KubeCon | CloudNativeCon

Europe 2020

Virtual

The Kubernetes Bug Bounty Program: What Researchers and Users Need to Know

Who are we?

Reed Loden
Open Source Security
HackerOne

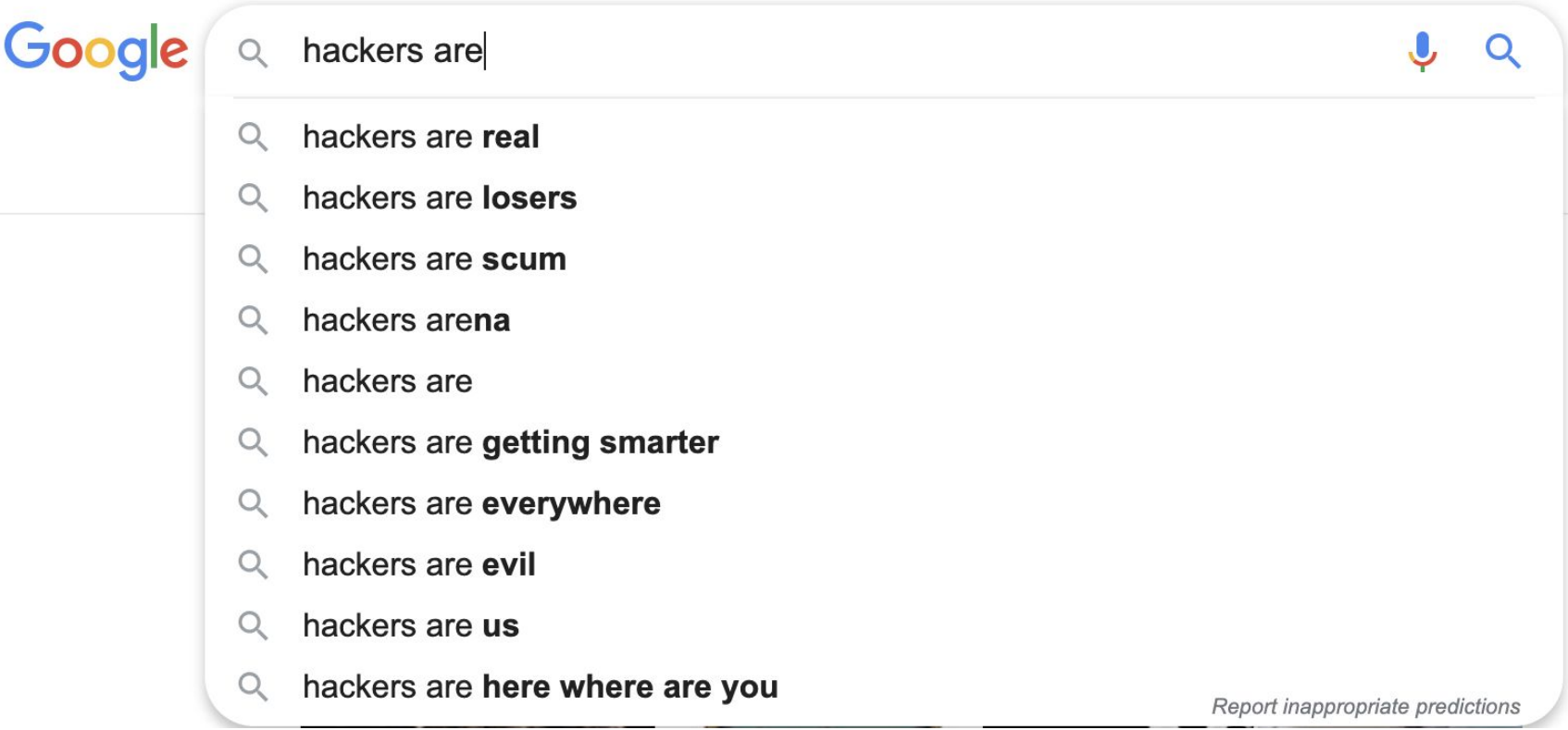
Taahir Ahmed
GKE Security
Google

What will you learn?

- What is hacking? Who are hackers?
- What is a bug bounty program?
- How does Kubernetes security work?
- What happens when a security vulnerability is reported in Kubernetes?
- How can you contribute?

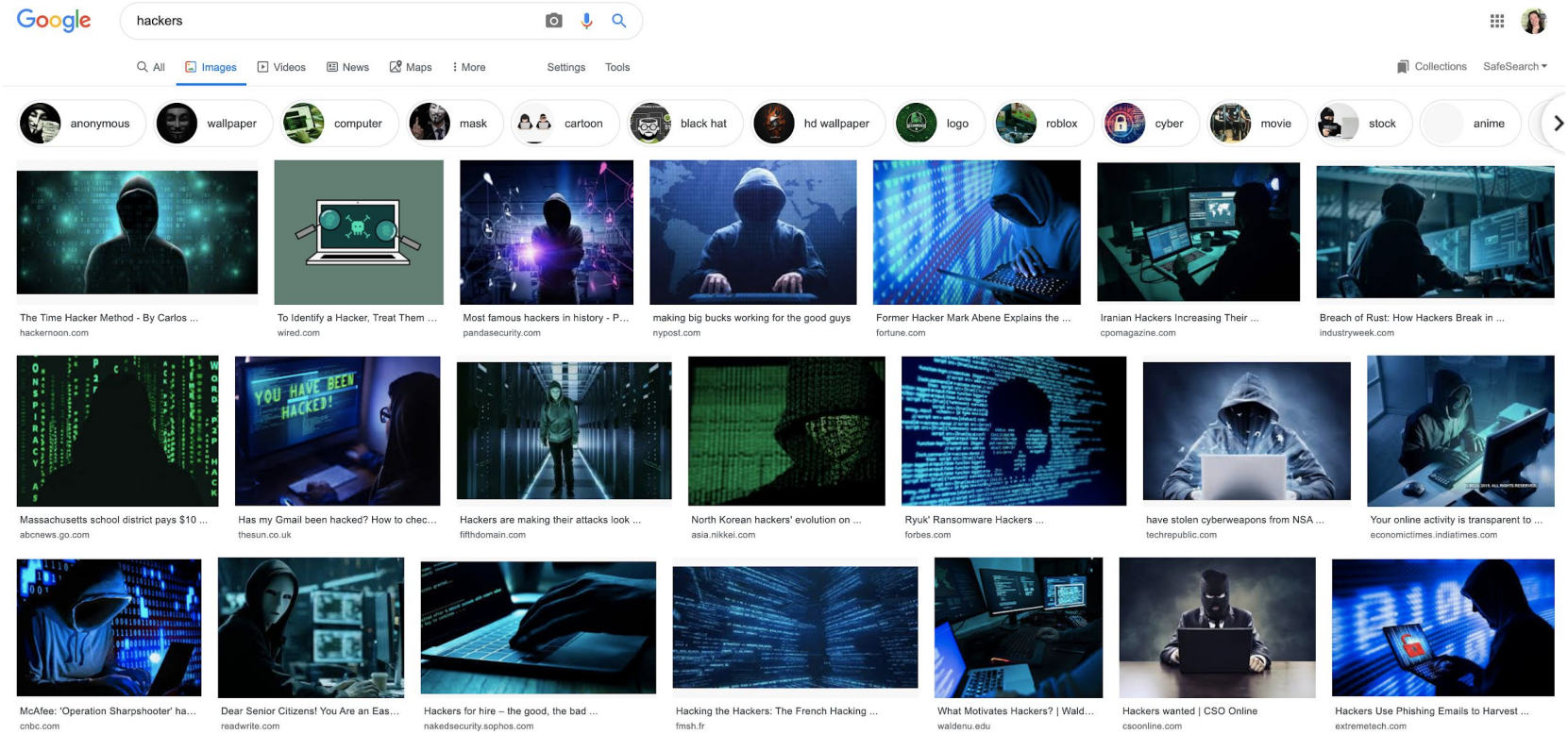
Let’s define “hacker”

What does the internet think about hackers?



What do people think hackers look like?

KubeCon CloudNativeCon Europe 2020 Virtual



What is a hacker?

Hacker:
NOUN

one who enjoys the intellectual challenge of creatively overcoming limitations.

How do you work with hackers?

Crowdsourced Security Testing

Vulnerability Coordination	Hacker-Powered Pentests	Bug Bounty Programs
Reactive Approach	Proactive; pay per finding	Proactive: Incentivize research with $$$
See Something? Say Something!	Real-time results	Engineers Learn through Practical Examples
“Welcome Mat”	Diverse testers; results in days	Save $$$ and reduce risk ongoing
Compliance (e.g. ISO 29147)	Compliance; vendor assessments	Cherry on top of the SDLC

Let’s get into Kubernetes

What is the PSC?

The Kubernetes Product Security Committee is the one-stop shop for all security-related issues in Kubernetes.

Business-hours on-call rotation by community members.

The active oncall triages incoming security reports:

- From the HackerOne Kubernetes bug bounty program
- From the security@kubernetes.io mailing list

Valid reports are handled as security incidents.

Why a BBP for Kubernetes?

First proposal was in February 2018:

- Get more security researcher attention on the Kubernetes codebase
- Simplify triage and response process for the Kubernetes Product Security Committee
- Show that Kubernetes is enterprise-ready
- Widen the net of contributors to Kubernetes security
- Define a way to get security coverage on Kubernetes project infrastructure

A vulnerability is submitted. Now what?

HackerOne Report

Collapse

TIMELINE

kebe submitted a report to **Kubernetes**. May 7th (3 months ago)

Report Submission Form

Summary:

Pod files /etc/hosts, /etc/hostname, /etc/resolve.conf are not readonly.
A normal pod running in kubernetes cluster can kil a host through write data to /etc/hosts.
Not only /etc/hosts, but also /etc/resolve.conf and /etc/hostname can do this.

Kubernetes Version:

<=1.18

Component Version:

Docker 19.03

Steps To Reproduce:

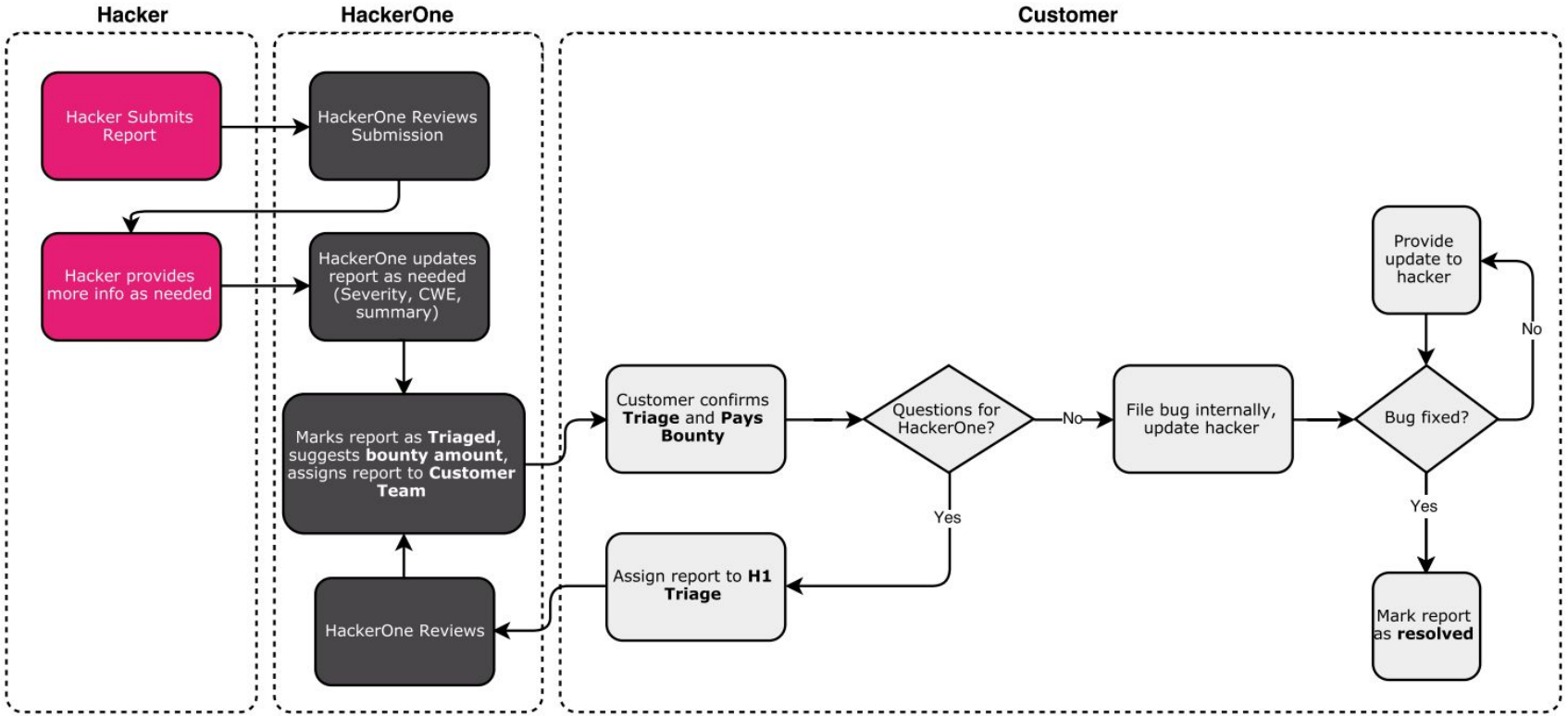
1. use kubectl create a pod like kubectl run
2. run `kubectl exec -it $POD_NAME -- dd if=/dev/zero of=/etc/hosts count=1000000 bs=10M`
3. run `df -h /var/lib/kubelet` on host that pod running, you can see the disk avaliable space are decreasing until the disk full.

Supporting Material/References:

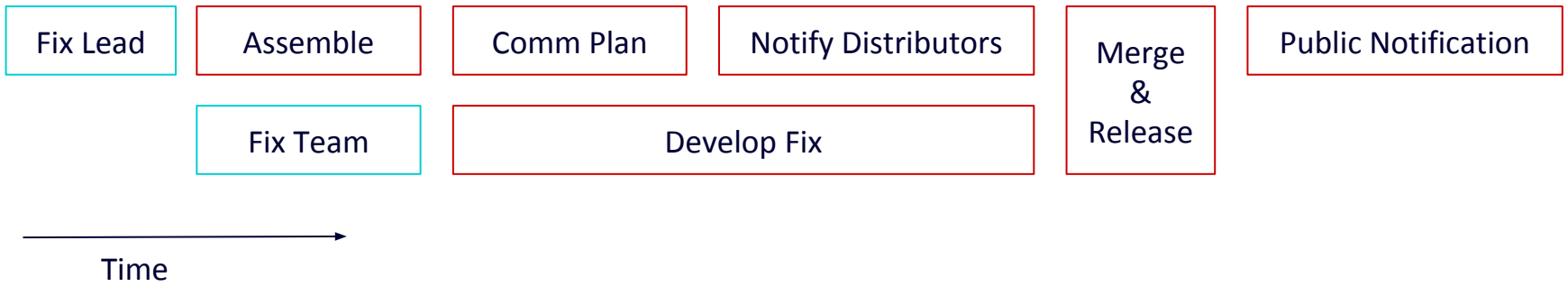
```
[root@kebe-sm-315 ~]# kubectl exec -it rate-c848c5c8b-5b8vm sh
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl kubectl ex
Defaulting container name to rate.
Use 'kubectl describe pod/rate-c848c5c8b-5b8vm -n default' to see all of the containers in this pod.
/ # df -h
Filesystem                Size      Used Available Use% Mounted on
/dev/mapper/docker-8:16-67108930-710dfe5c781bd17e11968371b9d0f84641a2efde95c68a47eddf9ae518e768d1
                         10.0G     40.3M     10.0G   0% /
tmpfs                    64.0M         0     64.0M   0% /dev
tmpfs                     9.7G         0      9.7G   0% /sys/fs/cgroup
/dev/mapper/centos-root
                         53.0G     28.6G     24.4G  54% /dev/termination-log
/dev/sdb                100.0G     40.9G     59.1G  41% /etc/resolv.conf
/dev/sdb                100.0G     40.9G     59.1G  41% /etc/hostname
/dev/mapper/centos-root
                         53.0G     28.6G     24.4G  54% /etc/hosts
shm                      64.0M      8.0K     64.0M   0% /dev/shm
tmpfs                     9.7G     12.0K      9.7G   0% /var/run/secrets/kubernetes.io/serviceaccount
tmpfs                     9.7G         0      9.7G   0% /proc/acpi
```

The HackerOne Triage Workflow

KubeCon CloudNativeCon Europe 2020 Virtual



Vuln Report: Passed to PSC



Success Metrics

Portable, extensible, open-source

BOUNTY TOTAL	INDIVIDUAL BOUNTIES	VALID REPORTS	HACKERS
Total Bounties Paid **$14,850**	Top Bounty **$5,000**	All-Time **80+**	Thanked **24**

Program launched January 2020

Vulnerabilities Found

Rate of reports has ticked up since launching the BBP.

Highlights:

CVE-2020-8557: (Medium) Pods can DOS the host by filling up /etc/hosts.

CVE-2020-8559: (Medium or High) An attacker who can modify kubelet traffic can use a malicious redirect to trick a client into operating on another pod.

How can I contribute?

Who can contribute?

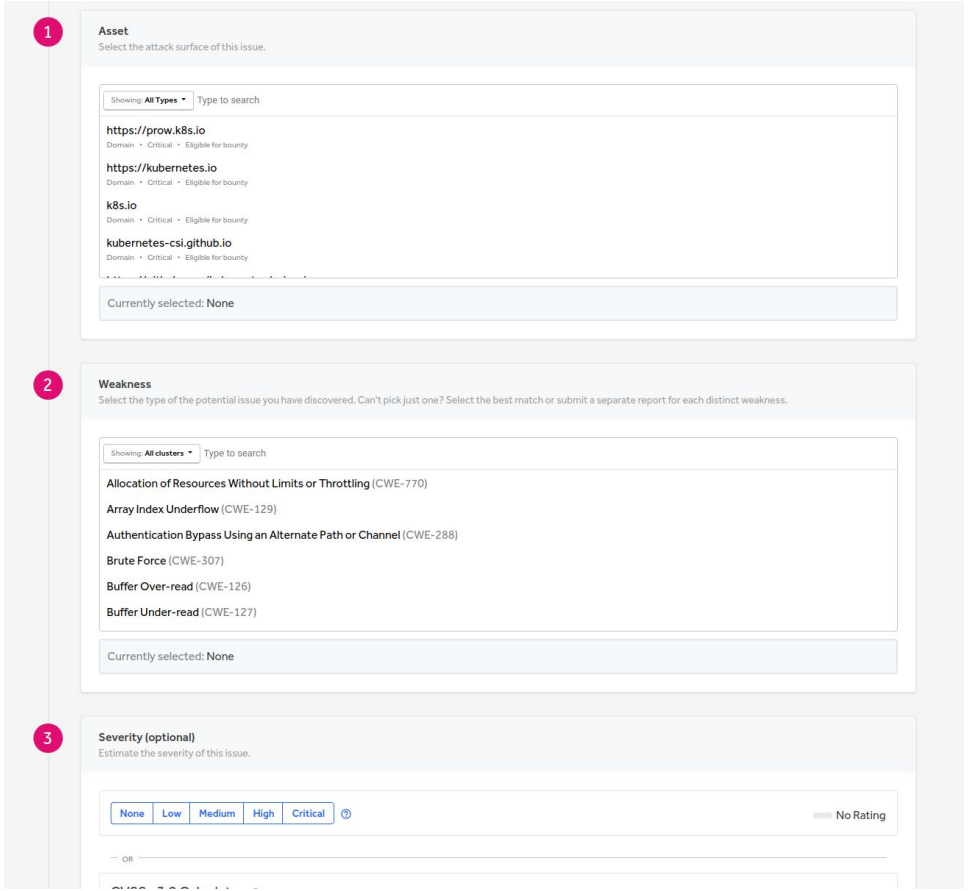
Anyone can contribute!

You don’t need to be a security wizard!

Security bugs often start as normal bugs.

Think it through; if there’s a security aspect, then submit it to hackerone.com/kubernetes

How do I submit?



What do I get for contributing?

TIER 1 (Core)	TIER 2 (Non-Core)	TIER 3 (Infra & Alpha)
Critical **$10,000**	Critical **$5,000**	Critical **$2,500**
High **$5,000**	High **$2,500**	High **$1,250**
Medium **$1,000**	Medium **$500**	Medium **$250**
Low **$200**	Low **$100**	Low **$100**

How can I stay up to date?

Kubernetes security announcements go to most channels.

For focused security announcements:

kubernetes-security-announce@googlegroups.com

What's to come for contributors?

KubeCon CloudNativeCon Europe 2020 Virtual

SIG Security is in the works.

A permanent home for the work done by the PSC.

You can join in the discussion and help establish processes for the new SIG.

Follow the discussion with SIG Auth and

kubernetes-security-discuss@googlegroups.com


KubeCon
CloudNativeCon
Europe 2020
Virtual
HELM
KEEP CLOUD NATIVE
CONNECTED