Kubernetes Attack Surface

Kubernetes is an open-source container-orchestration system, is increasingly vital for enterprises adopting cloud technologies, microservices, and containers. Despite its benefits, Kubernetes introduces new attack surfaces, and understanding prevalent attack paths is essential for maintaining security.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	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	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)		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					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

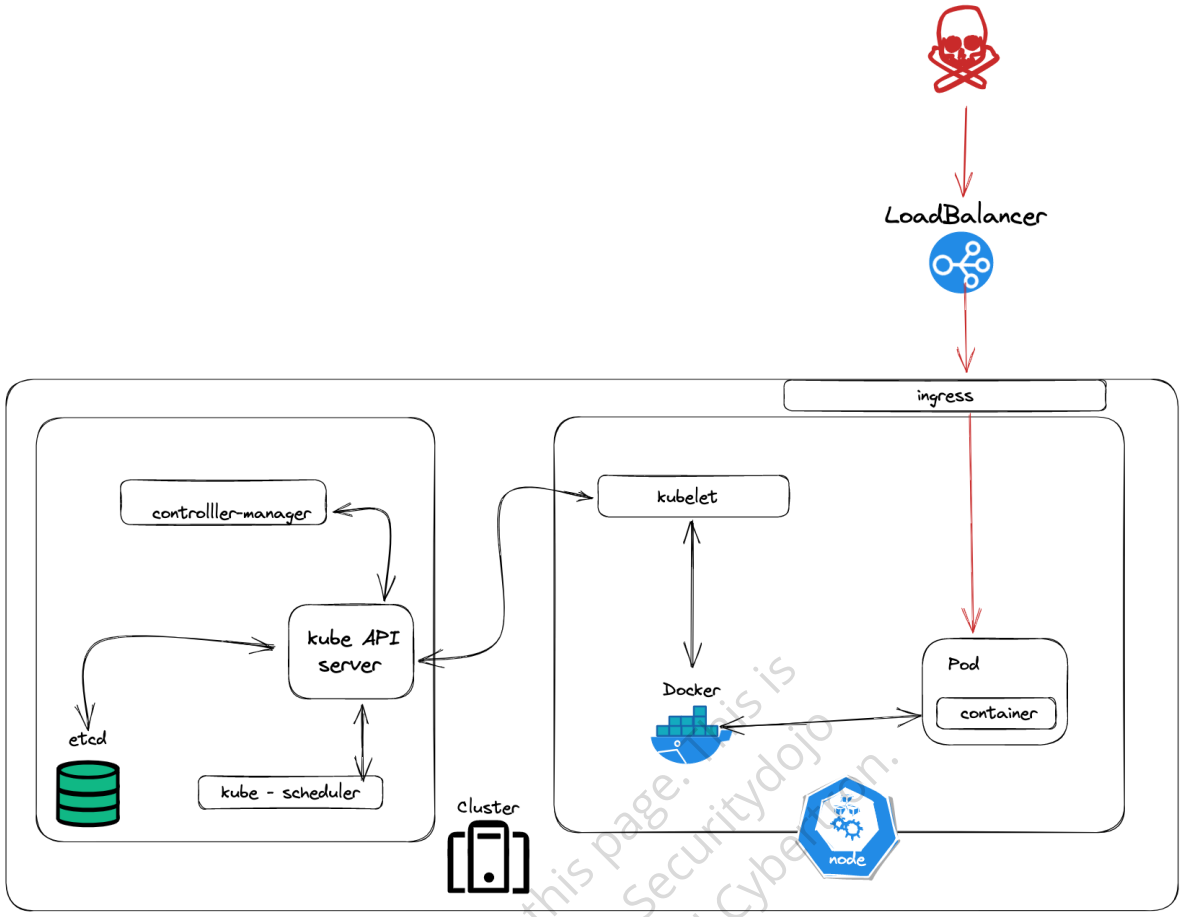
Reference: www.microsoft.com

List of Exposed Services & Ports

Port	Process	Description
443/TCP	Kube API Server	Kubernetes API Port
6443/TCP	Kubernetes API Port	Kube API Server
8443/TCP	Minikube API Port	Kube API Server
8080/TCP	Insecure K8s API Port	Kube API Server

Port	Process	Description
10250/TCP	kubelet API	Kube API Server
10251/TCP	kube-scheduler	Kube API Server
10252/TCP	Controller-manager	Kube API Server
2379/TCP	etcd Storage	etcd Client Server
2380/TCP	etcd Storage	etcd Client Server
6666/TCP	etcd Storage	etcd Client Server
4194/TCP	Container Metrics	cAdvisor
9099/TCP	calico-felix	Health Check Calico Server
6782-4/TCP	weave	Metrics and Endpoints
30000-32767/TCP	NodePort Service	Proxy to the services
10255	kubelet Service	Unauthenticated read-only HTTP port: pods, running pods and node state
10256	kube-proxy	Kube Proxy health check server
44134	Tiller	Helm service listening

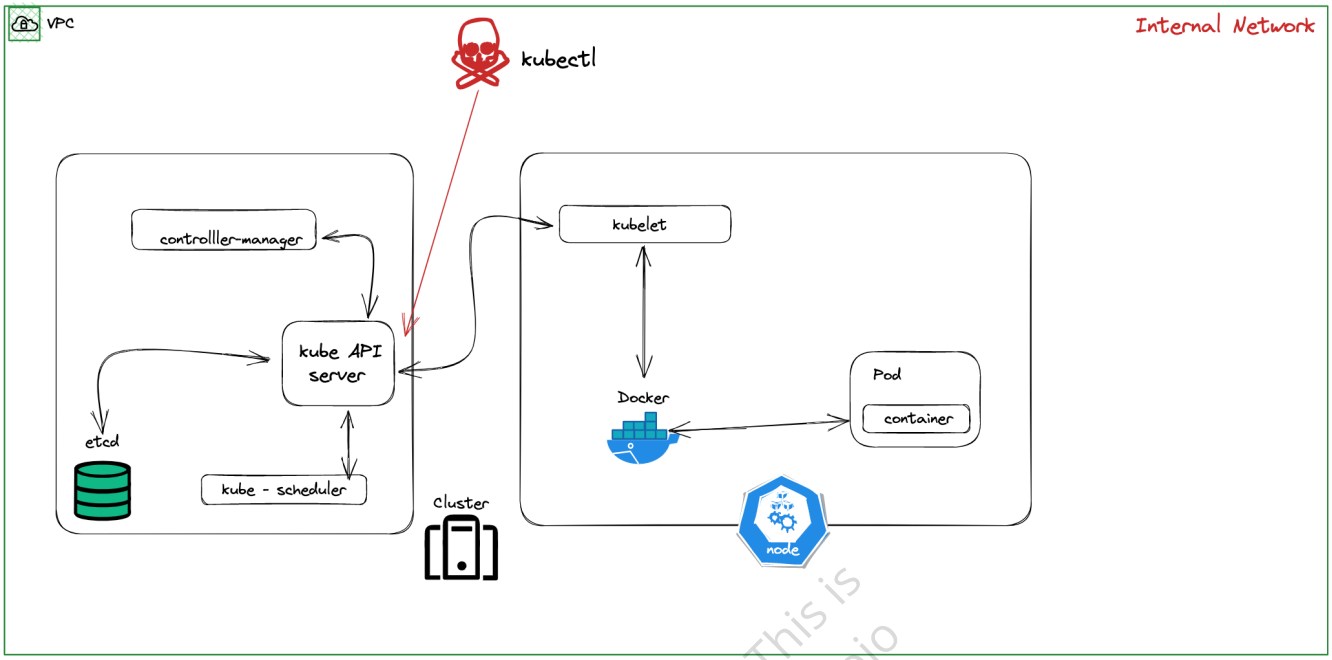
External Attack Surface



Reference: https://www.optiv.com/insights/source-zero/blog/kubernetes-attack-surface

- Kubernetes external attack surface refers to the vulnerabilities and potential points of exploitation that are reachable from outside the cluster. These are the points of entry that a hacker could employ to get unauthorized access to the cluster or its resources from the internet.
- List of key parts along with exterior attack surfaces:
    - API Server: The core of the Kubernetes control plane is the API server. If API-server is exposed it can directly lead to cluster compromise, however in cloud based kubernetes clusters, master plane is not accessible.
    - Services: The services which manages incoming traffic and the ingress controller which routes traffic to the cluster based on ingress rules. All the services which are vulnerable to any web attacks can be compromised leading to kubernetes cluster compromise.
    - Third-Party Components: Third-party components, such as Helm, monitoring tools like kubernetes dashboard, or storage providers, if misconfigured can lead to cluster compromise

Malicious Insider



- A malicious insider is someone with authorised access to a system or network, such as an employee, contractor, or business partner, who abuses that privilege to compromise the security of the Kubernetes cluster or infrastructure.
- Unusual modifications to Kubernetes resources, such as pods, services, secrets, or configmaps, which indicates compromised k8s cluster.
- Unexpected connections to external IPs or domains, or abnormal connections to internal resources in the k8s cluster.
- Unexpected or unknown processes running on a Kubernetes node or pod.
- Unusual spikes in resource usage, like CPU or memory, may suggest that an attacker is carrying out a resource-intensive attack.
- Unexpected error messages or log entries can indicate attempts by an attacker to exploit vulnerabilities in the Kubernetes software.

Reference:

- www.optiv.com
- cloud.hacktricks.xyz