Approaching Kubernetes Security

By Rod Soto
@rodsoto

$whoami

Over 15 years of experience in information technology and security. He has spoken at ISSA, ISC2, OWASP, DEFCON, RSA Conference,Hackmiami, DerbyCon, Splunk .CONF, Black Hat,BSides, Underground Economy and also been featured in Rolling Stone Magazine, Pentest Magazine, Univision, BBC, Forbes, VICE, Fox News and CNN.

Rod Soto was the winner of the 2012 BlackHat Las Vegas CTF competition and is the founder and lead developer of the **Kommand && KonTroll/NOQRTRCTF** competitive hacking Tournament series.

Secretary of the board of Hackmiami %27, Co-founder of Pacific Hackers Silicon Valley meetup. Founder & President Pacific Hackers Conference www.phack.org.

Kubernetes

Open-source container-orchestration system for automating application deployment, scaling, and management. It was originally designed by Google, and is now maintained by the Cloud Native Computing Foundation.

Known also as K8s

**Kubernetes (κυβερνήτης, Greek for "governor", "helmsman" or "captain")*

Kubernetes Objects

Pod

A pod consists of one or more containers that are guaranteed to be co-located on the host machine and can share resources.

Replica sets

Replica Sets[22] are a grouping mechanism that lets Kubernetes maintain the number of instances that have been declared for a given pod.

Services

A Kubernetes service is a set of pods that work together, such as one tier of a multi-tier application.

Kubernetes Objects

Volumes

Filesystems in the Kubernetes container provide ephemeral storage, by default. A Kubernetes Volume[25] provides persistent storage that exists for the lifetime of the pod itself. This storage can also be used as shared disk space for containers within the pod.

Namespaces

They are intended for use in environments with many users spread across multiple teams, or projects, or even separating environments like development, test, and production

Kubernetes Objects

ConfigMaps and Secrets

A common application challenge is deciding where to store and manage configuration information, some of which may contain sensitive data. Configuration data can be anything as fine-grained as individual properties or coarse-grained information like entire configuration files or JSON / XML documents.

Secrets ---> Example of use = Reference password for DB → (Base64 encoding decoded before passing it to the pod)

ConfigMaps → Referenced in yaml application deployment files, not good for storing sensitive information as they are in plain text. Example of use = Files mapped to a volume within a pod

Kubernetes Objects

Deployment

Sets of Identical Pods. Pod templates define how to rund pods. Pod definitions describe the pods including their state.(i.e number of pods)

StatefulSet

A type of Kubernetes controller used to manage and maintain Pods. StatefulSets assign unique identifiers to Pods. This enables tracking which pod is used by which client. Use for applications that need unique network identifiers or stable persistent storage (i.e a database).

Kubernetes Objects

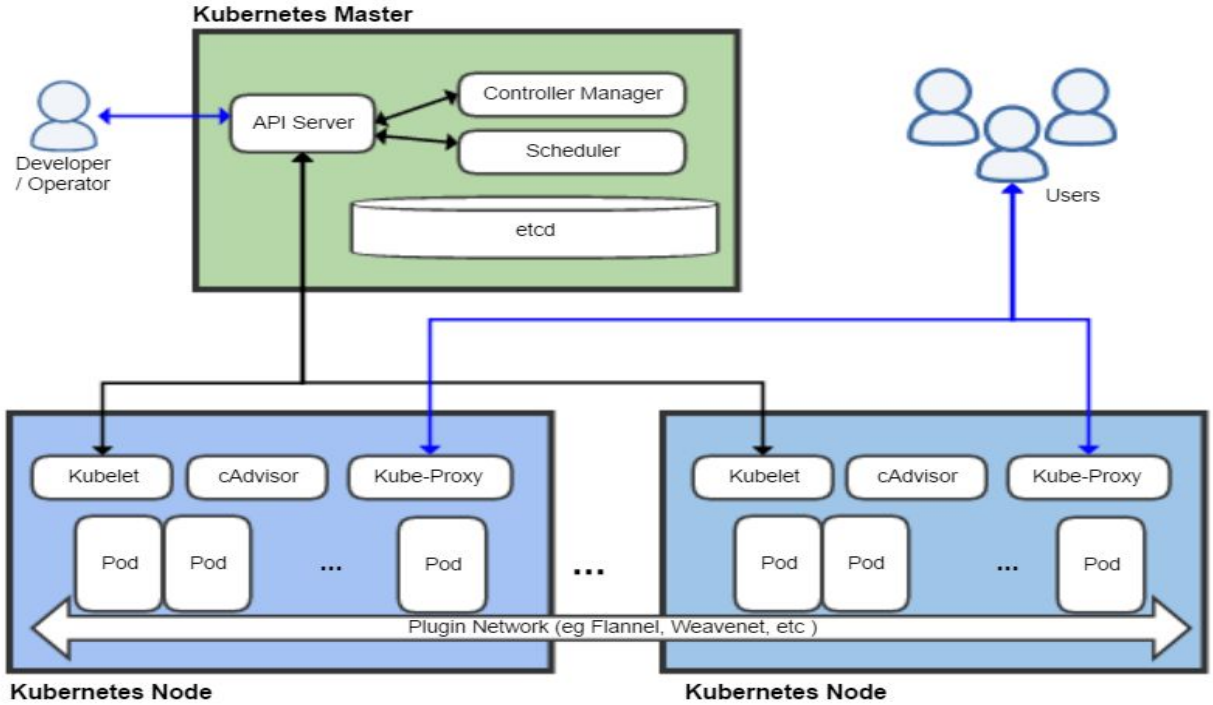
DaemonSets

Like other workload objects, **DaemonSets** manage groups of replicated Pods. However, DaemonSets attempt to adhere to a one-Pod-per-node model, either across the entire cluster or a subset of nodes. As you add nodes to a node pool, DaemonSets automatically add Pods to the new nodes as needed. (Example: fluentd, logstash)

Job

Kubernetes create pods and run them until application completes a workload. Specifications are in a configuration file, includes specifications about the container to use and what command to run.

Kubernetes Cluster



Kubernetes Cluster

Api-Server - The API server is a key component and serves the Kubernetes API using JSON over HTTP, which provides both the internal and external interface to Kubernetes.

Controller Manager - Control loops that watch the state of your cluster. A cluster has at least one worker node and at least one master node. , then make or request changes where needed.

Scheduler - The scheduler tracks resource use on each node to ensure that workload is not scheduled in excess of available resources.

Etcd - Stores the entire state of the cluster: its configuration, specifications, and the statuses of the running workloads.

Kubernetes Cluster

Kubelet - Primary “node agent” that runs on each node

CAdvisor - Open source container resource usage collector (Web Interface)

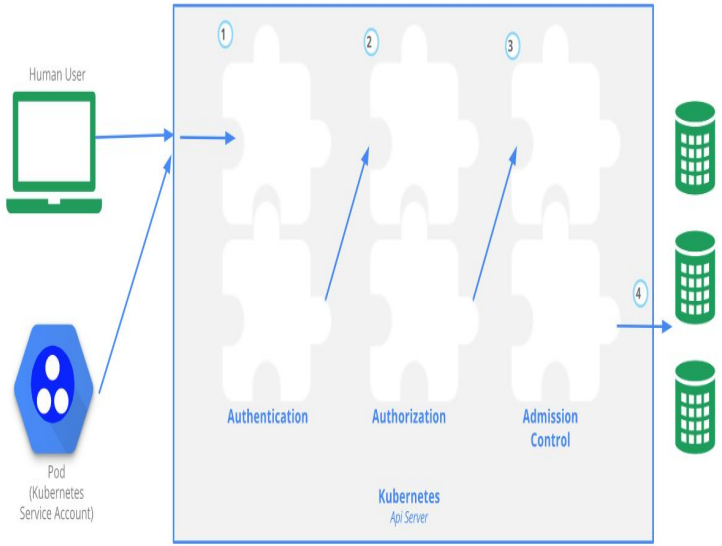
Kube-Proxy - Network proxy that runs on each node in your cluster, implementing part of the Kubernetes service concept. Reflects services as defined in the Kubernetes API on each node and can do simple TCP, UDP, and SCTP stream forwarding or round robin TCP, UDP, and SCTP forwarding across a set of backends.

Kube-Node - A node is a worker machine in Kubernetes, previously known as a `minion`. A node may be a VM or physical machine, depending on the cluster. Each node contains the services necessary to run pods and is managed by the master components. The services on a node include the container runtime, kubelet and kube-proxy.

Accessing Kubernetes

Users access the API using `kubectl`, client libraries, or by making REST requests. Both human users and Kubernetes service accounts can be authorized for API access. When a request reaches the API, it goes through several stages, illustrated in the following diagram

A request must include the username of the requester, the requested action, and the object affected by the action.



Accessing Kubernetes

- **Transport Security** - (API 6443)
- **Authentication** - Client Certificates, Password, and Plain Tokens, Bootstrap Tokens, and JWT Tokens (used for service accounts)
- **Authorization -** ABAC mode, RBAC Mode, and Webhook
- **Admission Control -** Admission Control Modules are software modules that can modify or reject requests.They act on objects being created, deleted, updated or connected (proxy).
- **API Server Ports and IPs -** (8080, 6443, 443)

Kubernetes - The CI/CD - Devops attack surface

- Source Code repository: github, gitlab, S3, SVN
- CI/CD Platform: Jenkins, CircleCI, TravisCI
- Container Repository: Docker, Vagrant
- IaaS Provider: Kubernetes flavor, Microsoft EKS, Amazon AKS
- IaC: Ansible, Terraform, Cloudformation, Chef

Kubernetes attack vectors

Internal VS External

Inside Cluster	-	**Outside Cluster**
CI/CD Devops attack surface (Accounts, Pods, Nodes)	-	Exposed API
Application Vulns(CVE-2019-16276)	-	Exposed Kubelet
Container Implantation (Mitre T1147)	-	Information disclosure
	-	Exposed Management GUI
	-	Denial of Service

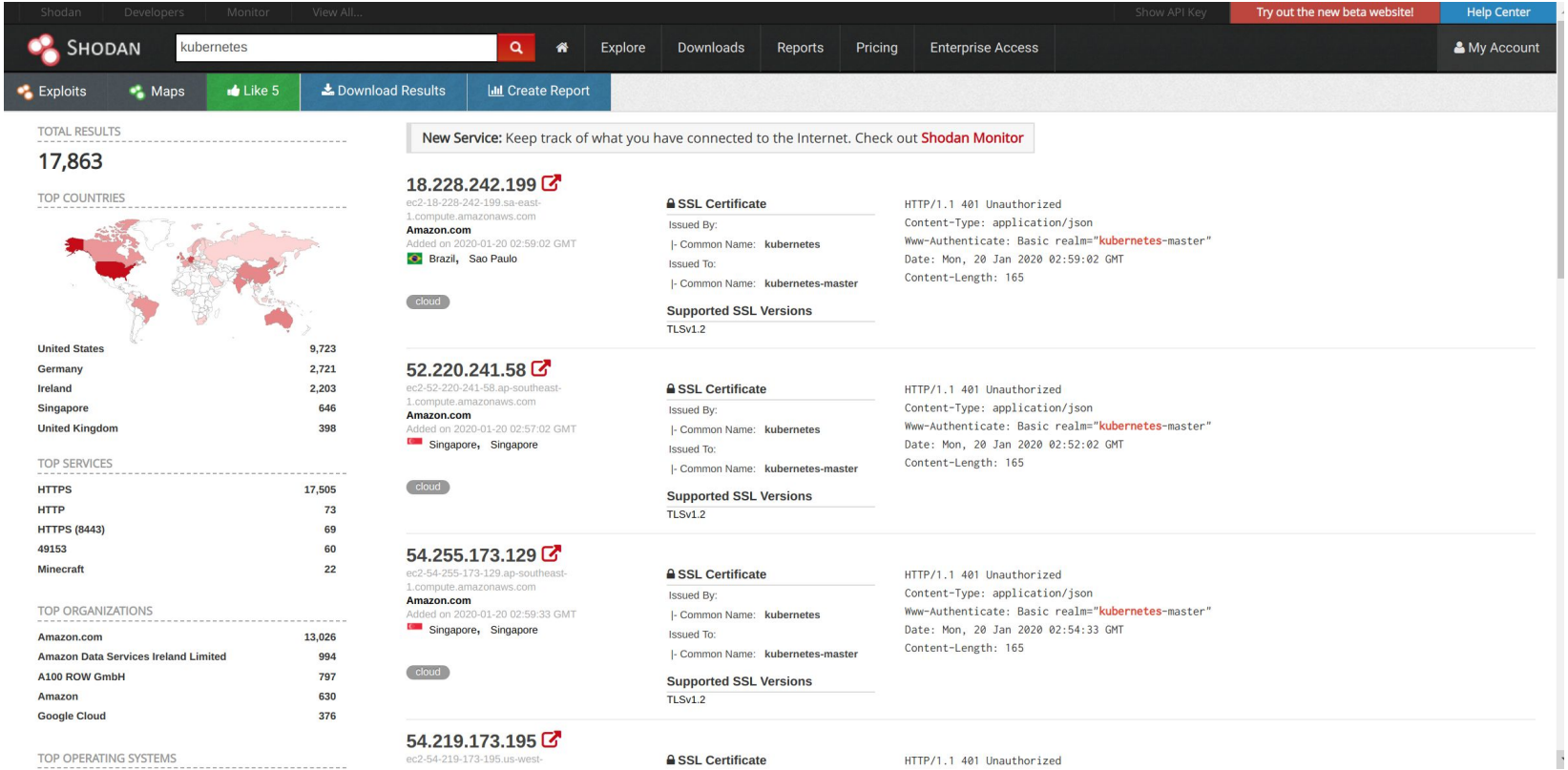
Vulnerability / Attack TTPs references

- Mitre ATT&CK https://attack.mitre.org/
- Mitre Cloud ATT&CK https://attack.mitre.org/matrices/enterprise/cloud/
- OWASP TOP 10 https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
- OWASP TOP 10 API https://www2.owasp.org/www-project-api-security/
- Mitre CWE https://cwe.mitre.org/
- NIST https://nvd.nist.gov/
- Mitre CVE https://cve.mitre.org/
- Mitre CAPEC https://capec.mitre.org/
- Cloud Security Alliance Egregious 11 https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/
- CVSS Score https://www.first.org/cvss/specification-document

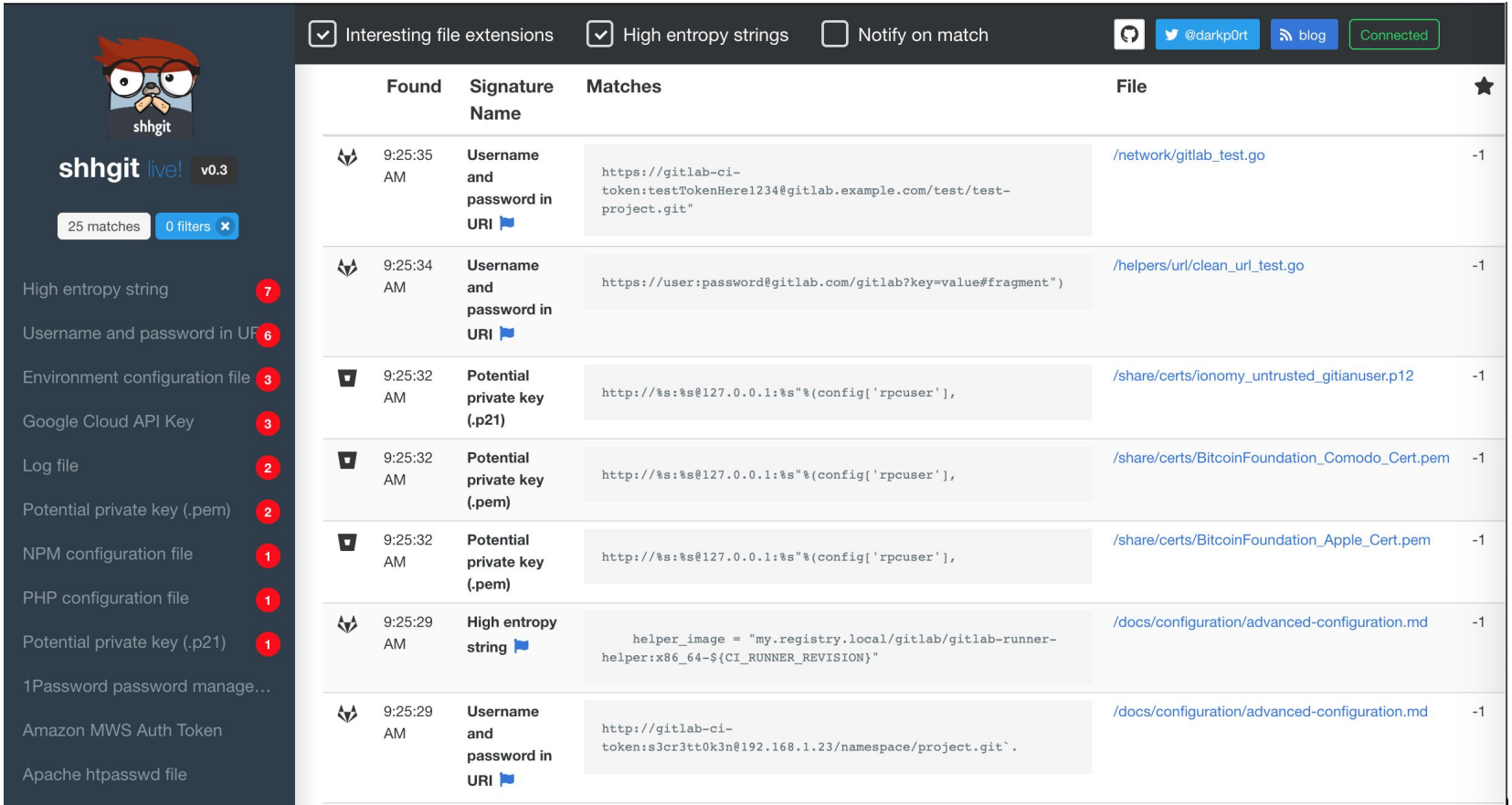
Kubernetes attack vectors

- **Cloud API** - Mitre Cloud ATT&CK T1522 Example: CVE-2018-1002105, CVE-2019-11253 (Improper input validation in the Kubernetes API)
- **Misconfiguration** - Mitre Cloud ATT&CK T1190 OWASP A6-Security Misconfiguration - Example: Tesla Hack
- **Information Disclosure** - OWASP A3-Sensitive Data Exposure - Exposed API, Kubelets.
- **CSA Abuse and nefarious use of cloud services -** Mitre ATT&CK T1496 (CryptoMining, DDoS)
- **CWE-59: Improper Link Resolution Before File Access** - CVE-2017-1002101
- **Application Vulnerability** - CVE-2019-16276 (Bypass authentication using HTTP request smuggling)
- **CVE-2019-9512/CVE-2019-9514** - HTTP/2 Ping Flood Mitre ATT&CK T1498

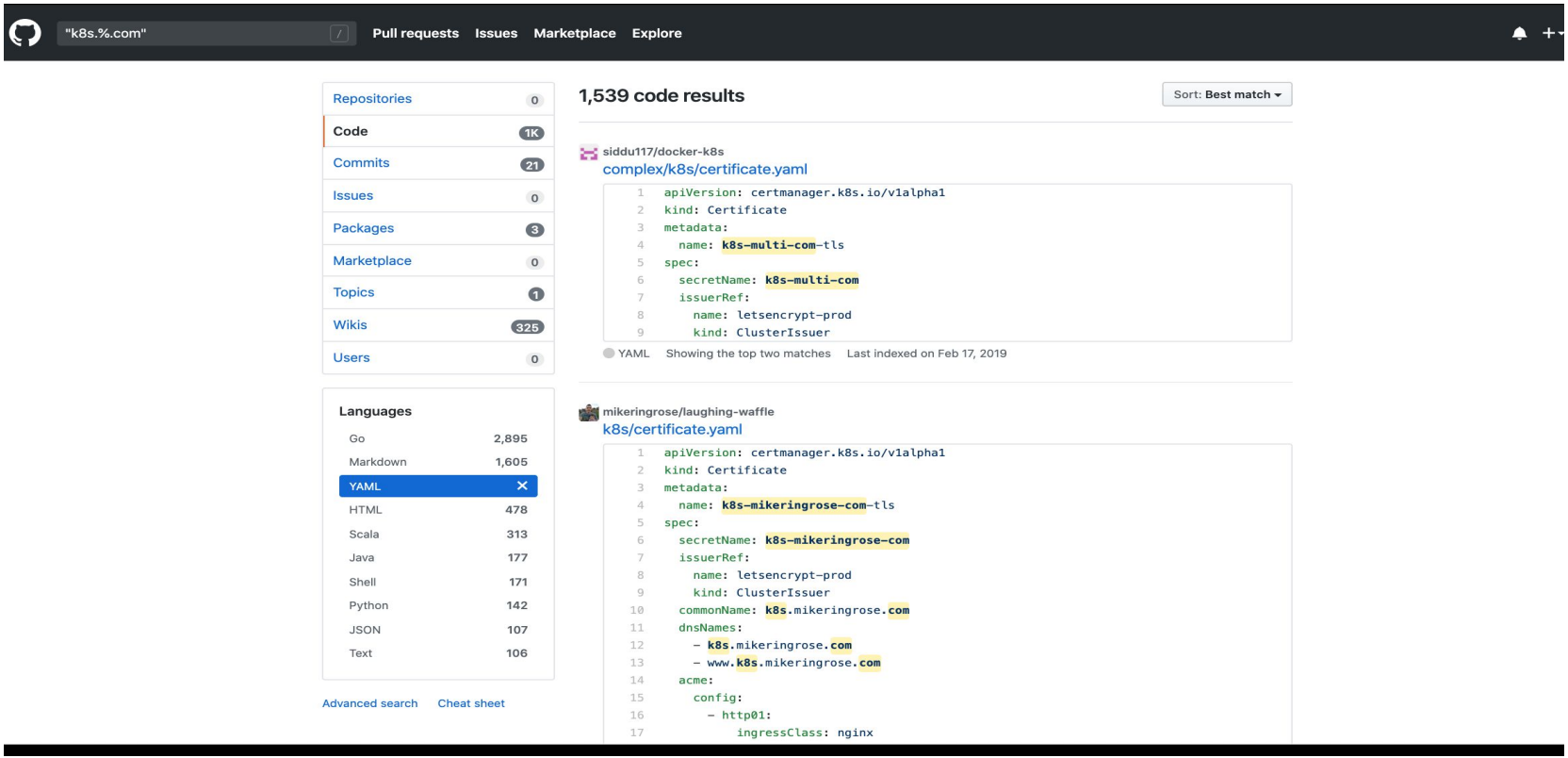
Tools to assess Kubernetes Security



Sshgit - https://shhgit.darkport.co.uk/



Tools to assess Kubernetes Security



Common Kubernetes ports

Port	Process	Description
443/TCP	kube-apiserver	Kuberntes API port
2379/TCP	etcd	
6666/TCP	etcd	etcd
4194/TCP	cAdvisor	Contrainer metrics
6443/TCP	kube-apiserver	Kubernetes API port
8443/TCP	kube-apiserver	Minikube API port
8080/TCP	kube-apiserver	Insecure API port
10250/TCP	kubelet	HTTPS API which allows full node access
10255/TCP	kubelet	Unauthenticated read-only HTTP port: pods, runningpods and node state
10256/TCP	kube-proxy	Kube Proxy health check server
9099/TCP	calico-felix	Health check server for Calico
6782-4/TCP	weave	Metrics and endpoints

Tools to assess Kubernetes Security

Kube-Bench https://github.com/aquasecurity/kube-bench

```
trajan@x-dre:~/kube-bench$ kubectl logs kube-bench-9q8d6
[INFO] 2 Worker Node Security Configuration
[INFO] 2.1 Kubelet
[PASS] 2.1.1 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 2.1.2 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 2.1.3 Ensure that the --client-ca-file argument is set as appropriate (Scored)
[FAIL] 2.1.4 Ensure that the --read-only-port argument is set to 0 (Scored)
[PASS] 2.1.5 Ensure that the --streaming-connection-idle-timeout argument is not set to 0 (Scored)
[FAIL] 2.1.6 Ensure that the --protect-kernel-defaults argument is set to true (Scored)
[PASS] 2.1.7 Ensure that the --make-iptables-util-chains argument is set to true (Scored)
[PASS] 2.1.8 Ensure that the --hostname-override argument is not set (Scored)
[FAIL] 2.1.9 Ensure that the --event-qps argument is set to 0 (Scored)
[FAIL] 2.1.10 Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate (Scored)
[INFO] 2.1.11 [DEPRECATED] Ensure that the --cadvisor-port argument is set to 0
[PASS] 2.1.12 Ensure that the --rotate-certificates argument is not set to false (Scored)
[PASS] 2.1.13 Ensure that the RotateKubeletServerCertificate argument is set to true (Scored)
[PASS] 2.1.14 Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers (Not Scored)
[INFO] 2.2 Configuration Files
[PASS] 2.2.1 Ensure that the kubelet.conf file permissions are set to 644 or more restrictive (Scored)
[PASS] 2.2.2 Ensure that the kubelet.conf file ownership is set to root:root (Scored)
[PASS] 2.2.3 Ensure that the kubelet service file permissions are set to 644 or more restrictive (Scored)
[PASS] 2.2.4 Ensure that the kubelet service file ownership is set to root:root (Scored)
[PASS] 2.2.5 Ensure that the proxy kubeconfig file permissions are set to 644 or more restrictive (Scored)
[PASS] 2.2.6 Ensure that the proxy kubeconfig file ownership is set to root:root (Scored)
[PASS] 2.2.7 Ensure that the certificate authorities file permissions are set to 644 or more restrictive (Scored)
[PASS] 2.2.8 Ensure that the client certificate authorities file ownership is set to root:root (Scored)
[PASS] 2.2.9 Ensure that the kubelet configuration file ownership is set to root:root (Scored)
[PASS] 2.2.10 Ensure that the kubelet configuration file has permissions set to 644 or more restrictive (Scored)

== Remediations ==
2.1.4 If using a Kubelet config file, edit the file to set readOnlyPort to 0 .
If using command line arguments, edit the kubelet service file
/etc/systemd/system/kubelet.service 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:
```

Tools to assess Kubernetes Security

Kube-Hunter https://github.com/aquasecurity/kube-hunter

```
trajan@x-dre:~/kube-hunter$ ./kube-hunter.py
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)
Your choice: 1
Remotes (separated by a ','): 18.228.242.199

Nodes
+-------------+-----------------+
| TYPE        | LOCATION        |
+-------------+-----------------+
| Node/Master | 18.228.242.199 |
+-------------+-----------------+

Detected Services
+----------------------+---------------------+-----------------------+
| SERVICE              | LOCATION            | DESCRIPTION           |
+----------------------+---------------------+-----------------------+
| Unrecognized K8s API | 18.228.242.199:443 | A Kubernetes API      |
|                      |                     | service               |
+----------------------+---------------------+-----------------------+

No vulnerabilities were found
```

Tools to assess Kubernetes Security

Kubeaudit - https://github.com/Shopify/kubeaudit/releases/tag/v0.7.0

```
trajan@x-dre:~/Downloads$ ./kubeaudit priv
INFO[0000] Not running inside cluster, using local config
ERRO[0001] Privileged set to true! Please change it to false!  Container=aws-node KubeType=daemonSet Name=aws-node Namespace=kube-sys
ERRO[0001] Privileged set to true! Please change it to false!  Container=kube-proxy KubeType=daemonSet Name=kube-proxy Namespace=kube
tem
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=coredns KubeType=deployment Name=
dns Namespace=kube-system
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=guestbook KubeType=pod Name=guest
-2dgvv Namespace=default
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=guestbook KubeType=pod Name=guest
-76rw2 Namespace=default
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=guestbook KubeType=pod Name=guest
-qqpwf Namespace=default
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=kube-bench KubeType=pod Name=kube
ch-9q8d6 Namespace=default
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=redis-master KubeType=pod Name=re
master-9lzld Namespace=default
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=redis-slave KubeType=pod Name=red
lave-4ktzs Namespace=default
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=redis-slave KubeType=pod Name=red
lave-rzfxl Namespace=default
ERRO[0001] Privileged set to true! Please change it to false!  Container=aws-node KubeType=pod Name=aws-node-g2nxs Namespace=kube-sys
ERRO[0001] Privileged set to true! Please change it to false!  Container=aws-node KubeType=pod Name=aws-node-nm948 Namespace=kube-sys
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=coredns KubeType=pod Name=coredns
d858ddc-4j8lm Namespace=kube-system
WARN[0001] Privileged defaults to false, which results in non privileged, which is okay.  Container=coredns KubeType=pod Name=coredns
d858ddc-nlhht Namespace=kube-system
ERRO[0001] Privileged set to true! Please change it to false!  Container=kube-proxy KubeType=pod Name=kube-proxy-xm78l Namespace=kube
tem
ERRO[0001] Privileged set to true! Please change it to false!  Container=kube-proxy KubeType=pod Name=kube-proxy-xp97d Namespace=kube
```

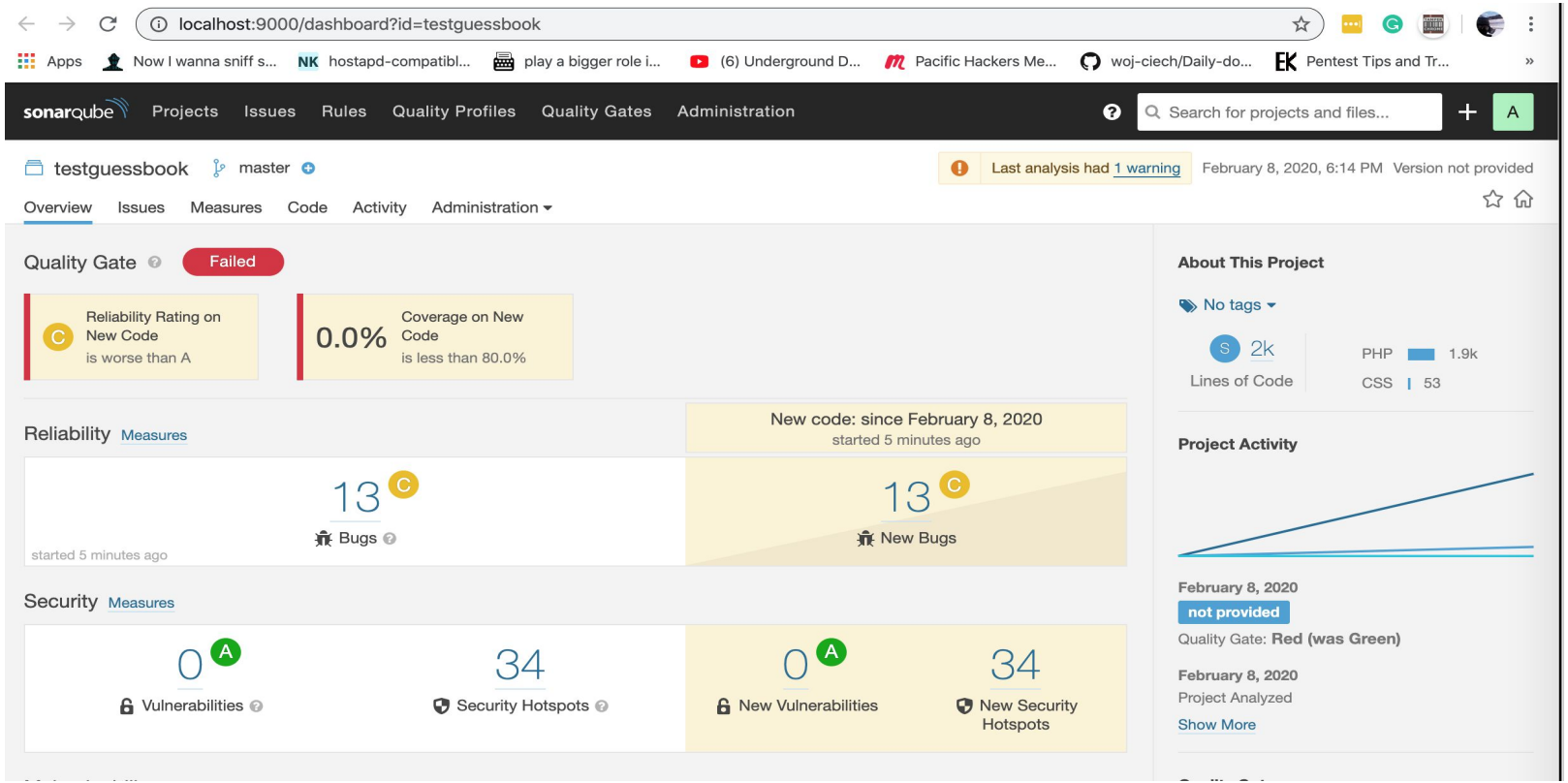
Tools to assess Kubernetes Security

Rhino Labs CCat https://github.com/RhinoSecurityLabs/ccat

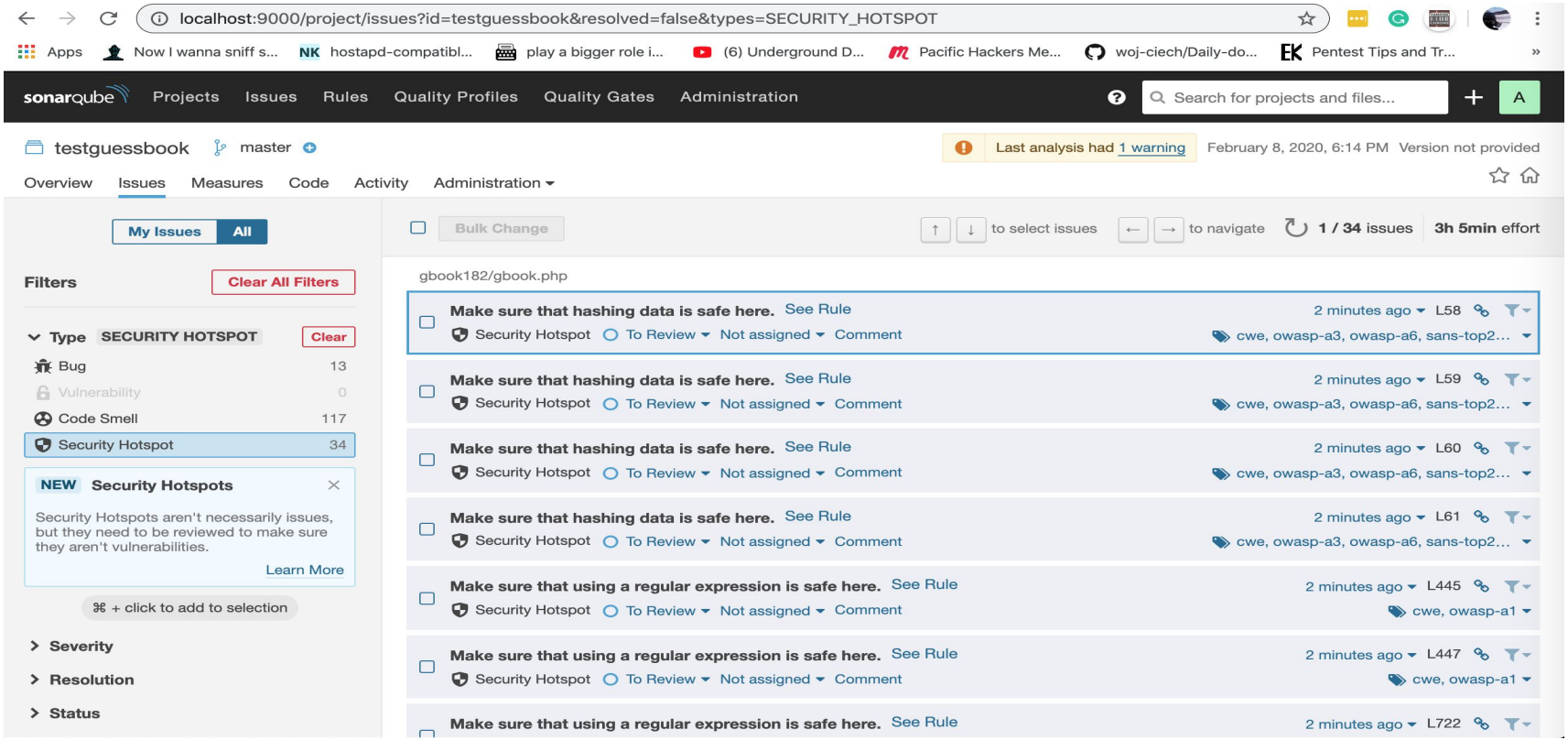
CyberArk KubiScan https://github.com/cyberark/KubiScan

```
    -ossss+/:::/+ssssssssssssssss+/:::/+sssso-
      :ssssssssssssssssssssssssssssssssssss/
       `+ssssssssssssssssssssssssssssssss+`
         -ossssssssssssssssssssssssssssss-
          `/sssssssssssssssssssssssssss/`

               KubiScan version 1.5
               Author: Eviatar Gerzi

/usr/local/lib/python3.6/dist-packages/urllib3/connectionpool.py:847: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification is strongly advised.
.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
/usr/local/lib/python3.6/dist-packages/urllib3/connectionpool.py:847: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification is strongly advised.
.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
/usr/local/lib/python3.6/dist-packages/urllib3/connectionpool.py:847: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification is strongly advised.
.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
/usr/local/lib/python3.6/dist-packages/urllib3/connectionpool.py:847: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification is strongly advised.
.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
+------------+
|Risky Users|
+----------+----------------+-------------+-----------------------------------+
| Priority | Kind           | Namespace   | Name                              |
+----------+----------------+-------------+-----------------------------------+
| CRITICAL | Group          | None        | system:masters                    |
| CRITICAL | ServiceAccount | default     | kubiscan-sa                       |
| CRITICAL | ServiceAccount | kube-system | clusterrole-aggregation-controller |
| HIGH     | ServiceAccount | kube-system | cronjob-controller                |
| HIGH     | ServiceAccount | kube-system | daemon-set-controller             |
| HIGH     | ServiceAccount | kube-system | deployment-controller             |
| CRITICAL | ServiceAccount | kube-system | expand-controller                 |
| CRITICAL | ServiceAccount | kube-system | generic-garbage-collector         |
| CRITICAL | ServiceAccount | kube-system | horizontal-pod-autoscaler         |
| HIGH     | ServiceAccount | kube-system | job-controller                    |
| CRITICAL | ServiceAccount | kube-system | namespace-controller              |
| CRITICAL | ServiceAccount | kube-system | persistent-volume-binder          |
| HIGH     | ServiceAccount | kube-system | replicaset-controller             |
| HIGH     | ServiceAccount | kube-system | replication-controller            |
| CRITICAL | ServiceAccount | kube-system | resourcequota-controller          |
| HIGH     | ServiceAccount | kube-system | statefulset-controller            |
| CRITICAL | User           | None        | system:kube-controller-manager    |
| HIGH     | ServiceAccount | kube-system | metrics-server                    |
| CRITICAL | ServiceAccount | kube-system | bootstrap-signer                  |
| HIGH     | ServiceAccount | kube-system | heapster                          |
| CRITICAL | ServiceAccount | kube-system | token-cleaner                     |
```

SonarQube.org Code analysis



SonarQube.org Code analysis



How to harden & defend K8s

- **Control access to API**

    - Use TLS
    - API Authentication / Authorization (RBAC)

- Control access to Kubelet (Authentication)

- Runtime variables

- Apply policies and controls limit by use case how those objects act on the cluster, themselves, and other resources. (Resource usage/limits/ranges)

- Limit privileges that containers run

- Prevent containers from loading unwanted kernel modules (be careful what AMIs you chose)

-

How to harden and defend K8s

- Restrict network access
- Restrict cloud metadata API access
- Control which Pods nodes may access
- Protect Cluster from compromise
  - Restrict access to etcd
  - Enable audit logging
  - Restrict access to alpha/beta features
  - Rotate infrastructure credentials
  - Review third party integrations
  - Encrypt secrets at rest/transit
  - Update and patch per alerts and vulnerability advisories

How to harden & defend k8s

- User cloud security assessment tools like CS Suite https://github.com/SecurityFTW/cs-suite
- Watch specifically for risky permissions (Eviatar Gerzi)
  - Listing secrets(potentially view all the secrets in a specific namespace)
  - Create pods
  - Impersonation of privilege accounts
  - Reading secrets (full secret's name may not get all secrets buy may help in brute forcing)
  - Privilege Rolebindings (allows account to add any user to high privilege roles) Watch specifically accounts with ClusterRole*

- Use tools such as SonarQube.org to harden CI/CD pipeline

How to harden & defend k8s

Watch for container scape

- *Cap_sys_admin*
  - Perform a range of system administration operations
- *Cap_sys_module*
  - Load and unload kernel modules
- *Cap_sys_boot*
  - Use reboot(2) and kexec_load(2)

*http://man7.org/linux/man-pages/man7/capabilities.7.html

Resources

- https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster/#controlling-access-to-the-kubernetes-api
- https://sysdig.com/blog/33-kubernetes-security-tools/
- https://www.cisecurity.org/blog/new-cis-benchmark-for-google-cloud-computing-platform/
- https://www.slideshare.net/Lacework/practical-guide-to-securing-kubernetes
- https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/
- https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/
- https://github.com/rsfl/researchdocs/blob/master/Using%20Splunk_ELK%20for%20Auditing%20AWS_GCP_Azure%20Security%20posture%20-%20defcon27.pptx
- https://www.amazon.com/Google-Cloud-Certified-Associate-Engineer/dp/1119564417/ref=sr_1_1?crid=2TGT6926CWROE&keywords=official+google+cloud+certified+associate+cloud+engineer+study+guide&qid=1580317660&sprefix=associate+engineer+%2Caps%2C194&sr=8-1

Resources

https://www.cyberark.com/threat-research-blog/kubernetes-pentest-methodology-part-2/
https://github.com/calinah/learn-by-hacking-kccn/blob/master/Learn%20by%20Hacking.pdf
https://www.cyberark.com/threat-research-blog/securing-kubernetes-clusters-by-eliminating-risky-permissions/
https://kubernetes.io/docs/reference/access-authn-authz/controlling-access/#authentication
https://www.cyberark.com/threat-research-blog/kubernetes-pentest-methodology-part-1/
https://www.cyberark.com/threat-research-blog/kubernetes-pentest-methodology-part-3/
https://github.com/calinah/learn-by-hacking-kccn/blob/master/k8s_cheatsheet.md
https://kubernetes.io/docs/concepts/policy/pod-security-policy/
https://github.com/kelseyhightower/kubernetes-the-hard-way
https://github.com/hardening-kubernetes/from-scratch
https://jwt.io
https://capsule8.com/blog/practical-container-escape-exercise/
https://bustakube.com

Q & A

Thank you

www.rodsoto.net

rod@rodsoto.net

Twitter

@rodsoto

Join us

%27 Slack

percent-27.slack.com