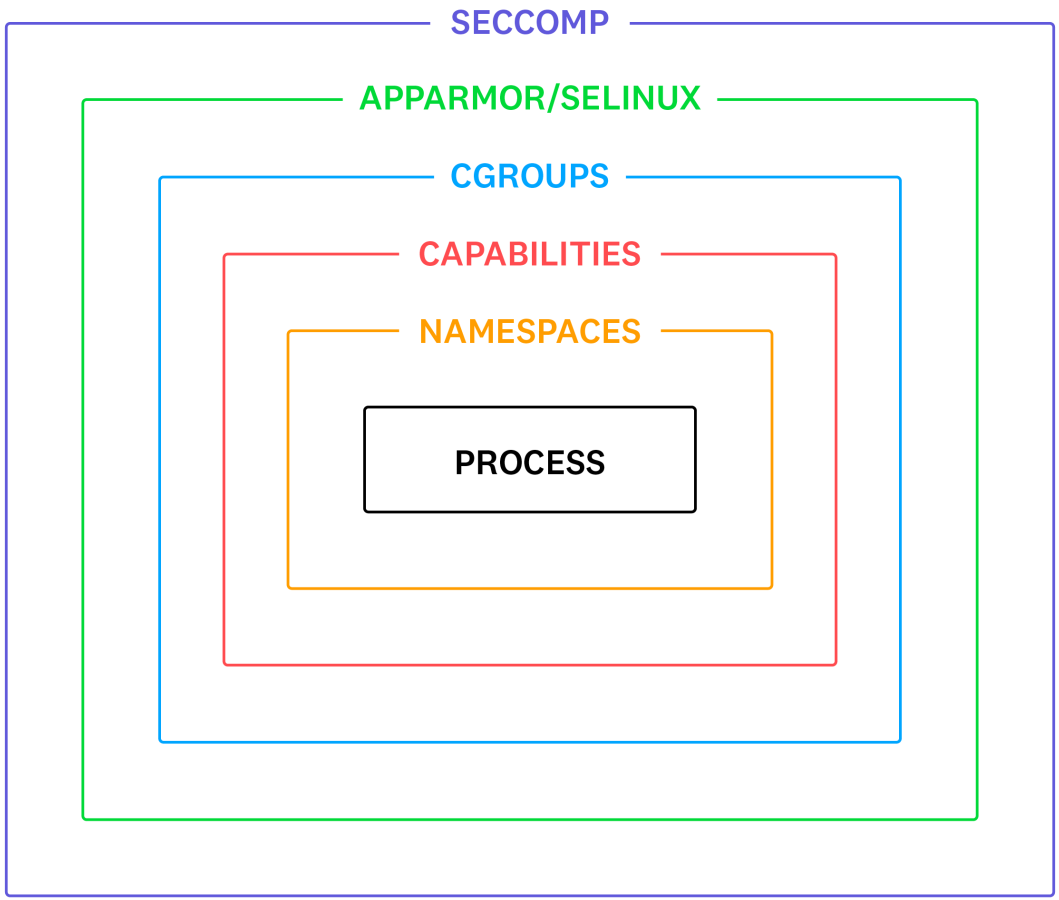
CONTAINERS FOR PENTESTERS

ABOUT ME

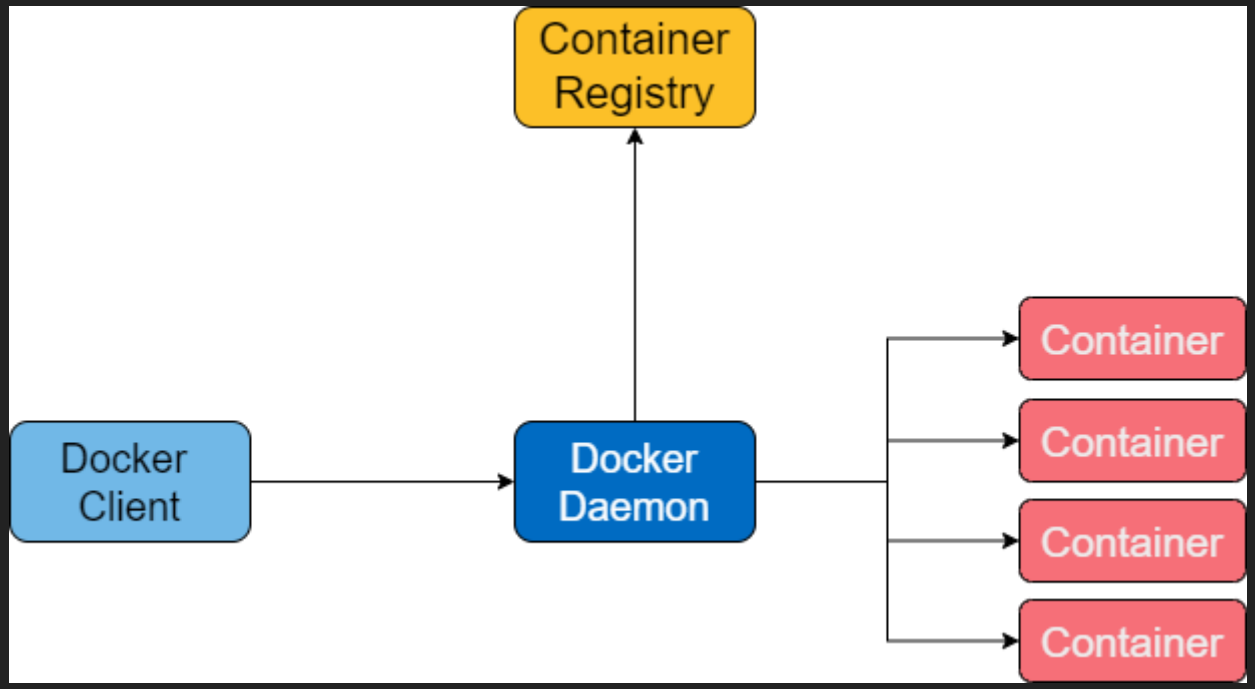
- Ex-Pentester/IT Security person
- Senior Security Advocate at Datadog
- CIS Benchmark author, Docker and Kubernetes
- Member of Kubernetes SIG-Security & CNCF TAG-Security

WHAT'S A CONTAINER THEN?



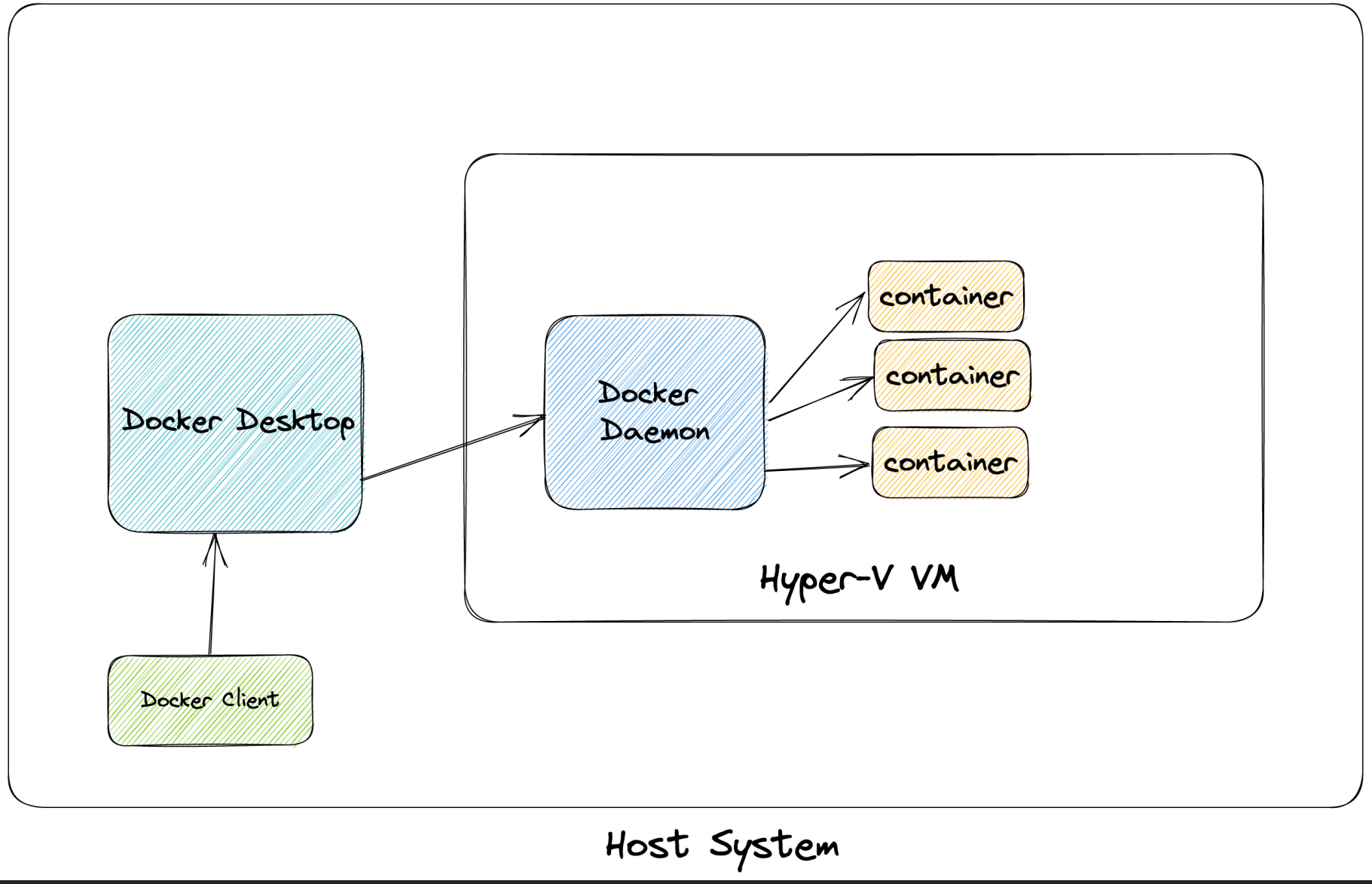
DEMO

WHAT DOES DOCKER DO?



DEMO

DOCKER DESKTOP


Docker Desktop
Docker Daemon
container
container
container
Hyper-V VM
Docker Client
Host System

AN IMPORTANT ASIDE : DOCKER SECURITY MODEL

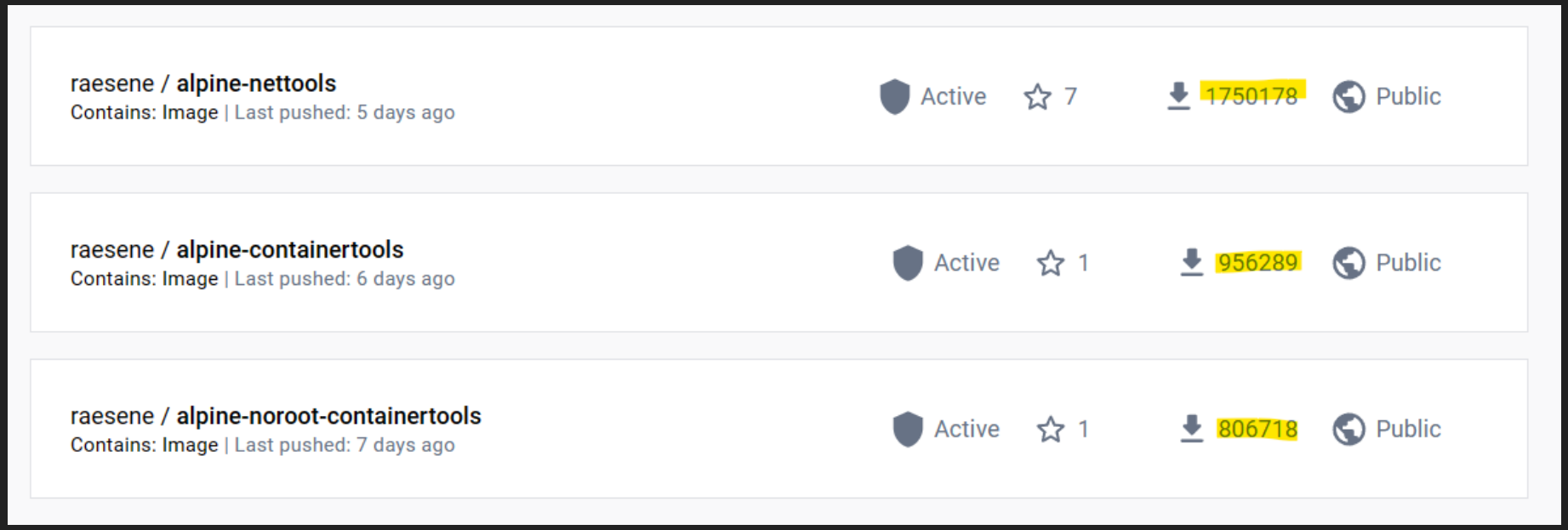
```
docker run -ti
    --privileged
    --net=host --pid=host --ipc=host
    --volume /:/host
    busybox
    chroot /host
```

DEMO

WHY DO WE NEED THESE THINGS AS PENTESTERS?

VM VS CONTAINER

DOCKER HUB


raesene / alpine-nettools
Contains: Image | Last pushed: 5 days ago
Active
7
1750178
Public
raesene / alpine-containertools
Contains: Image | Last pushed: 6 days ago
Active
1
956289
Public
raesene / alpine-noroot-containertools
Contains: Image | Last pushed: 7 days ago
Active
1
806718
Public

MAKE YOUR OWN IMAGES

TOOL SPECIFIC
VS
KITCHEN SINK

CHOOSING A BASE DISTRO

- Scratch
- Alpine
- Debian/Ubuntu
- Red Hat
- Not CentOS*

DOCKERFILE BASICS - SINGLE COMMAND IMAGE

```
1 FROM ubuntu:22.04
2
3 RUN apt update && apt install -y nmap && apt-get clean
4
5 ENTRYPOINT ["nmap"]
```

DEMO - USING THE BASIC IMAGE

```
1 docker build -t nmap -f Dockerfile.nmap .
```

```
1 docker run --net=host nmap  -v -n -sT 127.0.0.1
```

ROOT VS NON-ROOT

TRICK - GETTING ROOT BACK IN NON-ROOT ENVS

```
FROM ubuntu:22.04
RUN cp /bin/bash /bin/setuidbash && chmod 4755 /bin/setuidbash
RUN adduser tester
USER tester
CMD ["/bin/bash"]
```

GETTING DATA IN AND OUT OF CONTAINERS

```
1 docker run -it -v ~/testdata:/testdata [image] /bin/bash
```

CONCLUSION

- Containers are quite easy to use once you understand what they do.
- Very helpful for keeping tool envs clean
- Very helpful for jobs that use Kubernetes

RESOURCES AND LINKS

- https://github.com/raesene/alpine-containertools - Example kitchen sink image!
- https://github.com/raesene/dockerized-security-tools - Example Tool specific images (old)
- https://securitylabs.datadoghq.com - Blog series on container security fundamentals
- https://container-security.site - General container security resources
- https://talks.container-security.site - Archive of Container/Cloud Native security talks

THANKS

- E-Mail: rory.mccune@datadoghq.com
- Mastodon: @raesene@infosec.exchange
- Twitter: @raesene