**Trivy Installation steps & Use cases:-** 

* It is open-source security scanner tool developed by aqua security.
* **Used for vulnaribility scanning such as:**
* Docker Container images
* File systems/folders.
* Git repositories.
* Kubernetes clusters.
* AWS
* Microconfigurations in file such as Terraform, K8s manifest yml files.
* Scan sensitive info such as token, secret and passwds.
* Software licenses.
* Trivy helps identify security issues and configurations early in the software development lifecycle.

1. Create one AWS EC2 Machine (Ubuntu t2.micro).
2. Connect using ssh connection gitbash/putty/mobaxterm.

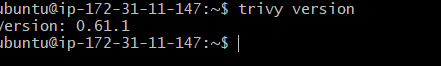
3)Go to the website link <https://trivy.dev/latest/getting-started/installation/> .

1. Click On Debian/ubuntu (official) and follow steps.

* sudo apt-get install wget gnupg
* wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | gpg --dearmor | sudo tee /usr/share/keyrings/trivy.gpg > /dev/null
* echo "deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb generic main" | sudo tee -a /etc/apt/sources.list.d/trivy.list
* sudo apt-get update
* sudo apt-get install trivy

1. Check trivy got installed.

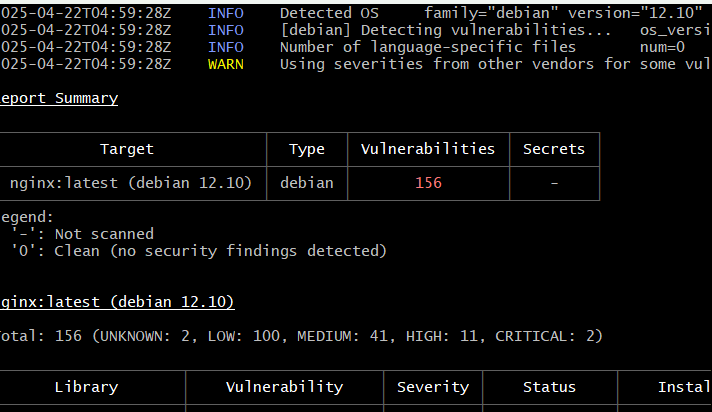
* Trivy version .



* Trivy installation successfully.

**Perform Docker Image scan locally:**

* $ Trivy image nginx:latest

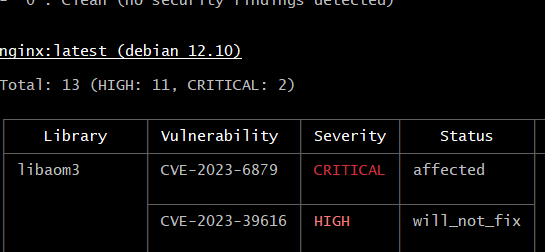


**You can pass the argument based on severity:**

$ trivy image –severity HIGH,CRITICAL,MEDIUM nginx:latest

Its filter based on criteria :

$ trivy image –severity HIGH,CRITICAL nginx:latest



**Perform scanning a Git Repo:**

$ trivy repo <https://github.com/rp2023/spring-boot-docker-app.git>

Where repo\_url in the public git repo that you want to scan.

Perform scanning a file/folder on your system locally.

Trivy fs your\_folder name

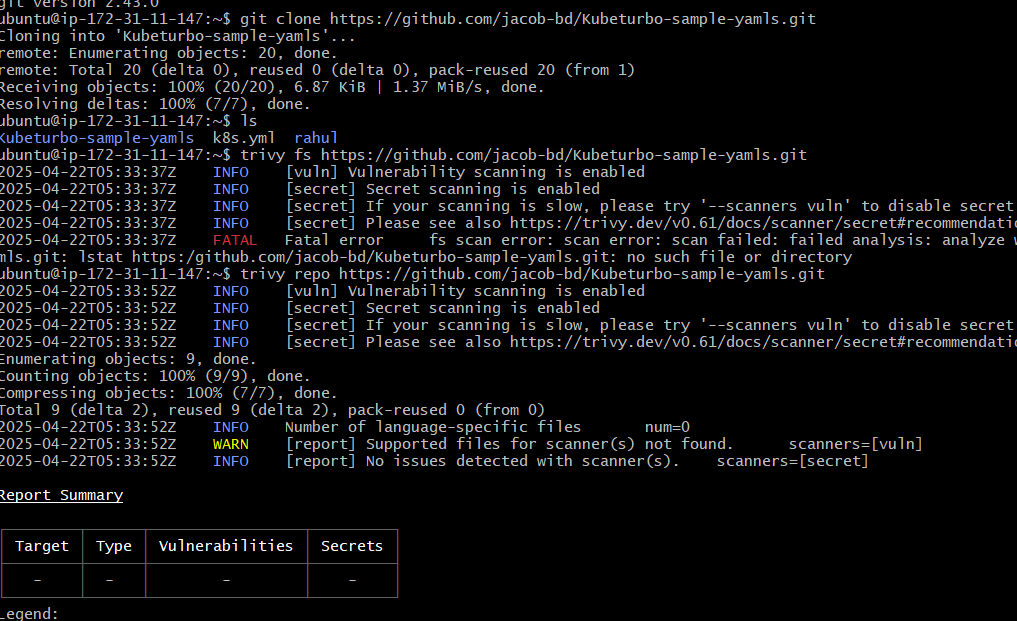
Ex:- $ mkdir rahul >> $ trivy fs rahul.

**Perform scan K8s yaml file:**

**$** trivy repo <https://github.com/jacob-bd/Kubeturbo-sample-yamls.git>

$ trivy fs --security-check vuln,config <yml filename>

$ trivy fs --security-checks vuln,config Kubeturbo-sample-yamls/

****

**Thanks….Rahul*patil***