Docker

"*Docker is a set of platform as a service (PaaS) products that use OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels. All containers are run by a single operating system kernel and therefore use fewer resources than virtual machines.*"

Installation:

1. https://docs.docker.com/engine/install/ubuntu/
2. https://docs.docker.com/docker-for-mac/install/
3. https://docs.docker.com/docker-for-windows/install/

References:

1. https://www.docker.com/
2. https://hub.docker.com/

Youtube tutorials:

1. Learning Docker

Kubernetes

"*Kubernetes (commonly stylized as k8s) is an open-source container-orchestration system for automating computer application deployment, scaling, and management.*"

"***Pods** are the smallest deployable units of computing that you can create and manage in Kubernetes. A Pod (as in a pod of whales or pea pod) is a group of **one or more containers**, with shared storage and network resources, and a specification for how to run the containers*"

Online playgrounds:

1. https://labs.play-with-k8s.com/
2. https://www.katacoda.com/courses/kubernetes/playground
3. https://training.play-with-kubernetes.com/kubernetes-workshop/

Installation tools:

1. Kubectl (*allows you to run commands against Kubernetes clusters*)
2. Kubeadm *(performs the actions necessary to get a minimum viable, secure cluster up and running in a user friendly way)*
3. Minikube (*sets up a local Kubernetes cluster on macOS, Linux, and Windows*)

Minikube info:

- Start a cluster using the docker driver: *minikube start --driver=docker*
- To make docker the default driver: *minikube config set driver docker*

References:

1. https://kubernetes.io/
2. https://codeburst.io/getting-started-with-kubernetes-deploy-a-docker-container-with-kubernetes-in-5-minutes-eb4be0e96370
3. Pods
4. Communicate Between Containers in the Same Pod Using a Shared Volume
5. https://medium.com/google-cloud/kubernetes-nodeport-vs-loadbalancer-vs-ingress-when-should-i-use-what-922f010849e0
6. https://computingforgeeks.com/deploy-ubuntu-pod-in-kubernetes-openshift/

Youtube tutorials:

1. Kubernetes Beginner Tutorial

Tcpdump

“tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached”

Simple example:

tcpdump -n -i eth0 -s 0 -w test.pcap

Will monitor eth0, capture the entire packet (-s 0) and save the captured packets to test.pcap. -n instructs tcpdump to not resolve addresses to domains.

References:

1. https://www.tcpdump.org/

BPF

The **Berkeley Packet Filter** (**BPF**) is a technology used in certain computer operating systems for programs that need to, among other things, analyze network traffic. It provides a raw interface to data link layers, permitting raw link-layer packets to be sent and received.

Tcpdump uses BPF syntax for packet filtering

References:

1. https://biot.com/capstats/bpf.html

Wireshark

“Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.”

Install on ubuntu:

1. sudo apt-get update
2. sudo apt-get install wireshark
3. sudo wireshark

Filters:

1. icmp (catches only pings)

References:

1. https://www.wireshark.org/

OpenFlow

“OpenFlow is a programmable network protocol designed to manage and direct traffic among routers and switches from various vendors. It separates the programming of routers and switches from underlying hardware.”

Installation:

1. Mininet *(Mininet creates a realistic virtual network, running real kernel, switch and application code, on a single machine) --- best option through vm*

Tutorial:

1. Mininet tutorial
2. Create a learning switch

Snort

“Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS)”

Installation:

- Ubuntu: *sudo apt-get install snort*

References:

1. https://www.snort.org/
2. https://linuxhint.com/snort-ubuntu-tutorial/