Trivy

Trivy is an open-source vulnerability scanner specifically designed for container images and applications.

1. **Overview:** Trivy is a vulnerability scanner that focuses on container security. It is often used in DevOps and CI/CD pipelines to ensure that containerized applications are free from known vulnerabilities.

2. **Container Security:** Containers, like those created with Docker, encapsulate an application and its dependencies. Trivy scans container images for known vulnerabilities in the operating system packages, libraries, and application dependencies.

3. **Features:**

   - **Fast Scanning:** Trivy is designed to provide quick vulnerability scans, making it suitable for integration into continuous integration (CI) processes.
   - **Comprehensive Databases:** It uses vulnerability databases such as CVE, NVD, and others to identify known vulnerabilities.
   - **Ease of Use:** Trivy is designed to be user-friendly, with a simple command-line interface. It is also integrable into various CI/CD tools.
   - **Support for Multiple Languages:** Trivy is not limited to a specific programming language; it can analyze container images containing applications developed in various languages.

4. **Usage:**

   - Users typically run Trivy on container images during the development and testing stages of the software development lifecycle.
   - It can be incorporated into CI/CD pipelines to automate vulnerability scanning as part of the deployment process.

5. **Integration:**

    - Trivy can be integrated with various CI/CD tools such as Jenkins, GitLab CI, GitHub Actions, and others.
    - It provides an API that allows developers and security teams to integrate vulnerability scanning into their custom workflows.

6. **Output Formats:**

    - Trivy provides scan results in various formats, including JSON, YAML, and others, making it easy to parse and integrate into different tools.

7. **Configuration Options:**

    - Users can configure Trivy to exclude specific vulnerabilities or specify custom policies based on their security requirements.

8. **Continuous Updates:**

    - Trivy's vulnerability databases are regularly updated to include the latest security information.

To use Trivy, you would typically install it on your system, point it to a container image, and let it analyze the image for vulnerabilities. Always make sure to check the official Trivy documentation for the latest information and updates, as the tool may have evolved after my last knowledge update in January 2022.

Trivy Installation Steps

```
# Install required packages
sudo apt-get install wget apt-transport-https gnupg lsb-release

# Download Trivy public key and add it to the keyring
wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | gpg --
dearmor | sudo tee /usr/share/keyrings/trivy.gpg > /dev/null

# Add Trivy repository to sources list
echo "deb [signed-by=/usr/share/keyrings/trivy.gpg]
https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main" | sudo tee
-a /etc/apt/sources.list.d/trivy.list

# Update package information
sudo apt-get update

# Install Trivy
sudo apt-get install trivy -y
```

Execution Commands

Trivy supports various output formats, including "table," "json," "template," "sarif," "cyclonedx," "spdx," "spdx-json," "github," and "cosign-vuln."

File System Scanning

```
# Scan a specific path
trivy fs path

# Scan a folder with specific scanners
trivy fs --scanners vuln,misconfig Folder_name_OR_Path

# Scan a folder with specific severity levels
trivy fs --severity HIGH,CRITICAL Folder_name_OR_Path

# Scan a folder with specific scanners and severity levels
trivy fs --scanners vuln,misconfig --severity HIGH,CRITICAL Folder_name_OR_Path

# Export the report
trivy fs --format table -o report.html folderpath
```

Docker Image Scanning

```
# Scan a Docker image
trivy image imagename

# Scan a Docker image with specific severity levels
trivy image --severity HIGH,CRITICAL image_name

# Save the scan report to a file
trivy image --format table -o trivy_report.txt your_container_image
```

Git Repository Scanning

```
# Scan a Git repository
trivy repo repo-url

# Example: Scan a GitHub repository
trivy repo repo-url https://github.com/jaiswaladi246/Ekart.git
```

Kubernetes Cluster Scanning

```
# Scan a Kubernetes cluster and generate a summary report
trivy k8s --report summary cluster
```

Additional Notes

- The GitHub repository for the Aqua Security Scanner Jenkins plugin can be found here.
- To retrieve a list of container images used by pods in a Kubernetes cluster, you can use the following command:

```
kubectl get pods -o=jsonpath='{range
.items[*]}{.spec.containers[*].image}{"\n"}{end}'
```

- The output of the above command can be piped to Trivy for vulnerability scanning:

```
kubectl get pods -o=jsonpath='{range
.items[*]}{.spec.containers[*].image}{"\n"}{end}' | trivy image --format json -
```

This command extracts container images from pod specifications and scans them using Trivy, with the output in JSON format.