Lesson 06 Demo 03

Performing SAST for a Docker Image Using Snyk CLI

Objective: To download, install, and configure the Snyk command line interface (CLI) to perform SAST scan for a Docker image, enabling automatic vulnerability detection for enhanced project security

Tools required: Snyk CLI

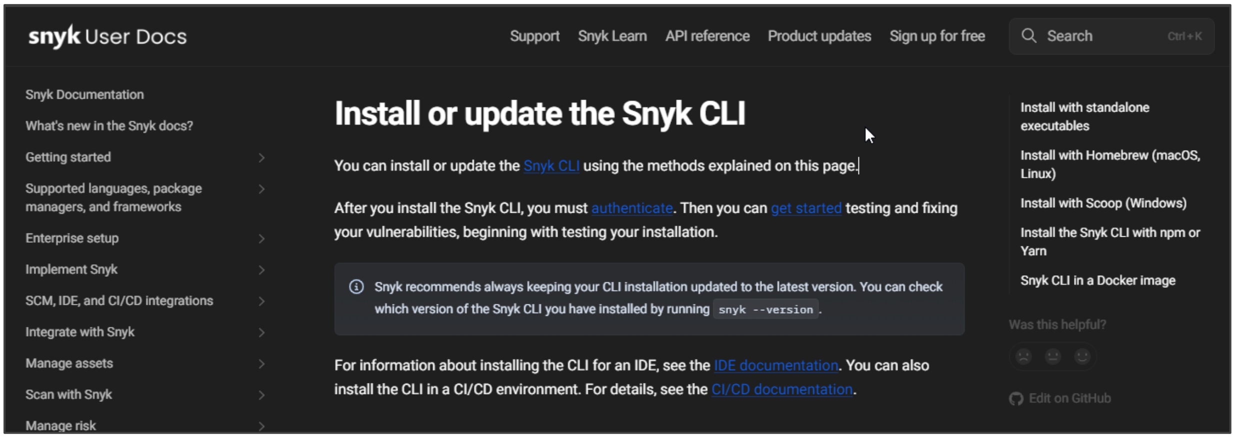
Prerequisites: None

Steps to be followed:

1. Download and install the Snyk CLI
2. Authenticate the Snyk CLI
3. Scan a Docker image

Step 1: Download and install the Snyk CLI

1.1 Visit the Snyk CLI installation guide **https://docs.snyk.io/snyk-cli/install-or-update-the-snyk-cli**


snyk User Docs
Support
Snyk Learn
API reference
Product updates
Sign up for free
Search
Ctrl + K
Snyk Documentation
What's new in the Snyk docs?
Getting started
Supported languages, package managers, and frameworks
Enterprise setup
Implement Snyk
SCM, IDE, and CI/CD integrations
Integrate with Snyk
Manage assets
Scan with Snyk
Manage risk
Install with standalone executables
Install with Homebrew (macOS, Linux)
Install with Scoop (Windows)
Install the Snyk CLI with npm or Yarn
Snyk CLI in a Docker image
Was this helpful?
Edit on GitHub

Install or update the Snyk CLI

You can install or update the Snyk CLI using the methods explained on this page.

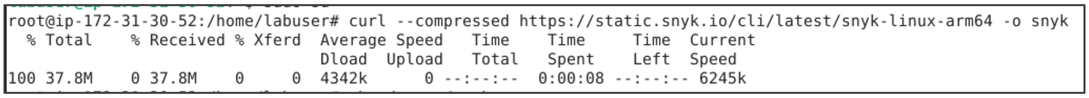
After you install the Snyk CLI, you must authenticate. Then you can get started testing and fixing your vulnerabilities, beginning with testing your installation.

Snyk recommends always keeping your CLI installation updated to the latest version. You can check which version of the Snyk CLI you have installed by running `snyk --version`.

For information about installing the CLI for an IDE, see the IDE documentation. You can also install the CLI in a CI/CD environment. For details, see the CI/CD documentation.

1.2 Run the following command to download the CLI using the curl command:

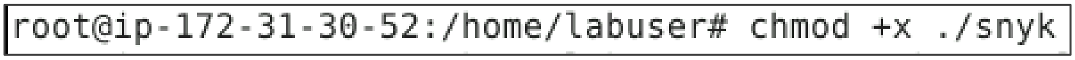
curl --compressed https://static.snyk.io/cli/latest/snyk-linux-arm64 -o snyk



```
root@ip-172-31-30-52:/home/labuser# curl --compressed https://static.snyk.io/cli/latest/snyk-linux-arm64 -o snyk
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 37.8M    0 37.8M    0     0  4342k      0 --:--:--  0:00:08 --:--:-- 6245k
```

1.3 Execute the following command to make the downloaded file executable:

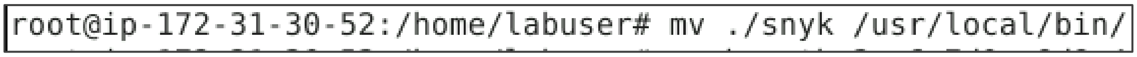
chmod +x ./snyk



```
root@ip-172-31-30-52:/home/labuser# chmod +x ./snyk
```

1.4 Run the following command to move the executable to a directory in your PATH to make it accessible:

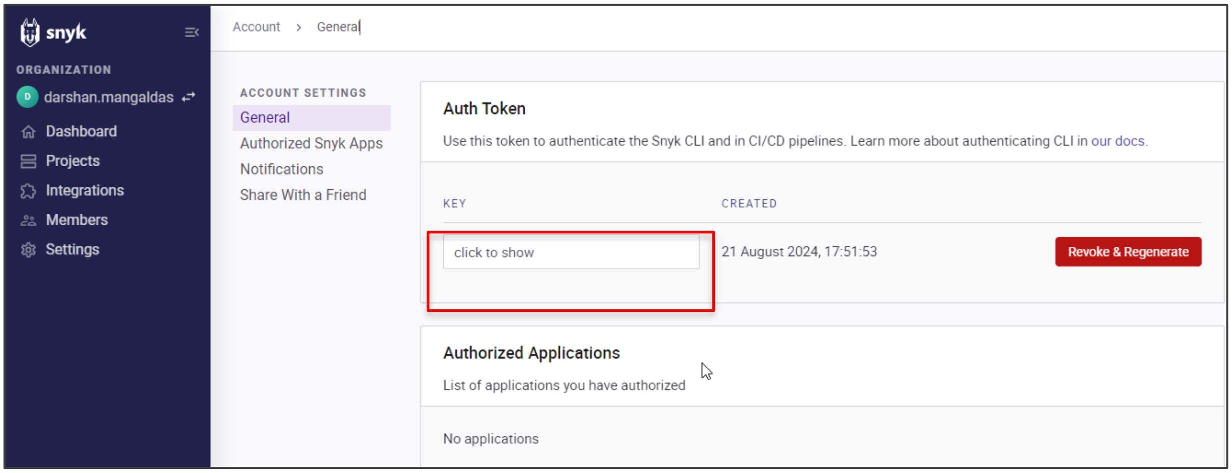
mv ./snyk /usr/local/bin/



```
root@ip-172-31-30-52:/home/labuser# mv ./snyk /usr/local/bin/
```

Step 2: Authenticate the Snyk CLI

2.1 Navigate to your Snyk account and copy the key



Auth Token

Use this token to authenticate the Snyk CLI and in CI/CD pipelines. Learn more about authenticating CLI in our docs.

KEY	CREATED
click to show	21 August 2024, 17:51:53

Authorized Applications

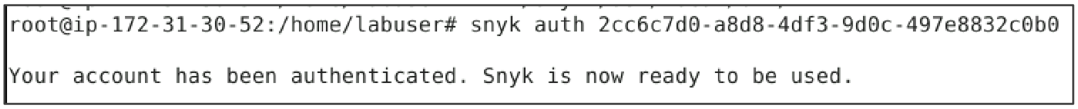
List of applications you have authorized

No applications

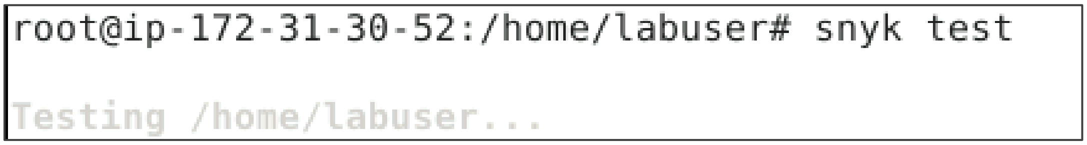
2.2 Execute the following command to set up the SNYK_TOKEN environment variable:

snyk auth <SNYK_API_TOKEN>

snyk test



```
root@ip-172-31-30-52:/home/labuser# snyk auth 2cc6c7d0-a8d8-4df3-9d0c-497e8832c0b0

Your account has been authenticated. Snyk is now ready to be used.
```

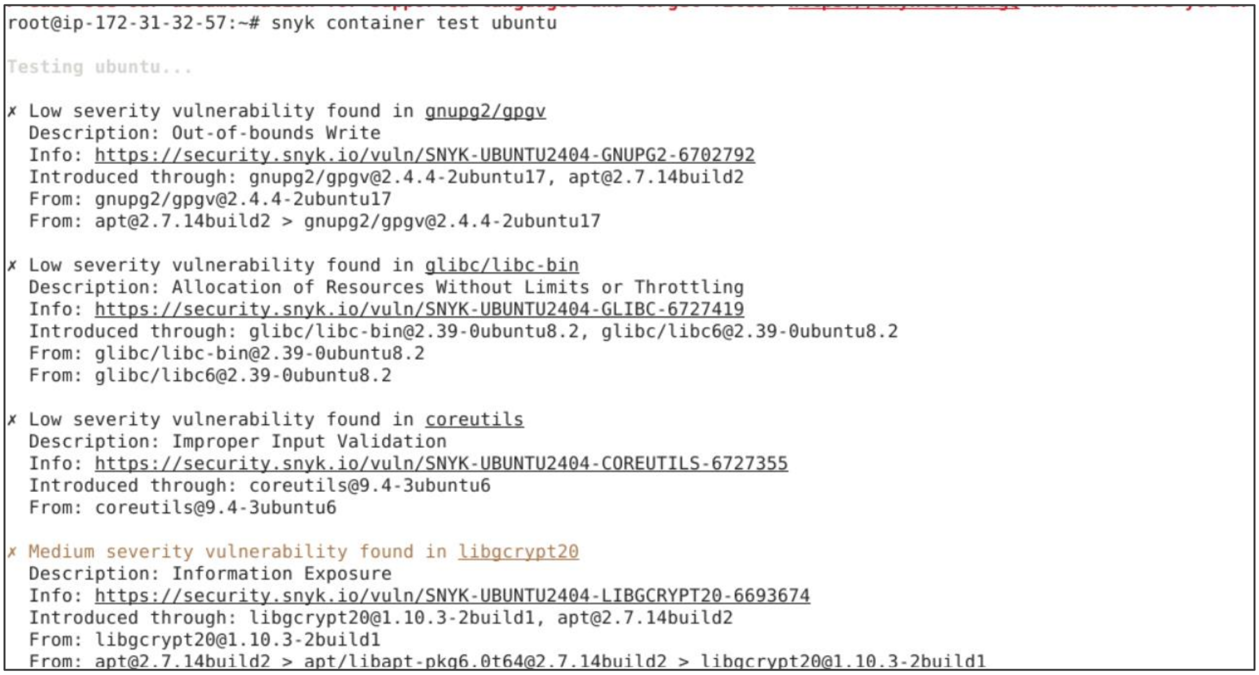


```
root@ip-172-31-30-52:/home/labuser# snyk test

Testing /home/labuser...
```

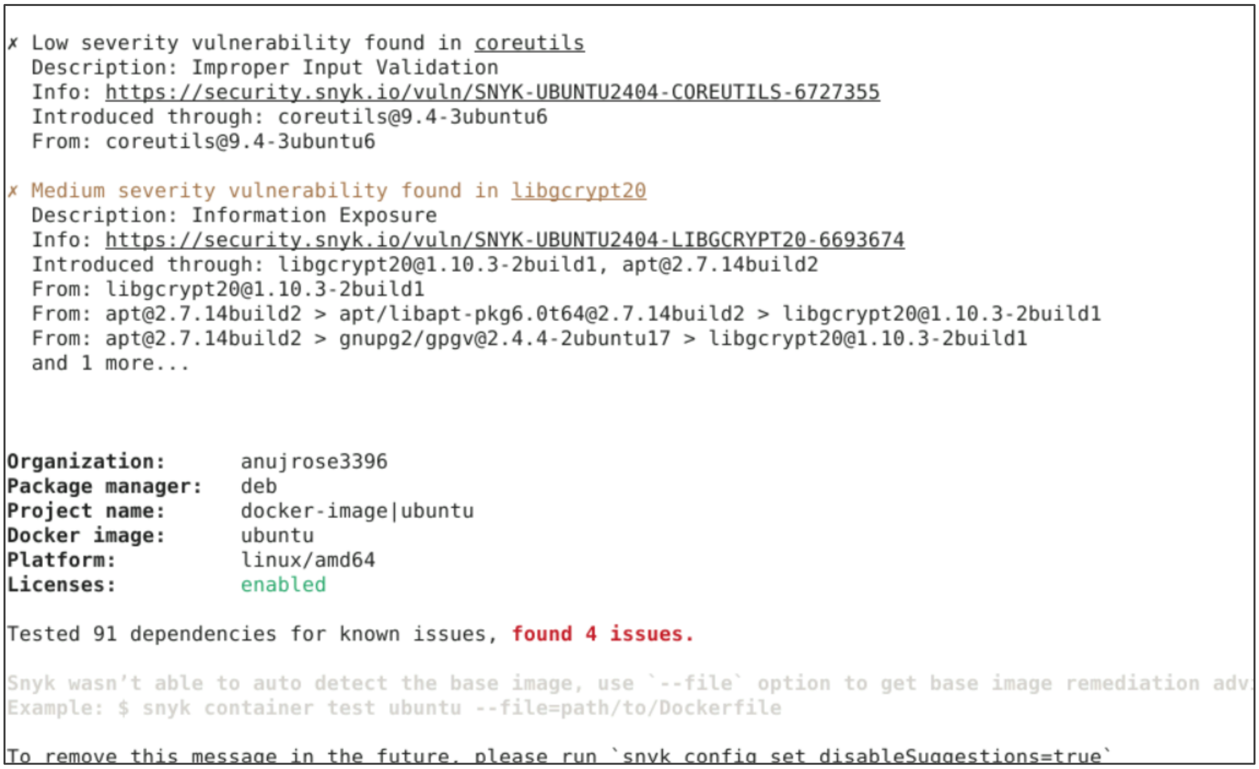
Step 3: Scan a Docker image

3.1 Run the following command to scan the Docker image named ubuntu for vulnerabilities:

snyk container test ubuntu



```
root@ip-172-31-32-57:~# snyk container test ubuntu

Testing ubuntu...

✗ Low severity vulnerability found in gnupg2/gpgv
  Description: Out-of-bounds Write
  Info: https://security.snyk.io/vuln/SNYK-UBUNTU2404-GNUPG2-6702792
  Introduced through: gnupg2/gpgv@2.4.4-2ubuntu17, apt@2.7.14build2
  From: gnupg2/gpgv@2.4.4-2ubuntu17
  From: apt@2.7.14build2 > gnupg2/gpgv@2.4.4-2ubuntu17

✗ Low severity vulnerability found in glibc/libc-bin
  Description: Allocation of Resources Without Limits or Throttling
  Info: https://security.snyk.io/vuln/SNYK-UBUNTU2404-GLIBC-6727419
  Introduced through: glibc/libc-bin@2.39-0ubuntu8.2, glibc/libc6@2.39-0ubuntu8.2
  From: glibc/libc-bin@2.39-0ubuntu8.2
  From: glibc/libc6@2.39-0ubuntu8.2

✗ Low severity vulnerability found in coreutils
  Description: Improper Input Validation
  Info: https://security.snyk.io/vuln/SNYK-UBUNTU2404-COREUTILS-6727355
  Introduced through: coreutils@9.4-3ubuntu6
  From: coreutils@9.4-3ubuntu6

✗ Medium severity vulnerability found in libgcrypt20
  Description: Information Exposure
  Info: https://security.snyk.io/vuln/SNYK-UBUNTU2404-LIBGCRYPT20-6693674
  Introduced through: libgcrypt20@1.10.3-2build1, apt@2.7.14build2
  From: libgcrypt20@1.10.3-2build1
  From: apt@2.7.14build2 > apt/libapt-pkg6.0t64@2.7.14build2 > libgcrypt20@1.10.3-2build1
```



```
✗ Low severity vulnerability found in coreutils
  Description: Improper Input Validation
  Info: https://security.snyk.io/vuln/SNYK-UBUNTU2404-COREUTILS-6727355
  Introduced through: coreutils@9.4-3ubuntu6
  From: coreutils@9.4-3ubuntu6

✗ Medium severity vulnerability found in libgcrypt20
  Description: Information Exposure
  Info: https://security.snyk.io/vuln/SNYK-UBUNTU2404-LIBGCRYPT20-6693674
  Introduced through: libgcrypt20@1.10.3-2build1, apt@2.7.14build2
  From: libgcrypt20@1.10.3-2build1
  From: apt@2.7.14build2 > apt/libapt-pkg6.0t64@2.7.14build2 > libgcrypt20@1.10.3-2build1
  From: apt@2.7.14build2 > gnupg2/gpgv@2.4.4-2ubuntu17 > libgcrypt20@1.10.3-2build1
  and 1 more...



Organization:      anujrose3396
Package manager:   deb
Project name:      docker-image|ubuntu
Docker image:      ubuntu
Platform:          linux/amd64
Licenses:          enabled

Tested 91 dependencies for known issues, found 4 issues.

Snyk wasn't able to auto detect the base image, use `--file` option to get base image remediation adv
Example: $ snyk container test ubuntu --file=path/to/Dockerfile

To remove this message in the future, please run `snyk config set disableSuggestions=true`
```

By following these steps, you have successfully installed and configured the Snyk command line interface (CLI) to perform SAST scan for a Docker image, enabling automatic vulnerability detection for enhanced project security.