Keeping your Kubernetes Secured with microscanner, kube-bench and kube-hunter

Agenda

- Kubernetes security configuration assessment (CIS benchmark)
- Kubernetes penetration testing – testing for vulnerabilities
- Micro-Scanner – scanning your images at build time

Github reference

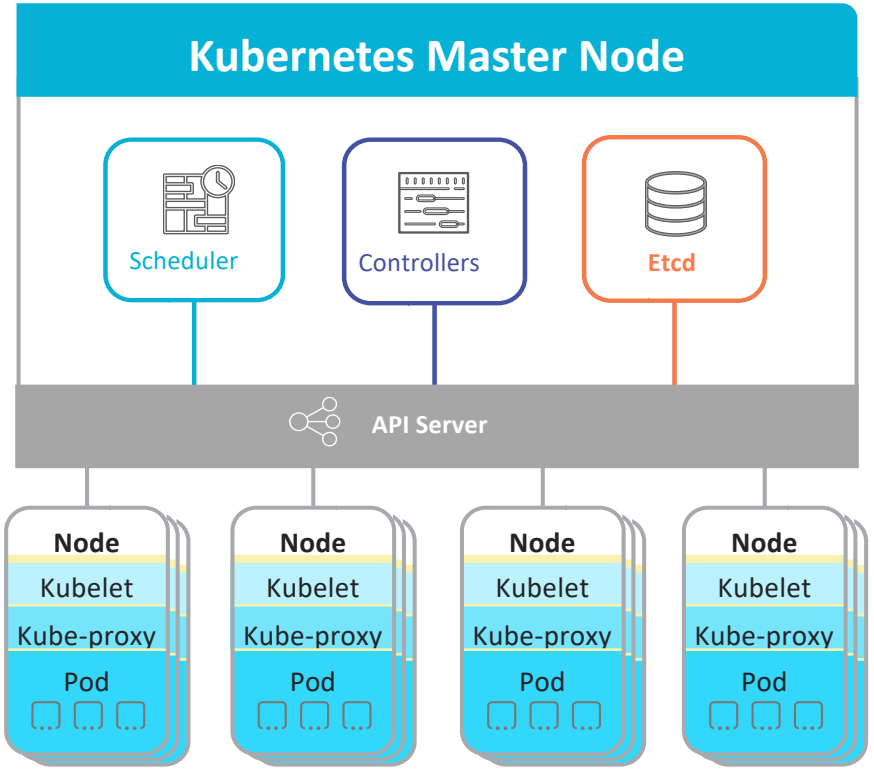
- References to the projects that will be shown in this workshop is available here:

  https://github.com/jerbia/kube-security/

Kubernetes Configuration Assessment for Security

Kubernetes components

- Kubernetes components installed on your servers
  - Master & node components
- Many configuration settings have a security impact
  - Example: open Kubelet port = root access
- Defaults depend on the installer



CIS Kubernetes benchmark

kube-bench

- Open source automated tests for CIS Kubernetes Benchmark
- Tests for Kubernetes Masters and Nodes
- Available as a container

`github.com/aquasecurity/kube-bench`

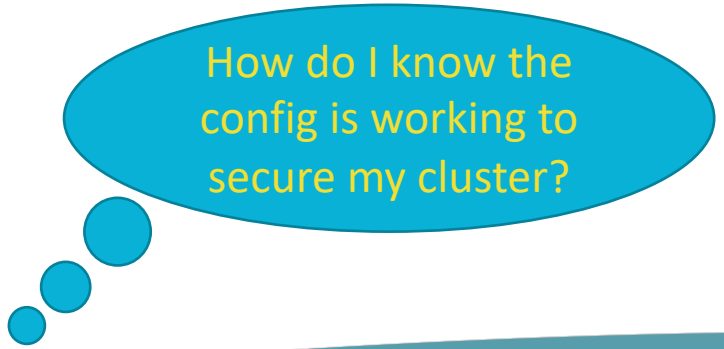
kube-bench

```
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[FAIL] 1.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 1.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 1.1.3 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.4 Ensure that the --insecure-allow-any-token argument is not set (Scored)
[FAIL] 1.1.5 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.6 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.7 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.8 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.9 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.10 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.11 Ensure that the admission control policy is not set to AlwaysAdmit (Scored)
[FAIL] 1.1.12 Ensure that the admission control policy is set to AlwaysPullImages (Scored)
[FAIL] 1.1.13 Ensure that the admission control policy is set to DenyEscalatingExec (Scored)
[FAIL] 1.1.14 Ensure that the admission control policy is set to SecurityContextDeny (Scored)
[PASS] 1.1.15 Ensure that the admission control policy is set to NamespaceLifecycle (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-path argument is set as appropriate (Scored)
[FAIL] 1.1.17 Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Scored)
[FAIL] 1.1.18 Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Scored)
[FAIL] 1.1.19 Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Scored)
[PASS] 1.1.20 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 1.1.21 Ensure that the --token-auth-file parameter is not set (Scored)
[FAIL] 1.1.22 Ensure that the --kubelet-certificate-authority argument is set as appropriate (Scored)
```

Kubernetes penetration testing

kube-hunter

- Open source penetration tests for Kubernetes
  - See what an attacker would see
  - `github.com/aquasecurity/kube-hunter`
- Online report viewer
  - `kube-hunter.aquasec.com`



kube-hunter.aquasec.com

```
Choose one of the options below:
1. Remote scanning      (scans one or more specific IPs or DNS names)
2. Subnet scanning      (scans subnets on all local network interfaces)
3. IP range scanning    (scans a given IP range)
Your choice: 1
Remotes (separated by a ','): 172.28.128.3
~ Started
~ Discovering Open Kubernetes Services...
|
| API Server:
|   type: open service
|   service: API Server
|_  host: 172.28.128.3:6443
|
| Kubelet API (readonly):
|   type: open service
|   service: Kubelet API (readonly)
|_  host: 172.28.128.3:10255
|
| Kubelet API:
|   type: open service
|   service: Kubelet API
|_  host: 172.28.128.3:10250
|
| Anonymous Authentication:
|   type: vulnerability
```

172.28.128.3

Node / Master

12 vulnerabilities

SEVERITY	CATEGORY	VULNERABILITY	DESCRIPTION	EVIDENCE
High	Remote Code Execution	Exposed Attaching To Container	Opens a websocket that could enable an attacker to attach to a running container	
High	Remote Code Execution	Anonymous Authentication	The kubelet is misconfigured, potentially allowing secure access to all requests on the kubelet, without the need to authenticate	
High	Remote Code Execution	Exposed Run Inside Container	An attacker could run an arbitrary command inside a container	
High	Remote Code Execution	Exposed Exec On Container	An attacker could run arbitrary commands on a container	
Medium	Information Disclosure	K8s Version Disclosure	The kubernetes version could be obtained from logs in the /metrics endpoint	v1.9.0
Medium	Information Disclosure	Exposed Pods	An attacker could view sensitive information about pods that are bound to a Node using the /pods endpoint	count: 9
Medium	Information Disclosure	Cluster Health Disclosure	By accessing the open /healthz handler, an attacker could get the cluster health state without authenticating	status: ok
Medium	Information Disclosure	Exposed Running Pods	Outputs a list of currently running pods, and some of their metadata, which can reveal sensitive information	9 running pods
Medium	Information Disclosure	Exposed Container Logs	Output logs from a running container are using the exposed /containerLogs endpoint	

kube-hunter with kube-bench

172.28.128.3

Node / Master

12 vulnerabilities

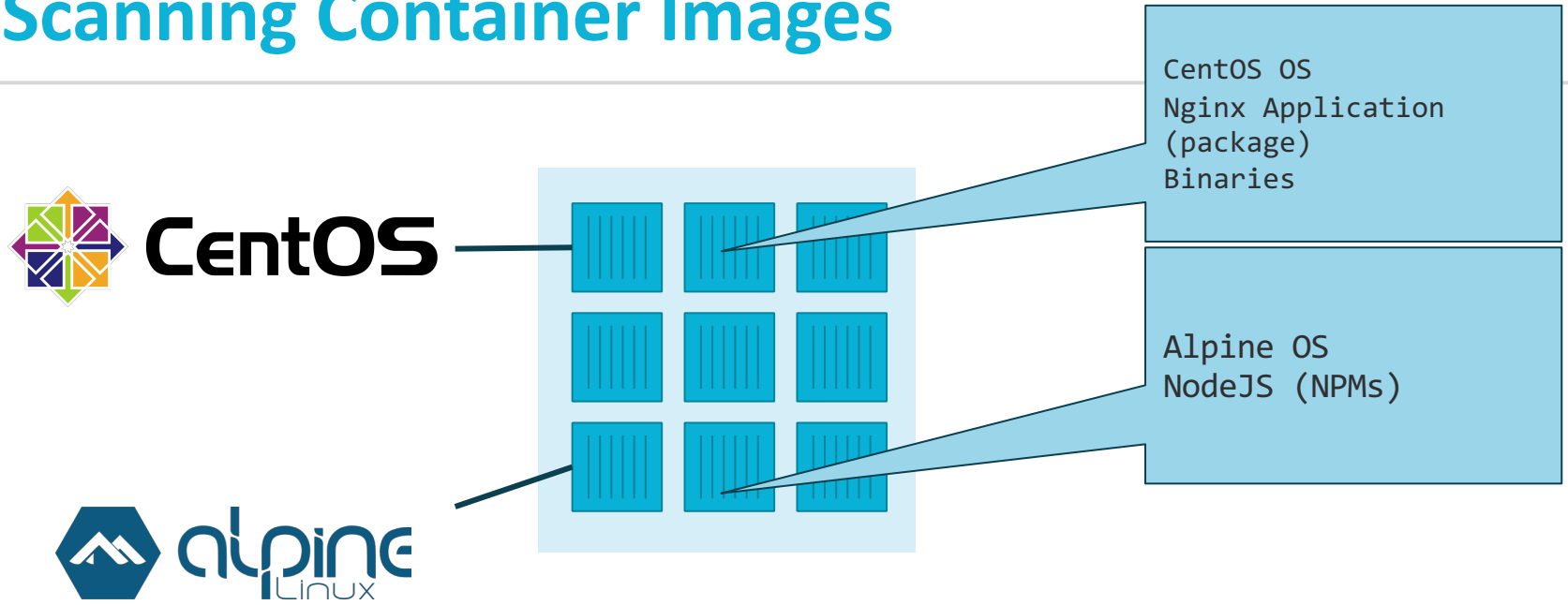
SEVERITY	CATEGORY	VULNERABILITY	DESCRIPTION	EVIDENCE
High	Remote Code Execution	Exposed Attaching To Container	Opens a websocket that could enable an attacker to attach to a running container	
High	Remote Code Execution	Anonymous Authentication	The kubelet is misconfigured, potentially allowing secure access to all requests on the kubelet, without the need to authenticate	
High	Remote Code Execution	Exposed Run Inside Container	An attacker could run an arbitrary command inside a container	
High	Remote Code Execution	Exposed Exec On Container	An attacker could run arbitrary commands on a container	
Medium	Information Disclosure	K8s Version Disclosure	The kubernetes version could be obtained from logs in the /metrics endpoint	v1.9.0
Medium	Information Disclosure	Exposed Pods	An attacker could view sensitive information about pods that are bound to a Node using the /pods endpoint	count: 9
Medium	Information Disclosure	Cluster Health Disclosure	By accessing the open /healthz handler, an attacker could get the cluster health state without authenticating	status: ok
Medium	Information Disclosure	Exposed Running Pods	Outputs a list of currently running pods, and some of their metadata, which can reveal sensitive information	9 running pods
Medium	Information Disclosure	Exposed Container Logs	Output logs from a running container are using the exposed /containerLogs endpoint	

```
[INFO] 2 Worker Node Security Configuration
[INFO] 2.1 Kubelet
[FAIL] 2.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 2.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[FAIL] 2.1.3 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 2.1.4 Ensure that the --client-ca-file argument is set as appropriate (Scored)
[FAIL] 2.1.5 Ensure that the --read-only-port argument is set to 0 (Scored)
[FAIL] 2.1.6 Ensure that the --streaming-connection-idle-timeout argument is not set to 0 (Scored)
[FAIL] 2.1.7 Ensure that the --protect-kernel-defaults argument is set to true (Scored)
[FAIL] 2.1.8 Ensure that the --make-iptables-util-chains argument is set to true (Scored)
[FAIL] 2.1.9 Ensure that the --keep-terminated-pod-volumes argument is set to false (Scored)
[PASS] 2.1.10 Ensure that the --hostname-override argument is not set (Scored)
[FAIL] 2.1.11 Ensure that the --event-qps argument is set to 0 (Scored)
[PASS] 2.1.12 Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as approp
[PASS] 2.1.13 Ensure that the --cadvisor-port argument is set to 0 (Scored)
[FAIL] 2.1.14 Ensure that the RotateKubeletClientCertificate argument is set to true
[FAIL] 2.1.15 Ensure that the RotateKubeletServerCertificate argument is set to true
[INFO] 2.2 Configuration Files
[FAIL] 2.2.1 Ensure that the kubelet.conf file permissions are set to 644 or more restrictive (Score
[FAIL] 2.2.2 Ensure that the kubelet.conf file ownership is set to root:root (Scored)
[FAIL] 2.2.3 Ensure that the kubelet service file permissions are set to 644 or more restrictive (Sc
[FAIL] 2.2.4 2.2.4 Ensure that the kubelet service file ownership is set to root:root (Scored)
[FAIL] 2.2.5 Ensure that the proxy kubeconfig file permissions are set to 644 or more restrictive (S
[FAIL] 2.2.6 Ensure that the proxy kubeconfig file ownership is set to root:root (Scored)
[WARN] 2.2.7 Ensure that the certificate authorities file permissions are set to 644 or more restric
[WARN] 2.2.8 Ensure that the client certificate authorities file ownership is set to root:root
```

```
== Remediations ==
2.1.1 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable.
--allow-privileged=false
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
systemctl restart kubelet.service

2.1.2 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable.
--anonymous-auth=false
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
systemctl restart kubelet.service

2.1.3 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_AUTHZ_ARGS variable.
--authorization-mode=Webhook
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
systemctl restart kubelet.service

2.1.5 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable.
--read-only-port=0
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
```

MicroScanner

Scanning Container Images



Vulnerability sources

- Vulnerabilities are published on different security advisories
- NVD – national vulnerability database
- Vendors will have their own advisories

Case study: Debian / CVE-2017-8807

- NVD reports this in Varnish HTTP Cache versions 4.0.0 - 5.2.0

Configuration 1
- OR
  - cpe:2.3:a:varnish-cache:varnish:4.0.0:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.0.1:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.0.2:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.0.3:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.0.4:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.0.5:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.0:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.1:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.2:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.3:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.4:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.5:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.6:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.7:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:4.1.8:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:5.0.0:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:5.1.1:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:5.1.2:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:5.1.3:*:*:*:*:*:*:*
  - cpe:2.3:a:varnish-cache:varnish:5.2.0:*:*:*:*:*:*:*

Configuration 2
- OR
  - cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

Case study: Debian / CVE-2017-8807

- NVD reports this in Varnish HTTP Cache versions 4.0.0 - 5.2.0
- Debian applied patch to 5.0.0

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
varnish (PTS)	wheezy, wheezy (security)	3.0.2-2+deb7u2	fixed
	jessie (security), jessie	4.0.2-1+deb8u1	fixed
	stretch (security), stretch	5.0.0-7+deb9u2	fixed
	sid	5.2.1-1	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
varnish	source	(unstable)	5.2.1-1	medium		881808
varnish	source	jessie	(not affected)			
varnish	source	stretch	5.0.0-7+deb9u2	medium	DSA-4034-1	
varnish	source	wheezy	(not affected)			

Notes

```
[jessie] - varnish <not-affected> (Vulnerable code not present, issue introduced in 4.1.0)
[wheezy] - varnish <not-affected> (Vulnerable code not present, issue introduced in 4.1.0)
http://varnish-cache.org/security/VSV00002.html
https://github.com/varnishcache/varnish-cache/pull/2429
Fixed by: https://github.com/varnishcache/varnish-cache/commit/176f8a075a
```

Case study: Alpine / busybox 1.27.2

Vuln ID	Summary	CVSS Severity
CVE-2017-16544	In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks. **Published:** November 20, 2017; 10:29:00 AM -05:00	*V3:* 8.8 HIGH *V2:* 6.5 MEDIUM
CVE-2017-15874	archival/libarchive/decompress_unlzma.c in BusyBox 1.27.2 has an Integer Underflow that leads to a read access violation. **Published:** October 24, 2017; 04:29:00 PM -04:00	*V3:* 5.5 MEDIUM *V2:* 4.3 MEDIUM
CVE-2017-15873	The get_next_block function in archival/libarchive/decompress_bunzip2.c in BusyBox 1.27.2 has an Integer Overflow that may lead to a write access violation. **Published:** October 24, 2017; 04:29:00 PM -04:00	*V3:* 5.5 MEDIUM *V2:* 4.3 MEDIUM

Case study: Alpine / busybox 1.27.2

path: root/main/busybox

Mode	Name
-rw-r--r--	0001-add-remove-shell-fix-crash-when-shell-is-already-add.patch
-rw-r--r--	0001-ash-add-support-for-command_not_found_handle-hook-fu.patch
-rw-r--r--	0001-ash-exec-busybox.static.patch
-rw-r--r--	0001-ash-introduce-a-config-option-to-search-current.patch
-rw-r--r--	0001-fsck-resolve-LABEL-.-UUID-.-spec-to-device.patch
-rw-r--r--	0002-app-location-for-cpio-vi-and-lspci.patch
-rw-r--r--	0003-udhcpc-set-default-discover-retries-to-5.patch
-rw-r--r--	0004-ping-make-ping-work-without-root-privileges.patch
-rw-r--r--	0005-fbsplash-support-console-switching.patch
-rw-r--r--	0006-fbsplash-support-image-and-bar-alignment-and-positio.patch
-rw-r--r--	0007-depmod-support-generating-kmod-binary-index-files.patch
-rw-r--r--	0008-diff-add-support-for-no-dereference.patch
-rw-r--r--	0009-sysklogd-add-Z-option-to-adjust-message-timezones.patch
-rw-r--r--	0010-udhcpc-Don-t-background-if-n-is-given.patch
-rw-r--r--	0011-testsuite-fix-cpio-tests.patch
-rw-r--r--	0012-microcom-segfault.patch
-rw-r--r--	0013-CVE-2017-16544.patch
-rw-r--r--	0014-CVE-2017-15873.patch
-rw-r--r--	0015-CVE-2017-15874.patch
-rw-r--r--	APKBUILD
-rw-r--r--	acpid.logrotate
-rw-r--r--	bbsuid.c
-rw-r--r--	busybox-extras.post-install
-rw-r--r--	busybox-extras.pre-deinstall
-rw-r--r--	busybox.post-install
-rw-r--r--	busybox.post-upgrade
-rw-r--r--	busybox.trigger
-rw-r--r--	busyboxconfig
-rw-r--r--	busyboxconfig-extras
-rw-r--r--	dad.if-up

Patches for the known vulnerabilities

MicroScanner - free package vulnerability scanning

- Runs as part of build
- Contacts Aqua Security cyber-center vulnerability database
- Jenkins plug-in available

```
FROM debian:jessie-slim
RUN apt-get update && apt-get -y install ca-certificates
ADD https://get.aquasec.com/microscanner
RUN chmod +x microscanner
ARG token
RUN /microscanner ${token} && rm /microscanner
```

github.com/aquasecurity/micro-scanner
github.com/aquasecurity/kube-bench
github.com/aquasecurity/kube-hunter