**Lesson 06 Demo 02**

**Checking Vulnerabilities Using Trivy**

**Objective:** To scan container images for vulnerabilities using Trivy to identify and mitigate security risks and ensure that containerized applications are secure

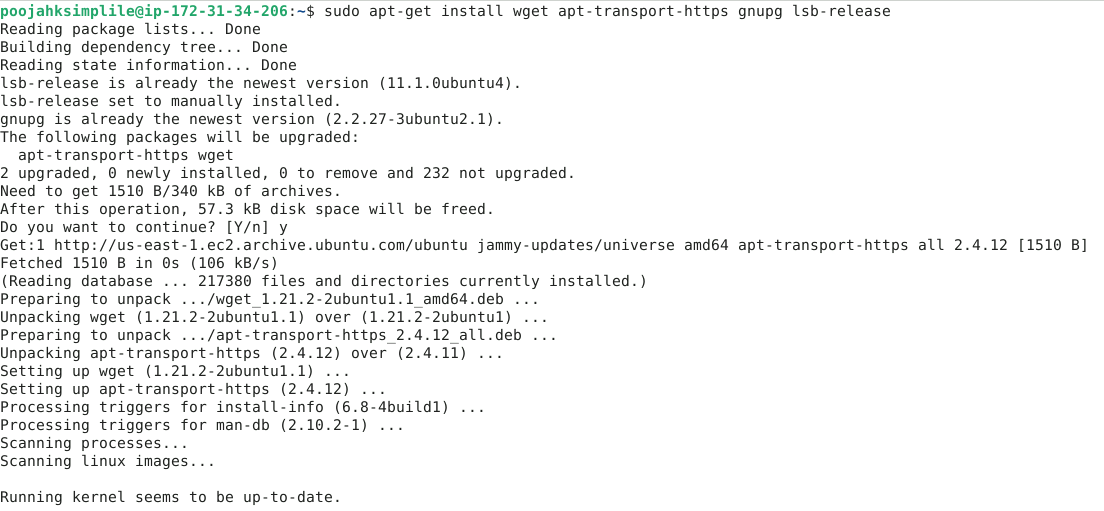
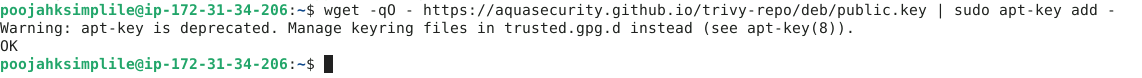
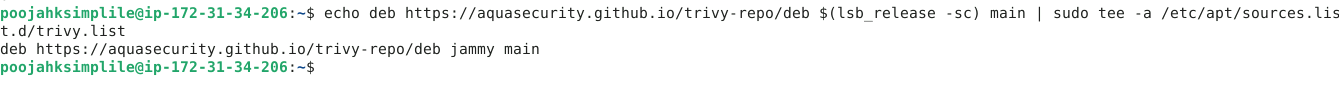
**Tools required:** Trivy

**Prerequisites:** None

Steps to be followed:

1. Install Trivy
2. Scan the vulnerabilities using Trivy

**Step 1: Install Trivy**

1. Run the following command to install tools for secure downloads, HTTPS repositories, encryption key management, and system version identification:   
   **sudo apt-get install wget apt-transport-https gnupg lsb-release**
2. Run the following command to download the Trivy repository's public key and add it to the system's trusted keys, ensuring secure package verification:  
   **wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -**  
   
3. Run the following command to add the Trivy repository to the system's sources list, enabling the installation of Trivy packages tailored to the Ubuntu version:  
   **echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb\_release -sc) main | sudo tee -a /etc/apt/sources.list.d/trivy.list**  
     
   
4. Run the following command to update the system's package lists, ensuring the latest information on available software and updates from all configured repositories:  
   **sudo apt-get update**A black and white text on a white background

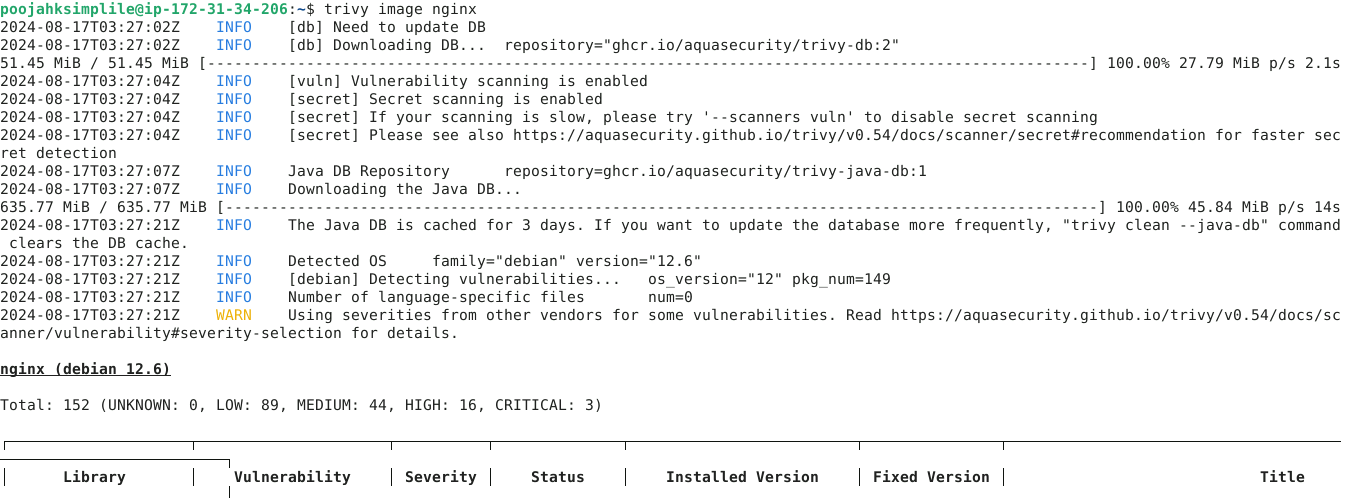
   Description automatically generated

1. Run the following command to install Trivy, a security scanner for containers, directly from the configured repository:   
   **sudo apt-get install trivy**A screenshot of a computer error

   Description automatically generated

**Step 2: Scan the vulnerabilities using Trivy**

1. Run the following command to scan the NGINX container image with Trivy for vulnerabilities and security issues:

**trivy image nginx**  
It shows the results of a Trivy security scan, listing vulnerabilities in installed packages, their severity, and whether they are affected. It also includes details like the installed version and links for more information.

A screenshot of a computer

Description automatically generated

A close up of a paper

Description automatically generated  
  
By following these steps, you have successfully scanned container images for vulnerabilities using Trivy to identify and mitigate security risks and ensure the security of containerized applications.