SEGURIDAD DESDE EL CÓDIGO HASTA EL RUNTIME EN CONTAINERS Y KUBERNETES

Trainer: Carol Valencia

Descripción general:

Cada módulo tendrá ejercicios prácticos para instalar las herramientas, y ejecutar scripts para probar los conceptos descritos en cada unidad.

La idea es mostrar los conceptos de seguridad en containers y kubernetes. Y usar github actions para automatizar algunos controles, instalar algunas herramientas open-source que nos ayude con el monitoreo de seguridad en containers y kubernetes.

Nivel del Training:

Intermedio

Temario:

Módulo 1: Introduction a containers

- Cloud native application
- Intro Containers
- Intro k8s
- Install docker
- Install kubernetes

Módulo 2: Container en la practica

- Construir una imagen.
- Comandos básicos para usar con container
- Networking containers
- Volumes containers
- Registrar una imagem
- Native Runtimes
- Sandboxed and Virtualized Runtimes
- Container Runtime low and high level
- OCI tools

Módulo 3: Deep en Containers - de 40 a 60 min

- Linux e Containers
- Linux System calls, permissions & capabilities
- Cgroups
- Namespaces
- Isolation in containers

Módulo 4: Container Runtimes

- container runtimes
- LXC
- rkt
- Containerd
- CRI-O

- gVisor
- Kata Containers
- Firecracker
- Open Container Initiative
- (OCI) Runtimes
- Security Inside the Container
- Security Outside the Container
- Hardening the Build Infrastructure
- Secure TRust SDC
- Docker security best practice

Módulo 5: Container Runtimes

- Security Principles
- Least Privilege
- Defense in Depth
- Reducing the Attack Surface
- Limiting the Blast Radius
- Segregation of Duties
- Container Image Misconfigurations
- Best practice to build a image (Dockerfile)

Módulo 6: Kubernetes Security

- Introduction to Kubernetes
- Kubernetes Security Design
- Logging and Auditing
- Master Hardening
- Monitoring the Cluster for Attacks
- Pod Security
- networking
- RBAC

Módulo 7: Applying Devops and Security in Containers

- Princípios e desafios de seguridad en containers. - Intro
- Automatización de controles de seguridad en el pipeline
- Vulnerabilities in Images
- Técnicas avanzadas de protección en runtime para containers

Módulo 8: Hacking containers & Kubernetes

- Reverse shell
- Fileless containers
- Crypto mining
- Demo hacking un cluster de kubernetes

Requerimientos:

Students taking Code Review should have an intermediate C Development background and hands-on experience with Linux. Hardware requirements for the class is an Internet connection as well as a laptop or workstation with a browser, SSH client and PDF viewer.

Reservá tu lugar

Costo:

USD 2.000

Reservá tu lugar

CONSULTAS

Para realizar consultas sobre el training o alguno de sus beneficios, escribir a: capacitacion@ekoparty.org

Trainer: Carol Valencia

Programadora de software interesada en las buenas prácticas de Desarrollo Seguro, Devops y despliegue de aplicaciones cloud-native con resiliencia, alta disponibilidad y seguridad. Entusiasta de comunidades de código abierto, co-organizadora de las comunidades Docker y Hashicorp en Sao Paulo. En mi tiempo libre me gusta correr y jugar tenis de playa.

Resources

- ARCHIVE: PAST EDITIONS
- CODE OF CONDUCT
- NEWSLETTER
- EKOMAGAZINE

About Ekoparty

- OVERVIEW
- CTFs & CHALLENGES
- HACKTIVITIES

- HACKTIVITIES
- SPONSORS

organizacion@ekoparty.org

 English