Kubernetes Security (en)

Agenda

1. Starting
    - The truth about security
    - The architecture of Kubernetes
    - Architecture DeepDive
    - Layers to protect (Security)
    - AttackVectors
    - The route from development to production to secure
    - Kill Chain
2. Getting hacked
    - Why is a cluster so rewarding to hack
    - Starting with Tesla
3. Category 1 by Layer: OS / Kernel
    - Securing the OS and the Kernel
    - Kernel Hardening Checker
4. Category 2 by Layer: Cluster
    - Securing the components
    - Securing kubelet
    - Least Privileges with RBAC
    - Admission Controller
5. Category 3 by Layer: Pods Container
    - The runAs Options in SecurityContext
    - sysctls in pods/containers
    - Overview capabilities
    - Start pod without capabilities & how can we see this
    - Hacking and exploration session HostPID
    - Great but still alpha User Namespaces
6. Reaction
    - The Audit Logs
7. RBAC
    - How does RBAC work ?
    - Where does RBAC play a role ?
    - kubeconfig decode certificate
    - kubectl check your permission - can-i
    - use kubectl in pod - default service account
    - create user for kubeconfig with using certificate
    - Components / moving parts of RBAC
    - practical exercise rbac
8. Obey Security Policies (AdmissionControllers)

- Admission Controller
- PSA (PodSecurity Admission)
- Exercise with PSA
- OPA Gatekeeper 01-Overview
- OPA Gatekeeper 02-Install with Helm
- OPA Gatekeeper 03-Simple Exercise
- OPA Gatekeeper 04-Example-Job-Debug
- Connaisseur: Verifying images before Deployment

9. Pod Security

   - Automount ServiceAccounts or not ?
   - Does every pod need to access the kubenernetes api server?

10. Unprivilegierte Pods/Container

    - Which images to use ?
    - How can i debug non-root - Container/Pods?

11. The SecurityContext

    - seccomp
    - privileged/unprivileged
    - appArmor / SELinux

12. Network Policies

    - Understand NetworkPolicies
    - Exercise NetworkPolicies

13. ServiceMesh

    - Why a ServiceMesh ?
    - How does a ServiceMeshs work? (example istio
    - istio security features
    - istio-service mesh - ambient mode
    - Performance comparison - baseline,sidecar,ambient

14. Image Security

    - When to scan ?
    - Image Security Scanning

15. Documentation

    - Great video about attacking kubernetes - older, but some stuff is still applicable
    - Straight forward hacking session of kubernetes
    - github with manifests for creating bad pods