CODE REVIEW: TP2

SUMMARY

In a high-stakes fantasy tech environment, the DevOps team faces a critical issue: the keystore password for the core server cluster has been lost. Without access to the keystore, vital certificates and encryption keys required for the machine reboot remain inaccessible. The challenge? Reverse-engineer the cryptographic library that secures the keystore to recover or bypass the password while maintaining the integrity of the stored secrets.

Your Mission: Your task is to analyze the jar library and to retrieve the secret key.

https://github.com/Fisjkars/CodeReview

The Zip file contains the Jar archive to reverse, a IBM JRE (it could help or not) and a keystore to validate your finding.

DELIVERABLES EXPECTED

The final report will provide a comprehensive analysis of the techniques employed to recover the lost keystore password with a detailed description of the reverse-engineering process used to analyze the cryptographic library, outlining the tools, methods, and reasoning behind each step. (decompiler, debug, instrumentation, manual reverse etc…).

The report will also include a technical breakdown of how the library secures the keystore, describing its encryption mechanisms and their implementations.