Mission SupAudit - Recherche de vulnérabilités sur les serveurs sensibles de PharmaGlass : openVAS

Le contexte

L'administrateur Derrick et ses collaborateurs ont participé à une conférence sur la sécurité informatique pilotée par le délégué régional de l'ANSSI dont l'objectif était de sensibiliser les informaticiens quant à de potentielles attaques sur des serveurs sensibles du groupe PHARMAGLASS.

Après réunion au niveau Direction Générale, Derrick décide de **mener régulièrement des audits sur certains serveurs considérés comme critiques**. Le logiciel Open Source openVAS - Open Vulnerability Assessment Scanner a été retenu.

Le plan d'action

- Vous êtes chargé, dans un premier temps, de lister les serveurs considérés comme sensibles sur l'infrastructure PharmaGlass,
- après installation d'openVAS (plusieurs options sont possibles et à étudier), vous lancer un audit de test sur un ou plusieurs serveurs,
- vous analyserez les vulnérabilités détectées par openVAS et en tirerez toutes les conclusions nécessaires et pertinentes.

Documentations

- Site officiel openVAS
- IT-Connect - openVAS
- Débuter avec Kali-Linux