**TRIVY**

**1) what is trivy?**

Trivy is an open-source vulnerability scanner for container images, filesystems, and Git repositories. It is developed by Aqua Security and is designed to help developers and security teams identify and mitigate vulnerabilities in their applications.

**2) Installing trivy on Linux as well in Jenkins as plugin?**

$ **sudo rpm -ivh https://github.com/aquasecurity/trivy/releases/download/v0.51.4/trivy\_0.51.4\_Linux-64bit.rpm**

or

$ **docker image ---------> sudo docker pull aquasec/trivy:latest**

$ **trivy --version** for checking version

**3) why we need trivy?**

Integrating Trivy into CI/CD pipelines allows you to catch vulnerabilities during the build or deployment process. This reduces the risk of deploying vulnerable software to production.

**3) how to configure trivy in Jenkins?**

Trivy can be installed directly on the Jenkins server. it does not required any other configurations in jenkins console.

**4) how to view trivy reports?**

$ **trivy image <image-name>**------------> When you run a This command, it outputs the results directly to the terminal in tabular format. This provides a quick view of the vulnerabilities found. we can customize the output in different formats like xml, yaml, json and txt.

$ **trivy image -f json -o trivy-report.json <image-name>**-------------->when you run this command, it Provides detailed vulnerability information in JSON format, which can be useful for integration with other tools or detailed analysis.

NOTE: if you want to read the json foramt you need to install the one specific plugin ("**pipeline utility steps**")

**trivy commands:**

# Scan a container image

$ **trivy image python:3.4-alpine**

# Scan a container image from a tar archive

$ **trivy image --input ruby-3.1.tar**

# Scan local filesystem

$ **trivy fs .**

# Run in server mode

$ **trivy server**

**Trivy Scanning supported file types:**

aws [EXPERIMENTAL] Scan AWS account

config Scan config files for misconfigurations

filesystem Scan local filesystem

image Scan a container image

kubernetes [EXPERIMENTAL] Scan kubernetes cluster

repository Scan a repository

rootfs Scan rootfs

sbom Scan SBOM for vulnerabilities and licenses

vm [EXPERIMENTAL] Scan a virtual machine image

Management Commands

module Manage modules

plugin Manage plugins

Utility Commands completion Generate the autocompletion script for the specified shell

convert Convert Trivy JSON report into a different format