Keeping your containers secure

David Becvarik
@dbecvarik
david@becvarik.cz

Its in a container, why should I care?

- Containers are good for running scripts from internet
- Containers are like lightweight VMS
- Containers are immutable

Its in a container, why should I care?

- Containers are good for running scripts from internet
- Containers are like lightweight Virtual Machines
  - /dev/mem
  - cgroups
  - selinux
  - /dev/sd*
  - a lot of others not namespaced
- Containers are immutable
  - your app usually is not
- Docker hub images are verified
  - not public ones


Demo:
What can possibly go wrong?


In Atomic we trust!

```
se rhel7

oscap" in path "/usr/bin/oscap".
oscap-ssh" in path "/usr/bin/oscap-ssh".
oscap-vm" in path "/usr/bin/oscap-vm".
oscap-docker" in path "/usr/bin/oscap-docker".
oscap-chroot" in path "/usr/bin/oscap-chroot".
t the 'docker' package. Container scanning functionality will be disabled.
CAP content at "/usr/share/openscap/cpe/openscap-cpe-oval.xml".
CAP content in path "/usr/share/xml/scap/ssg/content".
directory at '/var/lib/oscapd/tasks' because it didn't exist.
ts directory at '/var/lib/oscapd/results' because it didn't exist.
ts work in progress directory at '/var/lib/oscapd/work_in_progress' because it didn
uationSpec, exit_code=0.
rsion of /var/lib/oscapd/cve_feeds/com.redhat.rhsa-RHEL7.xml but it wasn't new enou
uationSpec, exit_code=0.
ned target 'chroot:///scanin/db7a70a0414e589d7c8c162712b329d4fc670fa47ddde721250fb9

589)

an

th this scan are in /var/lib/atomic/openscap/2017-10-29-18-18-19-457033.
```

Why atomic scan?

- easy to use
  - battery included on rhel ecosystem
  - can scan images and containers
- integrate openscap easily
  - lot of predefined scans
  - cves, configuration complience
  - nice reporting
- easy to extend
  - https://github.com/CentOS/container-pipeline-service/tree/master/atomic_scanners
  - Python - ops friendly

Why atomic

- nice tool for managing containers and images
- supports a lot of operations like:
  - mount
  - signing
  - managing registries trust

Securing your infrastructure

Keep your containers secure

- Scan images and containers often
- Scan not only for CVE but for configuration violations too
- Append that info to registry, so anyone can see
- Protect and plan your CI well
  - It's crucial for your safety
- Treat root in containers same as root at host
- Run your containers read only
  - make this default for new apps
  - limit amount of volumes used

Keep audit trail about your custom images

- Where it was build
- Where is the repo and commit
- How to rebuild it
- What image was used as a base
  - no :latest is not enough too
  - no :1.0 is not enough too
  - use sha256 tag
- Archive all artifacts used
- you should be able to rebuild exact image
  - think about yum, apt and others

Keep your hosts secure

- Keep your containers hosts minimalistic
- No shell access for users
- Be aware of user namespaces
- SELINUX is crucial
- Treat your volumes carefully
  - at least mount them with nosuid
  - noexec is much better
- Keep your host and containers updated
- Monitor CVE of all your components