DOCKER

SECURITY MYTHS - SECURITY LEGENDS

ABOUT ME

- 'X' Years in IT/Information Security
- 'X' - 5 Years in Security Testing
- Managing Consultant at NCC Group PLC

TOPICS

- Docker Introduction
- Container Security
- Attackers/Defenders View of Docker

DOCKER BACKGROUND

- Started in 2013
- Very Active Codebase (~25,000 commits)
- Lots of Interest from Big Tech Co's (e.g. IBM/Microsoft/Redhat)
- Involved in containerization software

WHAT IS CONTAINERIZATION?

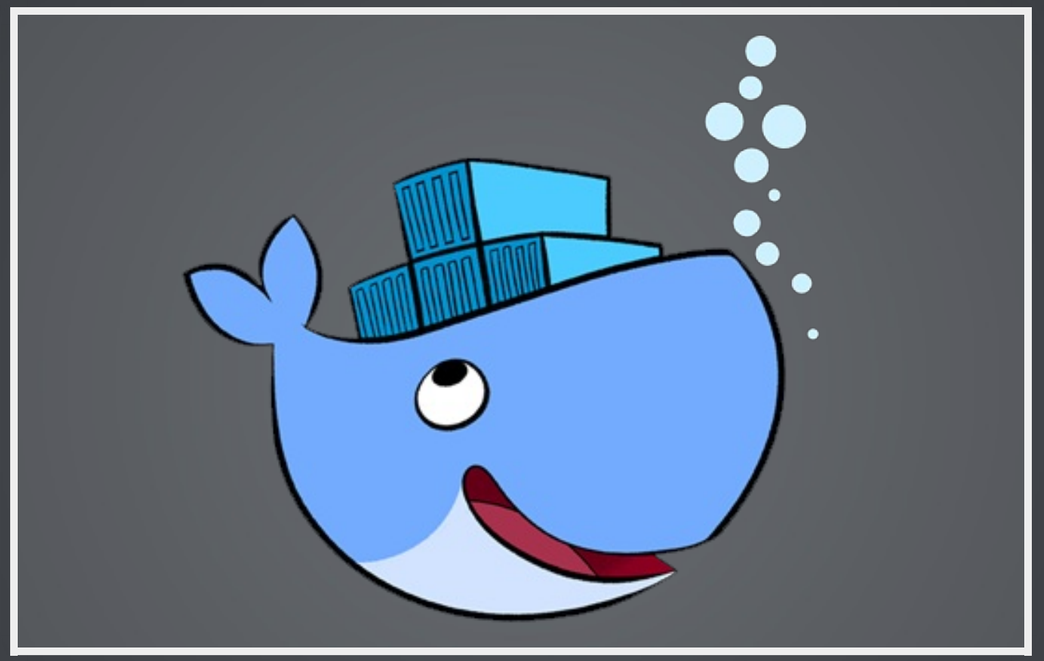
CONTAINERIZATION TECHNOLOGIES

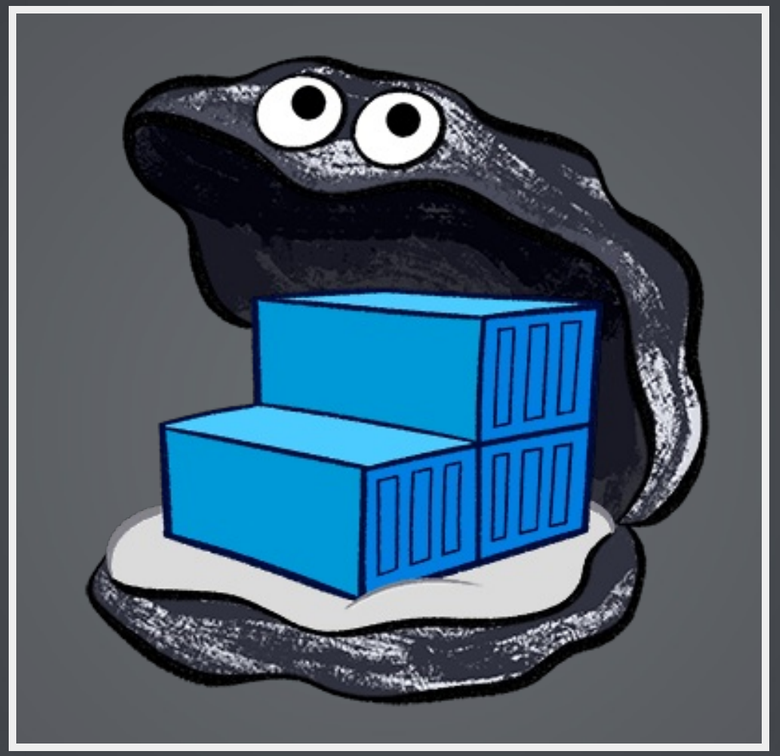
- chroot
- OpenVZ
- FreeBSD Jails
- Solaris Zones
- LXC

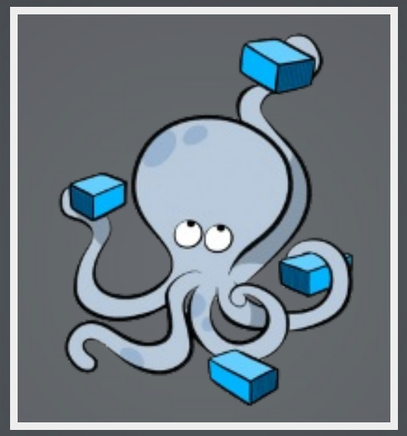
BENEFITS OF DOCKER

- Portability
- Speed
- Size

DEMO 1







USEFUL USES FOR DOCKER

SCRIPT ISOLATION DEMO

PENTEST ENVIRONMENT AUTOMATION DEMO

CONTAINERS DON'T CONTAIN?

CONTAINER SECURITY == LINUX SECURITY

NAMESPACES

MOUNT(CHROOT)

PROCESS

NETWORK

IPC

UTS

USER(!!)

CAPABILITIES

- Break up the monolithic 'root' Privilege
- Useful for commands that need one privilege
- Some need careful handling (e.g. CAP_SYS_ADMIN)

CGROUPS

- Resource Limits
- Restrict Access to Devices

SECCOMP

MANDATORY ACCESS CONTROL

- AppArmor
- SELinux

CONTAINERS VS VMS??

DEFENDERS VIEW

DOCKER ENGINE SECURITY

AUTHENTICATION & AUTHORIZATION

INTER CONTAINER COMMUNICATIONS (--ICC)

THE PERILS OF --PRIVILEGED

MOUNTING DOCKER.SOCK

DOCKER HUB

IMAGE PROVENANCE

IMAGE HARDENING

THINGS TO LOOK FOR

- Redundant images/containers
- Secrets Management
- Container History

TOOLS

- Docker Bench
- CIS Guide

ATTACKERS VIEW

AM I IN A CONTAINER?

- Process List
- Available Programs
- Read-only files as root

BREAKING OUT OF A CONTAINER

- Kernel Vulnerabilities
- Mounted Filesystems
- docker.sock access
- Container network access

CONCLUSION

- Lightweight application isolation.
- Security Model isn't perfect but improving.
- Lots of potential.

FURTHER READING

- Abusing Privileged and Unprivileged Linux Containers (https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/june/abusing-privileged-and-unprivileged-linux-containers/)
- Understanding and Hardening Linux Containers (https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2016/april/understanding-and-hardening-linux-containers/)

QUESTIONS?

- e-mail - rory.mccune@nccgroup.trust
- twitter - @raesene