T9 - Security

T-SEC-901

Hardening CI/CD

devops tools now securized

0.1.2

Hardening CI/CD

- The totality of your source files, except all useless files (binary, temp files, obj files,...), must be included in your delivery.
- All the bonus files (including a potential specific Makefile) should be in a directory named *bonus*.

Hello team,

A new project that we will sell as service has just been approved by the board: an on-premise, state of the art secure infrastructure for SMEs.*
The infrastructure must be production-grade and be able to scale along with the company.

It must include the following services:

- mail,
- video conferencing,
- code version management system,
- CI/CD chain,
- Kanban board.

It is of the utmost importance that:

- all communications must be secured,
- all services must be as hardened as possible,
- an information / configuration retention system must be in place,
- the client must be able to monitor its services and hosts health,
- apart from an active directory, the client was adamant that all services used must be open-source,
- the infrastructure must be as fault-proof and secure as possible.

No need to precise that a centralized way to manage user base with a single login location is required.

You are expected to build up a fully secured private repository containing an automatic system that will deploy the whole infrastructure so that it can be redeployed.

Make sure you gave the proper access to our testers.

Alongside with this repo, you must provide:

- a self-explanatory video presentation of your solution as a whole so we can show our shareholders,
- an exploitation manual,
- a deployment manual explaining what hardening steps you have put into place and what security policies you will have designed along with the reasoning behind your choices.