What is Compliance as Code?

Compliance as Code (CAC) is an approach to automate the enforcement of (IT) compliance regulations by writing policies in a file. These policies can then be enforced or checked in an automated manner.

The following components are there in this phase:

- CAC tools i.e. Inspec, ServerSpec

People involved: Developers

External sources

- What is Compliance as Code? https://amazicworld.com/what-compliance-as-code-means-for-your-business/

Why is it important in DevSecOps?

The Compliance as Code phase makes the compliance a part of the DevSecOps pipeline and ensures that on every release, the test server adheres to the security policies defined for the project. This reduces the attack surface and obviously helps with becoming compliance-ready.

What will you learn in this section?

The user will learn to perform the following tasks

- Analyze the code of provided web applications for issues

Tools Covered

- Inspec
- ServerSpec
- OpenSCAP

Labs

- Inspec: Automating Compliance Checks
  - A Kali machine is provided to the user with inspec installed on it. The files for setting up a Tomcat server are provided in the home directory of the root user.
    Objective: Audit the given web application using the Inspec utility!
- ServerSpec: Automating Configuration Tests
  - A Kali machine with Serverspec and a remote test server machine is provided to the user. The configuration test file for this test server is kept in the home directory of the root user.
    Objective: Run tests using Serverspec to check if the remote system is configured properly!
- OpenSCAP: Automating Compliance Checks
  - A Kali machine is provided to the user with OpenSCAP installed on it. OpenSCAP uses OVAL (Open Vulnerability and Assessment Language) XML files to read the list of vulnerabilities and then check for those on the local machine. Two example OVAL XML files are stored in the home directory of the root user. One file contains CVE (Common Vulnerabilities and Exposures) definitions and the other contains the USN (Ubuntu Security Notice).
    Objective: Use Openscap to scan the Kali machine!