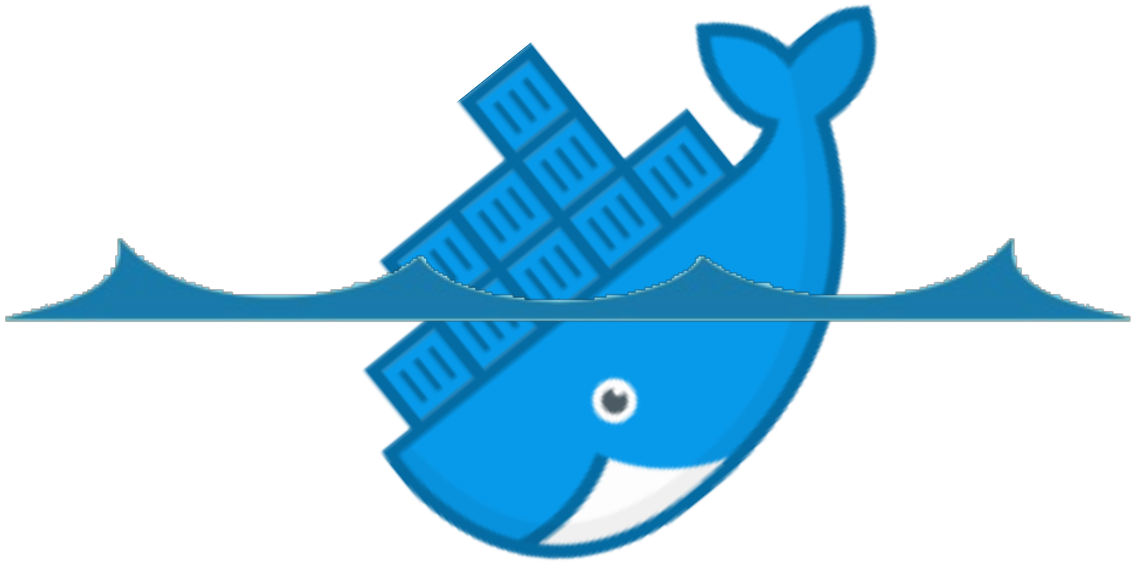
NOT SO SECURE



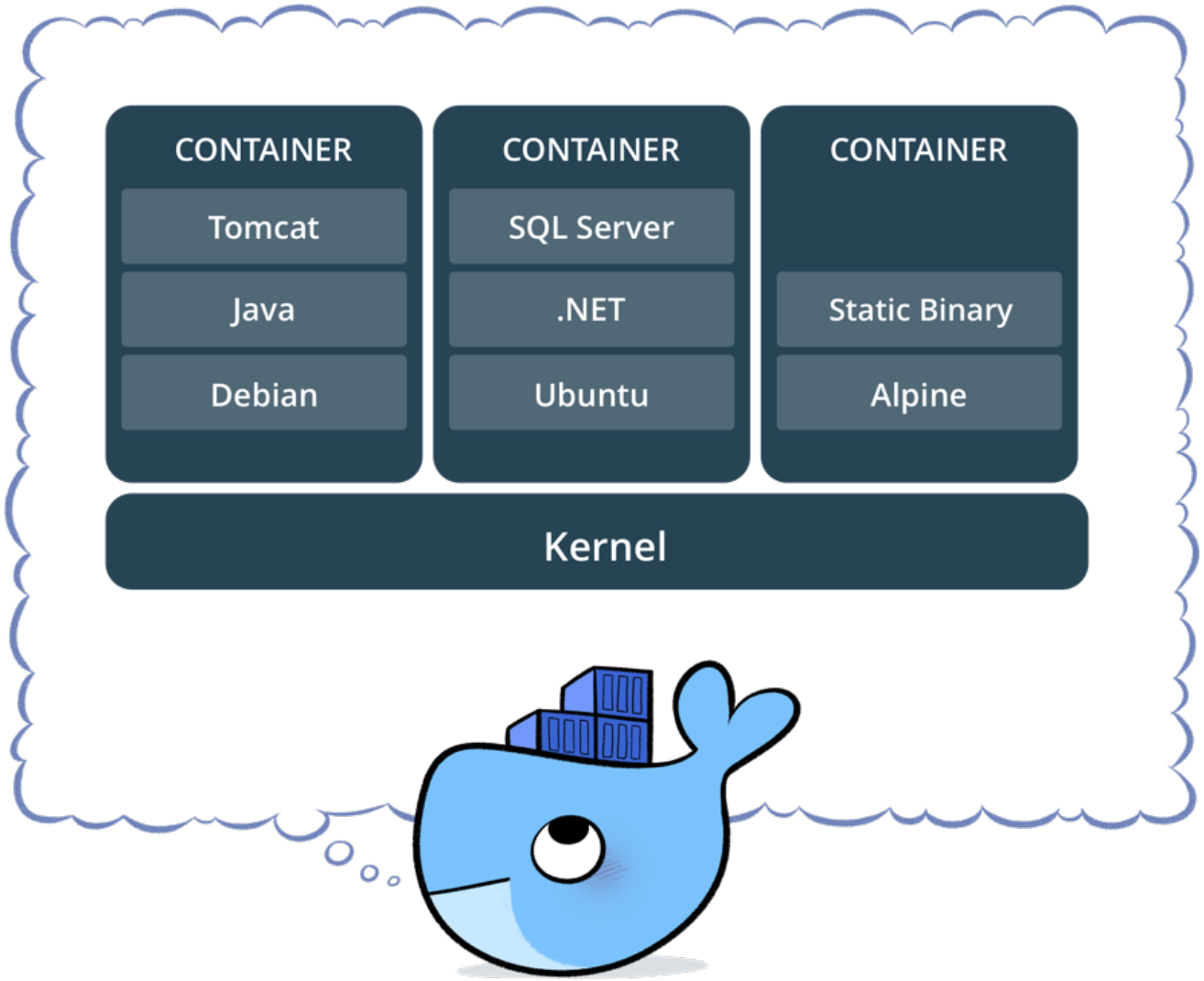
Down by the Docker

About Presenter

Anant Shrivastava (@anantshri)

- Regional Director - NotSoSecure Global Services Limited
- 9 yrs of corporate experience
- Expertise in Network, Mobile, Application and Linux Security
- Speaker / Trainer : BlackHat, Nullcon, RootConf, c0c0n
- Co-author for OWASP Testing guide version 4
- Project Lead : Code Vigilant, Android Tamer

Docker Overview



Why Docker

- Allows to get rid of “It works on my System” syndrome
- Easy & Quick to setup environments and test beds
- Loved by start-up's and for PoC Development teams
- Loved by Google and likes for scalability and deployment ease
- Secure: as secure as you configure it.

How does it differs for pentesters

- From outside it will all be the same
- `/proc/1/cgroup` will show docker references
- pid 1 != init / launchd

```
/ #
/ # ps
PID   USER     TIME   COMMAND
    1 root       0:00 sh
   26 root       0:00 ps
/ #
```

```
/ # cat /proc/1/cgroup
14:name=systemd:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277
13:pids:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
12:hugetlb:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8
11:net_prio:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f
10:perf_event:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e833027735
9:net_cls:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e
8:freezer:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e
7:devices:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e
6:memory:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e0
5:blkio:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
4:cpuacct:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e
3:cpu:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08f7
2:cpuset:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e0
1:name=openrc:/docker
/ #
```

How does it differs for pentesters

- Bash / Python / Perl isn't usually available
- Containers are disposable hence no Persistence ensured
- Containers can have different resources shared
- Container crash === new spawn anywhere
- Docker Internal Network (172.17.0.0/16)
  - https://docs.docker.com/engine/userguide/networking/

- Video: **https://vimeo.com/219495998**

Docker goof up: Running container process as root

- By default host UID == container UID
- Root in container == root on base box.
- If a file system or part of it is shared, you have direct path to write privileges files and get root
- `docker run -itv /:/host alpine /bin/sh`

DEMO

Docker goof up: Exposing docker sock / tcp

- Docker socket == access to docker daemon
- Docker could listen on port 2375 (noauth) 2376 (tls)
- Generally: Dashboard or reporting application containers
- Misconfiguration, (un)intended exposure == host compromise

DEMO

Docker goof up: Unpatched host / guest

- Docker shares kernel with the host
- Kernel bugs will result in host compromise
- Unpatched guest will result in guest compromise
- Video: **https://vimeo.com/218622598**

DEMO

Security is by secure configuration

- Docker security relies on secure configuration at all levels
  - Scrutinize “docker” group
  - Docker Socket : only available to root and docker group users
  - Docker daemon: only available to root and docker group users
  - Docker containers: run processes via limited users
  - Docker host + Guest: Keep then up-to-date

- Scan Docker configuration files

Docker configuration Review

- Docker Security Scanning via DockerHub
- Clair : https://github.com/coreos/clair
- Atomic Scan: https://developers.redhat.com/blog/2016/05/02/introducing-atomic-scan-container-vulnerability-detection/
- https://anchore.com/
- Dockerscan : https://github.com/cr0hn/dockerscan
- Dockscan: https://github.com/kost/dockscan

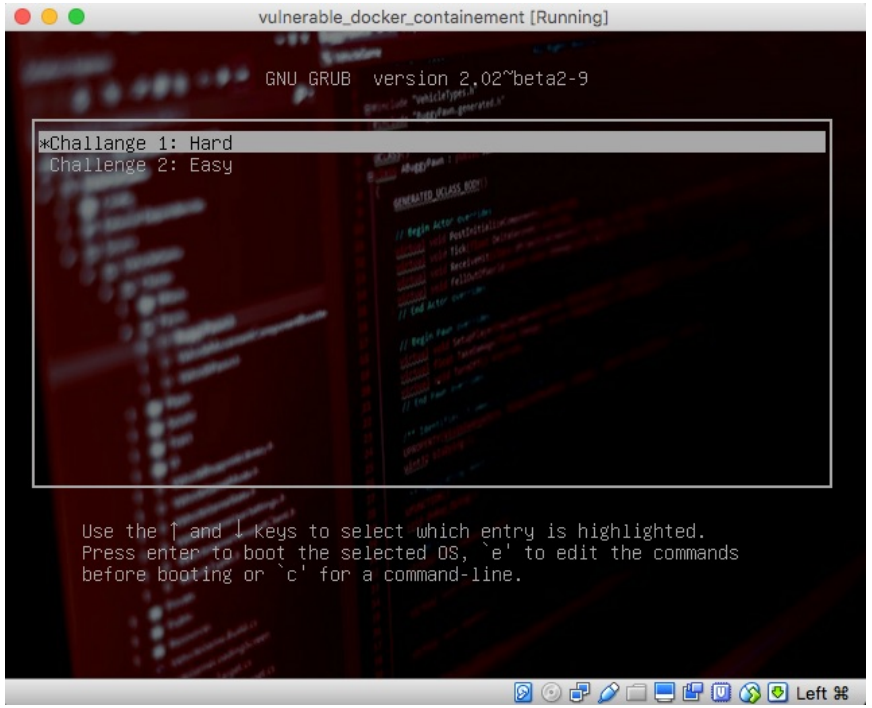
- Nessus: https://www.tenable.com/blog/auditing-docker-with-nessus-66

Docker VM

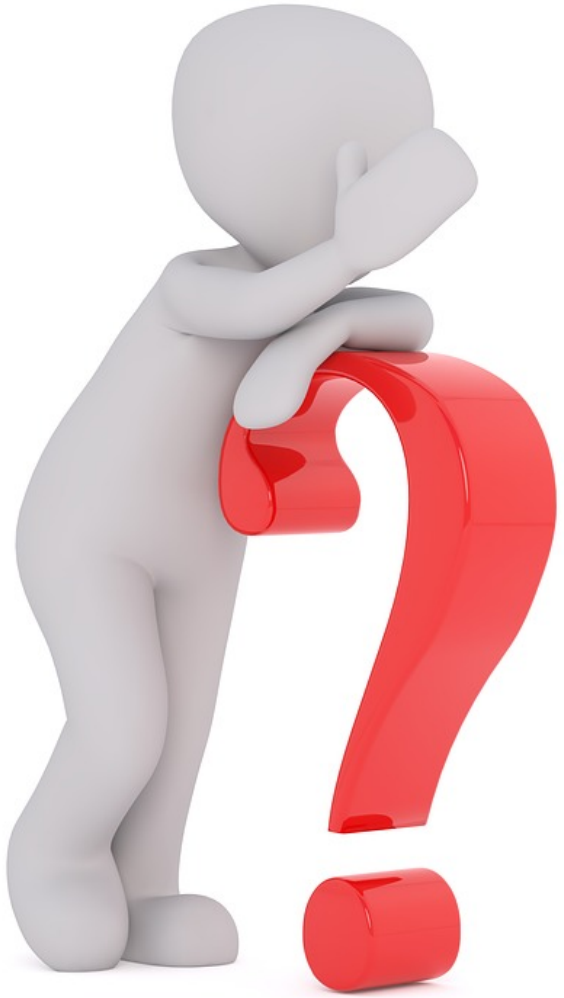
- We have created a vulnerable docker VM that suffers from many of the vulnerabilities discussed throughout this session.

This is available to download from the following URL:

https://www.notsosecure.com/vulnerable-docker-vm/



Questions?



END PRESENTATION