5.4 Packetbeats

El Beat que se verá en este tema será `Packetbeat` que hace las funciones de *sniffer* de paquetes de red, al igual que herramientas como `tcpdump` o `Wireshark` entre otras.

Instalación y configuración en Linux

El primer paso será descargar el servicio, instalarlo y configurarlo como servicio del sistema:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
sudo apt-get install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a
 /etc/apt/sources.list.d/elastic-6.x.list
sudo apt-get update && sudo apt-get install packetbeat
sudo update-rc.d packetbeat defaults 95 10
```

Una vez descargado, para configurarlo serán necesarias las mismas modificaciones que es han realizado en el servicio de Metricbeats modificando el archivo de configuración del servicio `/etc/packetbeat/packetbeat.yml`:

```
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.1.31:9200"]

setup.kibana:
  # Kibana Host
  host: "192.168.1.31:5601"
```

Para arrancar el servicio y monitorizar su ejecución se pueden utilizar los siguinetes comandos:

```
service packetbeat start
tail -f /var/log/packetbeat/packetbeat
```

Como ya se ha añadido en el archivo de configuración la ruta a Kibana, se puede realizar el importado automático de visualizaciones y dashboards a la misma. Para ello deberemos irnos al *home* de Packetbeat y ejecutar los siguientes comandos para la subida de los mismos:

```
cd /usr/share/packetbeat
mv kibana bin
./bin/packetbeat setup --dashboards -c /etc/packetbeat/packetbeat.yml
```