Container Security

DevSecOps

Agenda

- Container Security
- Container Vulnerability Scanners

Container Security

Secure DevOps

Container Security

- The usage of containers is growing every year (good report here)
- Gartner says that more than 90% of global organizations will run containerized application in production
- Most of the base images used are public available
- Docker Hub increased it's security on last years but still hard to have a hardened strategy

Container Vulnerabilities

- The Sysdig 2023 Cloud-Native Security and Usage Report reported that 87% of Container images have high-risk vulnerabilities
- In simple words, containers refer to packages of software files that contain everything needed to run an application
- Even being a container, you are exposed not only to your vulnerabilities but even on vulnerabilities of all OS components inside the container
- They are an essential step forward in modernizing applications, however, with the benefits of containers also comes the responsibility of securing them, especially container images that often contain vulnerabilities due to the use of outdated packages.

Container Vulnerability Scanners

Secure DevOps

Container vulnerability scanning

- Container vulnerability scanning is a process that uses automated tools to compare the contents of each container to a database of known vulnerabilities
- If a library or other dependency within a container image is subject to a known vulnerability, the tool will flag the image as insecure
- This scanning can be run in several moments of the DevOps flow like on developer machine, on CI/CD pipelines, on Kubernetes deployment phase, on push for Container Registry, etc.

Why is Container Security complex?

- The container ecosystem has grown significantly, which means many more components need to be checked for vulnerabilities
- The more components you add to your application, the more complex the process of checking for vulnerabilities becomes
- The complexity of containers makes them a more difficult target for developers and security researchers
- The challenge is that containers are a new technology and container security is relatively new

Container Vulnerabilities And How To Avoid Them

- Image vulnerabilities
  - The container image itself can contain vulnerabilities, such as outdated or unpatched software components
  - Avoid this by keeping your images up-to-date with the latest patches and security updates.
- Configuration vulnerabilities
  - Misconfigurations can also lead to security vulnerabilities. For example, running a container with unnecessary privileges or leaving open ports can leave your system vulnerable to attacks
  - To avoid this, it is important to follow best practices for container configuration and use tools like security scanners to detect potential issues.

Container Vulnerabilities And How To Avoid Them

- Runtime vulnerabilities
  - Once the container is running, it may still be vulnerable to attacks. For example, a container running as the root user may allow attackers to gain access to the host system.
  - To avoid this, it is important to use appropriate user permissions and to monitor the container for any suspicious activity.
- Supply chain vulnerabilities
  - Containers may contain dependencies from external sources, which can introduce vulnerabilities.
  - Avoid this by carefully reviewing and auditing any external dependencies before adding them to your container.

Types of Container Security Scanning

- Image Scans
  - Analyzes container images for vulnerabilities and misconfigurations before they are deployed
  - Image scanning tools use various methods to detect potential issues, such as analyzing software dependencies, comparing with known vulnerabilities databases, and examining system configurations
- Runtime Scans
  - Runtime scanning analyzes running containers for any changes or suspicious activities that could indicate a security breach
  - Various methods are used to monitor the behavior of running containers, such as examining system logs, network traffic, and file systems
- Configuration Scans
  - Configuration scans check container configuration settings for security issues, such as open network ports, elevated privileges, or insecure authentication mechanisms
  - Configuration scanning tools can detect misconfigurations and guide how to remediate them.

Types of Container Security Scanning

- Compliance Scans
  - Compliance scan checks containers and images against security policies, regulations, and standards such as HIPAA, PCI DSS, or GDPR
  - Deviations from these standards are detected and alerts and reports on potential compliance issues are provided.
- Dependency Scans
  - This analyzes container dependencies, such as libraries and frameworks, for known vulnerabilities and exploits
  - Outdated or vulnerable dependencies are identified and recommendations are given on how to update them.

Container Vulnerability Scanning Tools

Demo: Trivy + Snyk

Secure DevOps

Lab 07: Add Trivy to your workflow

Secure DevOps