Ksniff as a Kubernetes-integrated packet sniffer
Troubleshooting containers in Kubernetes is a recurring topic.

The current traditional tools are not enough.

So, in those cases, how do we get to inspect this traffic? So this is the question that this work answers.
Ksniff as a Kubernetes-integrated packet sniffer

- Ksniff is shipped as a kubectl plugin that allows using tcpdump and Wireshark to capture traffic on a specific pod within a cluster.
- Ksniff uses kubectl to upload a tcpdump binary (packet sniffer) to the target container, and redirects the output to the Wireshark instance running in my machine.
- Well, Ksniff has specific flag (-p) for that. This approach can be also used to sniff traffic in distroless containers.
Installation process

1. Install Falco. Open Source run time security tool.
   - Parsing the Linux system calls from the kernel at runtime.
   - Asserting the stream against a powerful rules engine.
   - Alerting when a rule is violated.

2. Install Krew.
   - Krew is a tool that makes it easy to use kubectl plugins. Krew helps you discover plugins, install and manage them on your machine. It is similar to tools like apt, dnf or brew.

3. Installing sniff/Ksniff.
   - capture traffic on a specific pod within a cluster. Ksniff uses kubectl to upload a tcpdump binary (packet sniffer) to the target container, and redirects the output to the Wireshark instance running in your machine.

4. Installing libpcap-dev for tcpdump compilation (generate the binary file).

5. Install LOIC

6. Install Wireshark

Falco → Krew → Ksniff → LOIC → libpcap-dev → Wireshark
Installing Falco

update-alternatives: using /usr/bin/fakercut-sysv to provide /usr/bin/fakercut (fakercut) in auto mode

Setting up libgcc-7-dev:amd64 (7.5.0-3ubuntu1-18.04) ...
Setting up cpp-7 (7.5.0-3ubuntu1-18.04) ...
Setting up libstdc++-7-dev:amd64 (7.5.0-3ubuntu1-18.04) ...
Setting up libalgorithm-merge-perl (0.08-3) ...
Setting up libalgorithm-diff-xs-perl (0.04-5) ...
Setting up binutils-x86-64-linux-gnu (2.30-2ubuntu1-18.04.6) ...
Setting up cpp (4:7.4.0-1ubuntu2.3) ...
Setting up binutils (2.30-2ubuntu1-18.04.6) ...
Setting up gcc-7 (7.5.0-3ubuntu1-18.04) ...
Setting up g++-7 (7.5.0-3ubuntu1-18.04) ...
Setting up gcc (4:7.4.0-1ubuntu2.3) ...
Setting up dpkg-dev (1.19.0.5ubuntu2.3) ...
Setting up dkms (2.3-3ubuntu9.7) ...
Setting up g++ (4:7.4.0-1ubuntu2.3) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode

Setting up falco (0.29.1) ...
Loading new falco-17f5df52a7d9ed6bb12d3b176860d0def8439936d DKMS files...

Building for 4.15.0-156-generic
Building initial module for 4.15.0-156-generic
Can't load /var/lib/shim-signed/mok/.rnd into RNG
145628393900352: error:2406FF79:random number generator:RAND_load_file:Cannot open file:...crypto/rand
d/randfile.c:88:Filename=/var/lib/shim-signed/mok/.rnd
Generating a RSA private key
.........................................................+++5
..................................................................++++
writing new private key to '/var/lib/shim-signed/mok/MOK.priv'

-----
EFI variables are not supported on this system
/sys/firmware/efi/efivars not found, aborting.
Done.

falco:
Running module version sanity check.
  - Original module
  - No original module exists within this kernel
  - Installation
  - Installing to /lib/modules/4.15.0-156-generic/updates/dkms/
Setting up libalgorithm-diff-xs-perl (0.04-5) ...
Setting up binutils-x86-64-linux-gnu (2.30-21ubuntu1-18.04.5) ...
Setting up cpp (4.7.4.0-1ubuntu2.3) ...
Setting up binutils (2.30-21ubuntu1-18.04.5) ...
Setting up gcc-7 (7.5.0-3ubuntu1-18.04) ...
Setting up g++-7 (7.5.0-3ubuntu1-18.04) ...
Setting up gcc (4.7.4.0-1ubuntu2.3) ...
Setting up dpkg-dev (1.19.0.5ubuntu2.3) ...
Setting up dkms (2.3-3ubuntu9.7) ...
Setting up g++ (4.7.4.0-1ubuntu2.3) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up Falco (0.29.1) ...
Loading new falco-17f65df52a7d9ed6bb12d3b1768468def8439936d DKMS files...
Building for 4.15.0-156-generic
Building initial module for 4.15.0-156-generic
Can't load /var/lib/shim-signed/mok/.rdn into RND
Generating a RSA private key

.......................................................++++
.......................................................++++
writing new private key to '/var/lib/shim-signed/mok/MOK.priv'

---
EFI variables are not supported on this system
/sys/firmware/efi/efivars not found, aborting.
Done.

[Boxed text]

```
Falco:

Running module version sanity check.
  - Original module
    - No original module exists within this kernel
  - Installation
    - Installing to /lib/modules/4.15.0-156-generic/updates/dkms/
```

depmod...

DKMS: install completed.
Setting up build-essential (12.4ubuntu1) ...
Processing triggers for man-db (2.8.3-2ubuntu8.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.4) ...
ubuntu@hackfest-team-0:$
Installing Krew

```bash
$ git (Ubuntu Hackfest: microk8s-9)

set -x; cd "$(mktemp -d)" &&
OS="$(uname | tr '[[:upper:]]' '[[:lower:]]')" &&
ARCH="$(uname -m | sed -e 's/x86_64/amd64/' -e 's/\(arm\)/\1/2/' -e 's/aarch64$/arm64/')" &&
tar zxfv krew.tar.gz &&
KREWW="$(OS)_$ARCH" &&
"$KREWW" install krew

-bash: syntax error near unexpected token `newline'
++ mktemp -d
+ cd /tmp/tmp.u5SxmsL3YM
++ unset
++ tr '[[:upper:]]' '[[:lower:]]'
++ OS
++ unset -m
++ sed -e 's/x86_64/amd64/' -e 's/\(arm\)/\1/2/' -e 's/aarch64$/arm64/'
+ ARCH=amd64
+ tar zxfv krew.tar.gz
./LICENSE
./krew-darwin_amd64
./krew-darwin_arm64
./krew-linux_amd64
./krew-linux_arm
./krew-linux_arm64
./krew-windows_amd64.exe
+ KKEWW="./krew-linux_amd64

+ ./krew-linux_amd64 install krew

Adding "default" plugin index from https://github.com/kubernetes-sigs/krew-index.git.
Updated the local copy of plugin index.
Installing plugin: krew
Installed plugin: krew
```
Installing sniff

```
ubuntu@hackfest-microk8s-9:/tmp/tmp.u58xmsL3YMS$ kubectl krew install sniff
+ kubectl krew install sniff
Updated the local copy of plugin index.
Installing plugin: sniff
Installed plugin: sniff
```

Use this plugin:
- kubectl sniff

Documentation:
- https://github.com/eldadru/ksniff

Caveats:

This plugin needs the following programs:
- wireshark (optional, used for live capture)

**WARNING:** You installed plugin "sniff" from the krew-index plugin repository.
These plugins are not audited for security by the Krew maintainers. Run them at your own risk.

```
ubuntu@hackfest-microk8s-9:/tmp/tmp.u58xmsL3YMS$
```
Installing libpcap-dev for tcpdump compilation

```
$ sudo apt-get install libpcap-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-dev-bin libc6-dev libcrypt-dev libpcap0.8-dev linux-libc-dev manpages-dev
Suggested packages:
  glibc-doc
The following NEW packages will be installed:
  libc-dev-bin libc6-dev libcrypt-dev libpcap-dev libpcap0.8-dev linux-libc-dev manpages-dev
0 upgraded, 7 newly installed, 0 to remove and 10 not upgraded.
Need to get 6324 kB of archives.
After this operation, 31.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] 
```
Installing libpcap-dev For Tcpdump Compilation

Reading package lists... Done
Building dependency tree
Reading state information... Done

The following additional packages will be installed:
  libpcap-dev libpcap-dev libpcap-dev libpcap-dev libpcap-dev
  manpages-dev
Suggested packages:
  libpcap-doc

The following NEW packages will be installed:
  libpcap-dev libpcap-dev libpcap-dev libpcap-dev libpcap-dev
  manpages-dev
0 upgraded, 7 newly installed, 0 to remove and 10 not upgraded.
Need to get 6324 kB of archives.
After this operation, 31.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpcap-dev amd64 2.31-0ubuntu9.2 [71.8 kB]
Get:2 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 linux-libc-dev amd64 5.4.0-84.94 [1115 kB]
Get:3 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libpcap-dev amd64 1:4.4.10-1ubuntu4 [184 kB]
Get:4 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 linux-libc-dev amd64 2.31-0ubuntu9.2 [2028 kB]
Get:5 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libpcap-dev amd64 1.9.1-3 [244 kB]
Get:6 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 libpcap-dev amd64 1.9.1-3 [3484 kB]
Get:7 http://nova.clouds.archive.ubuntu.com/ubuntu/focal/main amd64 manpages-dev all 5.85-1 [2266 kB]
Fetched 6324 kB in 3s (2188 kB/s)
Selecting previously unsselected package libpcap-dev.
(Reading database ... 94565 files and directories currently installed.)
Preparing to unpack .../0-libpcap-dev_2.31-0ubuntu9.2_amd64.deb ...
Unpacking libpcap-dev (2.31-0ubuntu9.2) ...
Selecting previously unsselected package linux-libc-dev.
Preparing to unpack .../1-linux-libc-dev_5.4.0-84.94_amd64.deb ...
Unpacking linux-libc-dev:amd64 (5.4.0-84.94) ...
Selecting previously unsselected package libpcap-dev:amd64.
Preparing to unpack .../2-libpcap-dev_1:4.4.10-1ubuntu4_amd64.deb ...
Unpacking libpcap-dev:amd64 (1:4.4.10-1ubuntu4) ...
Selecting previously unsselected package libpcap-dev.
Preparing to unpack .../3-libpcap-dev_2.31-0ubuntu9.2_amd64.deb ...
Unpacking libpcap-dev:amd64 (2.31-0ubuntu9.2) ...
Selecting previously unsselected package libpcap8-dev:amd64.
Preparing to unpack .../4-libpcap8-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap8-dev:amd64 (1.9.1-3) ...
Selecting previously unsselected package libpcap-dev:amd64.
Preparing to unpack .../5-libpcap-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap-dev:amd64 (1.9.1-3) ...
Selecting previously unsselected package manpages-dev.
Preparing to unpack .../6-manpages-dev_5.85-1_all.deb ...
Unpacking manpages-dev (5.85-1) ...
Setting up manpages-dev (5.85-1) ...
Setting up linux-libc-dev:amd64 (5.4.0-84.94) ...
Setting up libpcap-dev:amd64 (1:4.4.10-1ubuntu4) ...
Setting up libpcap-dev:amd64 (2.31-0ubuntu9.2) ...
Setting up libpcap8-dev:amd64 (1.9.1-3) ...
Setting up libpcap-dev:amd64 (1.9.1-3) ...
Processing triggers for man-db (2.9.1-1) ...
The name of the pod to collect the TCPDUMP:
Pod/Kubernetes-bootcamp-57978f5f5d-vbzb4

Nodes deployed in the cluster

```bash
Last login: Fri Sep 17 02:19:56 2021 from 172.21.10.1
ubuntu@hackfest-microk8s-9:~$ microk8s kubectl get nodes
NAME           STATUS    ROLES       AGE       VERSION
hackfest-microk8s-9  Ready  <none>  6611h  v1.21.4-3+e5758f73ed2a04

ubuntu@hackfest-microk8s-9:~$ microk8s kubectl get deployments
NAME            READY UP-TO-DATE AVAILABLE AGE
kubernetes-bootcamp 1/1     1           1      71m
ubuntu@hackfest-microk8s-9:~$`
```
The LOIC

![Low Orbit Ion Cannon](image-url)
The Wireshark analysis