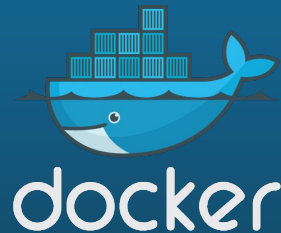


User Namespaces and Seccomp

24 August 2016

Paul Novarese
Technical Account Manager
Docker, Inc.
pvn@docker.com
@pvn



Agenda

- Preliminaries
- Container Security Considerations
- Containment
- Namespaces
- The User Namespace
- What is Seccomp?
- Demos

"CONTAINER"



"SECURITY"

memegenerator.net

Namespaces



cgroups



seccomp



Containment

- namespaces -> what you can see
- cgroups -> what you can use
- seccomp -> what you can do



STOP TALKING



DEMO TIME

memegenerator.net

GET EXCITED



IT'S DEMO TIME

memegenerator.net

TIME FOR A LIVE

DEMO



COULD GO WRONG?

memegenerator.net

Further Reading, References, etc

- The definitive presentation on userns support:
https://events.linuxfoundation.org/sites/events/files/slides/User%20Namespaces%20-%20ContainerCon%202015%20-%202016-9-final_0.pdf
- Default seccomp profile:
<https://github.com/docker/docker/blob/master/profiles/seccomp/default.json>
- Run without seccomp (don't ever do this): `--security-opt seccomp=unconfined`
- Security non-events:
<https://docs.docker.com/engine/security/non-events/>



docker