Creación práctica de reglas de Falco

Prerequisitos

- Ordenador Linux, Windows o Mac (Intel)
- Vagrant : https://www.vagrantup.com
- VirtualBox : https://www.virtualbox.org
- Git : https://git-scm.com

Repositorio con ficheros para practicar:
https://github.com/sysdiglabs/falco-workshop

```
$ git clone git@github.com:sysdiglabs/falco-workshop.git
```

QUANTIKA 14

Usando Vagrant

```
# Entrar en carpeta box2
cd box2

# Arrancar máquina virtual
vagrant up

# Login en máquina virtual
vagrant ssh

# Para ejecutar commandos con sudo, el password del usuario 'vagrant' es 'vagrant'

# Para usar el commando su y ser root
sudo su
```

```
# salir de la máquina virtual
exit

# Parar la máquina virtual
vagrant halt

# Borrar completamente la máquina virtual
vagrant destroy -f
```

Validar y recargar reglas

Probar reglas en directorio por defecto:

```
$ falco –L
```

Probar reglas en directorio por defecto(no mostrar lista complete después):

```
$ falco -L >/dev/null
```

Probar fichero individual de reglas (debe incluir todas sus listas y macros)

```
$ falco -V filename1.yaml -V filename2.yaml
```

Reiniciar servicio con Falco instalado en host

```
$ sudo /etc/init.d/falco restart
```