Bernardo Gómez Carrasco

6. SBOM Generation Results

During this part of the lab, I generated two Software Bills of Materials (SBOMs) for the NG911 repository using Syft and Trivy. Although both tools analyze the same source code directory, they follow different SBOM standards and therefore produce outputs with different levels of detail and component counts.

SBOM Component Counts (Syft vs. Trivy)

Based on the generated SBOM files:

- Syft (SPDX JSON) reported 107 components. This number appears directly in Syft's console output, which reports: "Packages: [107 packages]"
- Trivy (CycloneDX) reported 106 components

Syft detected slightly more components than Trivy.

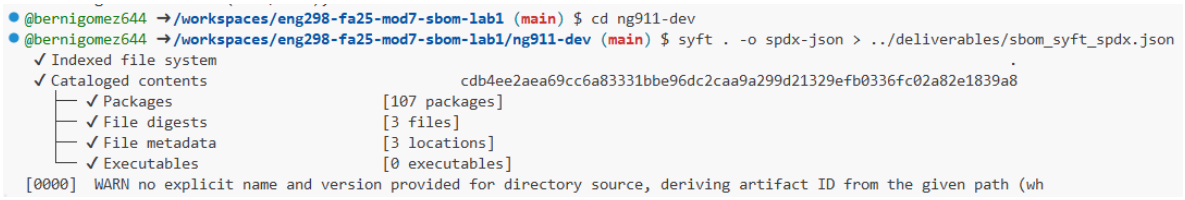
One Key Difference Between SPDX and CycloneDX SBOMs

The SPDX SBOM (Syft) uses a structured packages array with detailed metadata such as license info, originator, and multiple external references for each package.
The CycloneDX SBOM (Trivy) organizes data under a components list and focuses more on package type and PURL identifiers, with a simpler structure and fewer metadata fields.

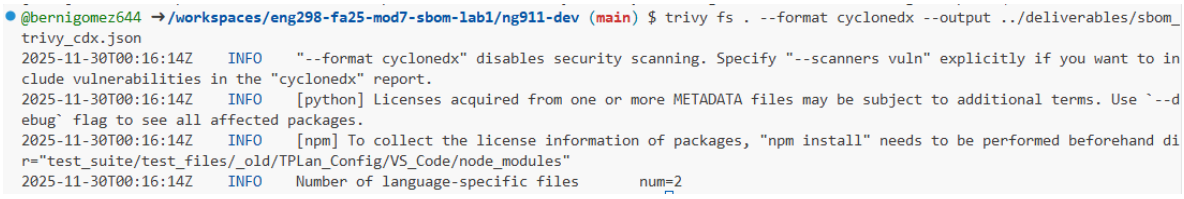
Screenshots of Terminal Output

The screenshots included in this section illustrate:

- the Syft execution, showing successful indexing of the file system and the detection of 107 packages;



- the Trivy execution, showing informational messages about license detection, npm metadata, and the generation of a CycloneDX SBOM.



These screenshots demonstrate that both tools executed successfully and produced SBOMs in the required formats.

Part 2: SBOM Vulnerability Analysis

CVE / Advisory ID	Severity	Component	Version	Comment
GHSA-79v4-65xg-pq4g	Low	cryptography	43.0.0	Input validation issue leading to potential misuse of cipher APIs.
GHSA-5rjg-fvgr-3xxf	High	setuptools	72.1.0	Command injection risk due to improper handling of package metadata.
GHSA-9hjg-9r4m-mvj7	Medium	requests	2.32.3	Possible redirect handling issue affecting request safety.
GHSA-2qfp-q593-8484	High	brotli	1.1.0	Integer overflow in Brotli compression that may allow denial of service.
GHSA-pq67-6m6q-mj2v	Medium	urllib3	2.2.2	Header parsing flaw that may weaken request integrity.

Copy the top 5 rows into your report table. Then select one CVE, locate it in the NVD Database, and summarize its cause or impact in one sentence.

GHSA-5rjg-fvgr-3xxf — A command-injection vulnerability in setuptools allows attackers to execute arbitrary commands during package installation when malicious metadata is processed.