

ABSTRACT

Docker is an open-source project that provides a platform for developers and administrators to build, package, and run applications in containers across various environments. Containers allow for the isolation of applications and their dependencies, but they also pose potential security risks if not properly managed. In the context of system security, it is essential to identify and anticipate vulnerabilities that may exist in Docker images.

As the use of containers in production environments increases, so do the associated security threats. Vulnerability scanning becomes a critical step in ensuring that the images used are free from harmful components or security flaws. However, not all scanning tools are equally effective in identifying these risks. Therefore, an evaluation of commonly used vulnerability scanners is necessary.

This study analyzes and compares two vulnerability scanning tools—OpenVAS and Docker Scout—in detecting security flaws in Docker images. The scanning process refers to the Penetration Testing Execution Standard (PTES) as a guideline for conducting security assessments. Each tool is tested on several Docker images to determine the types and number of vulnerabilities detected.

The results show that each tool has its own strengths in identifying specific types of vulnerabilities. OpenVAS excels in comprehensive system-level detection, while Docker Scout focuses more on vulnerabilities specific to Docker images. The security recommendations provided by both tools can be used to develop mitigation strategies to effectively enhance Docker container security.

Keywords: *Docker, PTES, OpenVAS, Docker Scout, Vulnerability*