Using eBPF in Kubernetes

[GitHub repo 1](#_Toc515587229)

[Lab-1 1](#_Toc676677603)

[Takeaways 1](#_Toc847064552)

[Lab-2 1](#_Toc206132902)

[Takeaways 1](#_Toc589912148)

[Lab-3 2](#_Toc1232990200)

[Lab-4 2](#_Toc1960776531)

[Takeaways 2](#_Toc654229554)

[Lab-5 2](#_Toc152439171)

[Takeaways 2](#_Toc1036435320)

[Lab-6 3](#_Toc629265373)

[Takeaways 3](#_Toc1231217020)

[Lab-7 3](#_Toc49209535)

[Lab-8 3](#_Toc1693774853)

[Takeaways 3](#_Toc802810477)

[Lab-9 4](#_Toc702176097)

[Takeaways 4](#_Toc1189147895)

[References 4](#_Toc1062222604)

# GitHub repo

<https://github.com/NamrathaPrabhanjana/eBPF-kubernetes-training/tree/workhorse>

# Lab-1

1. Setup microk8s cluster and docker env as detailed in the README/steps.txt
2. Use the Dockerfile in the root folder and build a base container for all further labs.

## Takeaways

1. Python BCC repo
2. Bpftools
3. Linux-headers required for eBPF builds

# Lab-2

1. Follow the instructions in the README of helloworld folder
2. Trace the bpf() syscall using: strace -e bpf ./hello-buffer-config.py
3. Microk8s kubectl ctr info

## Takeaways

1. Introduction to BCC
2. Structure of a BCC program
3. Life of a BCC program
4. eBPF Data structures

Refer: <https://github.com/iovisor/bcc/blob/master/docs/reference_guide.md>

# Lab-3

Setup additional pods using the instructions in additional-pods/ folder.

# 

# Lab-4

Follow README in icmp-blocker-xdp folder

## 

## Takeaways

1. Understand XDP

# Lab-5

Follow README in ddos-attack-detector folder

## Takeaways

Explore more bpf hooks

# Lab-6

Follow README in flow-tracing folder

## Takeaways

1. Explore more bpf hooks
2. Understand how ebpf programs can be correlated with Kubernetes pod info

# Lab-7

Run any of the ebpf containers that you built in the class and explore BCC tools like: runqlat, sslsniff, cpudist etc.

# Lab-8

Follow README in cilium-setup folder

## Takeaways

1. Intro to cilium and cilium command line

# Lab-9

1. Write a CIlium network policy to limit traffic to a certain pod
2. Follow README in cilium-setup folder

## Takeaways

1. Understand CNP and associated command line.
2. Compare against native kubernetes constructs.

# References

<https://github.com/iovisor/bcc/blob/master/docs/reference_guide.md>

<https://github.com/iovisor/bcc/blob/master/docs/tutorial.md>

<https://github.com/iovisor/bcc/blob/master/docs/tutorial_bcc_python_developer.md>

<https://github.com/iovisor/bcc/blob/master/docs/kernel_config.md>