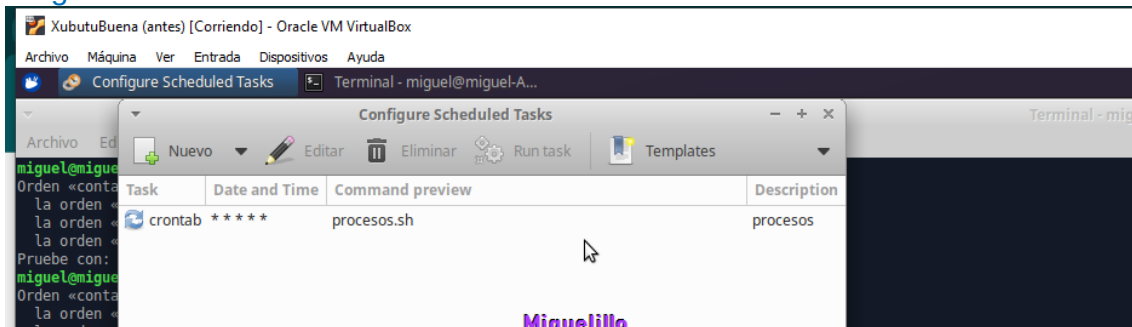
Ponemos el contenido

```
* * * * * /usr/local/bin/procesos.sh
```



```
# m h dom mon dow   command
* * * * * /usr/local/bin/procesos.sh
```

En mi caso voy a configurarlo en una aplicación de programador de tareas que tengo



Task	Date and Time	Command preview	Description
crontab	*****	procesos.sh	procesos

He tenido un problema y es que necesita ser ejecutado en una consola para poder lanzar el mensaje de notificación he probado con varias sentencias como `* * * * * export DISPLAY=:0 && xterm -e /usr/local/bin/procesos.sh` que lanza una ventana para ejecutarlo y luego se cierra