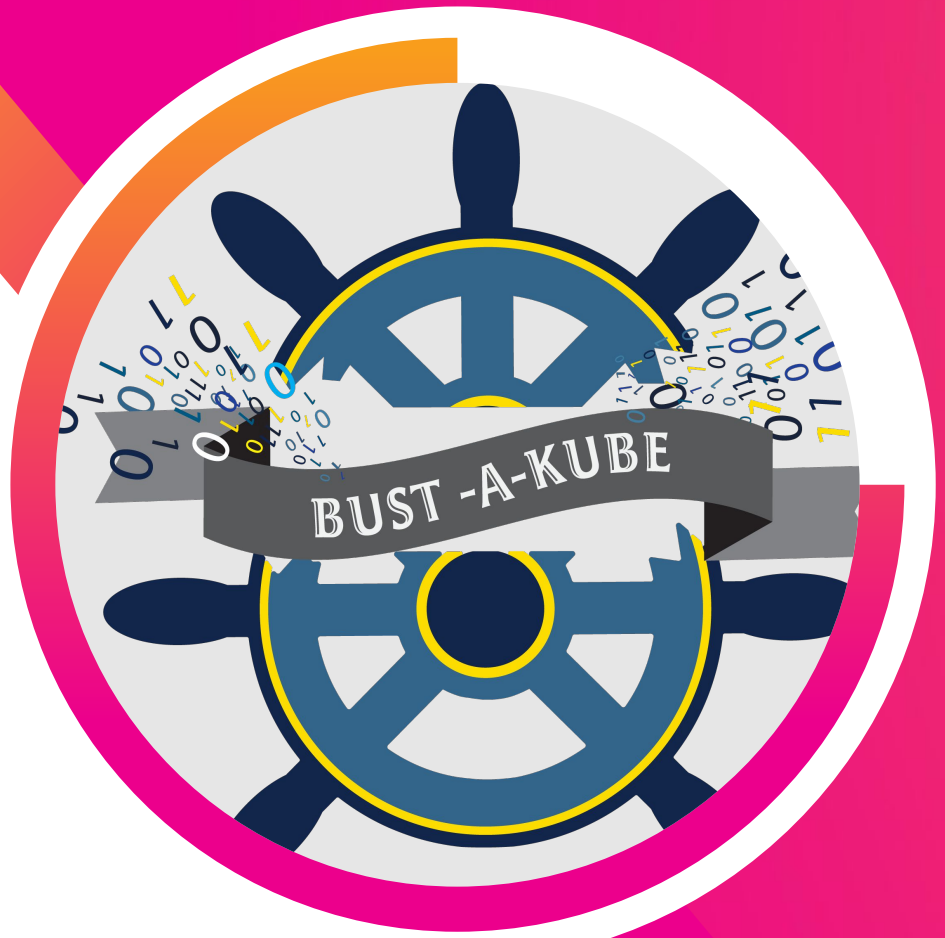
Attacking and Defending Kubernetes



A Purple Team Approach to Improving Detection Using Splunk Enterprise Security, Splunk Phantom and Peirates

Jay Beale
CTO | InGuardians.

Brian Genz
Senior Manager, Threat & Vuln Management, Splunk

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Jay Beale
CTO | InGuardians.

Brian Genz
Senior Manager, Threat & Vuln Management,
Splunk Global Security

splunk> .conf19

Where Are We Going Today?

Kubernetes – a Pre-Attack Introduction

How Do We Attack Kubernetes?

Attack Demonstration Against an Intentionally-vulnerable Kubernetes Cluster

Kubernetes Attack Demonstration with Peirates

Purple Team Methodology, Combining Attack and Defense

Detecting these Attacks with Splunk Enterprise Security

Demonstrating Detection with Splunk Enterprise Security

Demonstrating Automated Response with Splunk Phantom

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction ←
- How Do We Attack Kubernetes?
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security
- Purple Team Methodology, Combining Attack and Defense

Kubernetes

A Pre-attack introduction

splunk> .conf19

Where Did Kubernetes Come From?

Solving Google's scalability problem

Google stages a tremendous number of workloads to millions of physical servers

- 2.5 million servers (2014/2016)
- 3 billion containers per week (2014)
- Workloads crash, hard drives fail, power supplies fail

The "microservice" development model allows teams to build more complex software without falling victim to problems outlined in "The Mythical Man Month"

- Microservices means all the components of an application need to find all the others

How Does Kubernetes Solve This?

An open source software-defined data center

Explain Kubernetes Features by Describing What You Interact With

Containers started from images

Pods as the smallest unit of work

Services as the method for reaching pods

- Labeled objects instead of static-named objects

Volumes as the smallest unit of storage

Namespaces to organize it

Service accounts to authorize it

What Central Components Can We Attack?

How does the system work?

Kubernetes API Server

- Ask it to create a resource and make sure there are always 5 copies of it

ETCD State Server

- API server stores this new state in the etcd server

Controller Manager

- Run infinite control loops to make sure the state always matches the etcd server's description

Scheduler

- Bin-pack containers onto nodes

Kube-DNS

- Give every requested network endpoint (service and pod) a name

What Node Components Can We Attack?

What does a Kubernetes Node run?

Kube-Proxy

- Forwards network traffic to each member of a load-balanced network service

Container Runtime (e.g. Docker)

- Instruct the Linux kernel to create containers

Host Operating System

- Filesystem
- Network
- Kernel

Workloads

- Containers on the system

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction
- How Do We Attack Kubernetes? ←
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security
- Purple Team Methodology, Combining Attack and Defense

How Do We Attack It?

Attacking Kubernetes

splunk> .conf19

Attack Types Possible in Kubernetes

Cluster-native attacks

Ask the API Server to:

- stage containers
- change pod definitions
- allow us to MitM network traffic
- run commands in containers we don't own

Ask the Kubelet to:

- run commands in containers we don't own
- display details of all workloads running in the cluster

Attack Types Possible in Kubernetes

Cloud-only attacks

Interact with the Cloud Provider

- Obtain the node's credentials from the Metadata API
- Gain Kubernetes authentication tokens from cloud storage buckets
- Modify or create compute instances
- Modify or duplicate storage
- Interact with any API that the node's credentials allow!

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction
- How Do We Attack Kubernetes?
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster ⬅
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security
- Purple Team Methodology, Combining Attack and Defense

Attack Demonstration

Attacking the Bust-a-Kube intentionally-vulnerable Kubernetes cluster

splunk> .conf19

Demo

Review that Attack Path

How did we do that?

Gain access inside a Kubernetes cluster

- Exploited a remote code execution vulnerability in Matthew Patel's DHC web application

Attempt API server actions

- Attempt to deploy a host volume-mounting pod, but fail

Move laterally to another host

- Compromise the LLSD Deployment backend service to gain RCE in another pod

Gain another service account

- Exec into another pod via the API server

Start a host-mounting pod

- Ask the API server to start a host-mounting pod

Review that Attack Path

How did we do that?

Start host-mounting pods on all nodes

- Ask the API server to start a daemonset full of host-mounting pods

Make filesystem writes

- Modify the /etc/shadow and /etc/sudoers files on every node

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction
- How Do We Attack Kubernetes?
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security
- Purple Team Methodology, Combining Attack and Defense

Demonstrating Peirates

Attacking the Kubernetes Cluster with the Open Source Peirates Tool

splunk> .conf19

Demo

Review the Second Attack Path

How did we do that?

Gain access inside a Kubernetes cluster

- Exploited a remote code execution vulnerability in an Internet-accessible Redis server

Attempt API server actions

- Attempt to read all secrets in the cluster, but fail on most

Gain the cloud API account for a single node

- Contact the AWS Metadata API and request temporary credentials

Search the cloud storage provider for secrets and access tokens

- Discover the bootstrap certificates for the cluster in an S3 bucket

Pull an Administrative Certificate for the Cluster and Exec Into a Master Pod

- Pull the certificate from the S3 bucket, then exec into a host filesystem-mounting monitoring pod

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction
- How Do We Attack Kubernetes?
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security
- Purple Team Methodology, Combining Attack and Defense

Purple Team Methodology

Combining Attack and Defense to enable the defenders

splunk> .conf19

“Every contact leaves a trace.”

Locard’s Exchange Principle

Purple Team Methodology

Coordinated Attack, Detection & Response

Red and Blue Teams Perform “Coordinated Attack, Detection & Response”

Pre-planned attack path and execution

Working together in real time, perform the steps of the attack:

- Gain access inside a Kubernetes cluster
- Attempt API server actions
- Move laterally to another host
- Gain another service account
- Start a host-mounting pod

Blue team increases understanding of offensive technique

Red team increases awareness of attack artifacts

Document detection gaps, iterate, improve

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction
- How Do We Attack Kubernetes?
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security
- Purple Team Methodology, Combining Attack and Defense

Splunk ES Detection

Detecting the Attacks with Splunk Enterprise Security

splunk> .conf19

Splunk Enterprise Security

Analytic Stories: Adversary Tactics

Define use case: What problem are we trying to solve?

Identify log sources required for visibility for each step of the attack:

- Gain access inside a Kubernetes cluster
- Attempt API server actions
- Move laterally to another host
- Gain another service account
- Start a host-mounting pod

Identify relevant correlation searches

Surface results in notable events

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction
- How Do We Attack Kubernetes?
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security ←
- Purple Team Methodology, Combining Attack and Defense

Detection Demo

Demonstrating Detection with Splunk Enterprise Security

splunk> .conf19

Demo

© 2019 SPLUNK INC.

You Are Here

- Kubernetes – a Pre-Attack Introduction
- How Do We Attack Kubernetes?
- Attack Demonstration against an intentionally-vulnerable Kubernetes cluster
- Kubernetes Attack Demonstration with Peirates
- Detecting these Attacks with Splunk Enterprise Security
- **Demonstrating** Detection with Splunk Enterprise Security ←
- Purple Team Methodology, Combining Attack and Defense

Splunk Phantom

Demonstrating Automated Response with Splunk Phantom

splunk> .conf19

Demo

Q&A

Jay Beale | Attack Questions
Brian Genz | Detection Questions

splunk> .conf19

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION