DOSSIER TECHNIQUE ET FONCTIONNEL

Sommaire

Architecture logique du module

Le module d'audit d'obsolescence réseau a pour objectif d'identifier les systèmes d'exploitation présents sur un réseau et d'évaluer leur statut de support en fonction de leur cycle de vie éditeur.
Le fonctionnement repose sur cinq étapes principales :
• Acquisition des données (scan réseau via Nmap ou import CSV)
• Extraction et normalisation des systèmes d'exploitation détectés
• Interrogation d'une API publique (endoflife.date)
• Calcul dynamique du statut d'obsolescence
• Génération automatique de rapports (CSV, JSON, HTML)

Justification du choix de Nmap

Nmap a été choisi car il constitue une référence reconnue en matière de scan réseau et d'identification de systèmes d'exploitation. Il permet la détection d'OS (-O), la détection des versions de services (-sV), et l'export des résultats au format XML (-oX), facilitant leur traitement automatisé en Python.
Le choix du format XML permet une lecture structurée des données et l'extraction automatisée des informations pertinentes à l'aide de la bibliothèque xml.etree.ElementTree, assurant ainsi robustesse et fiabilité du traitement.

Gestion des droits Nmap (setcap)

Certaines fonctionnalités avancées de Nmap requièrent l'utilisation de raw sockets. Plutôt que d'exécuter l'ensemble du script avec les droits root, la commande suivante a été appliquée au binaire Nmap **:**

sudo setcap cap_net_raw,cap_net_admin,cap_net_bind_service+eip $(which nmap)

Cette approche permet à un utilisateur standard sur Linux d'exécuter le script sans privilèges administratifs, en lui accordant uniquement les capacités nécessaires pour le scan.
Elle respecte ainsi le principe du moindre privilège et améliore la sécurité globale.

Répartition par modules

Dans le cadre du projet global, ce module est dédié exclusivement à l'audit d'obsolescence des systèmes d'exploitation. Il s'intègre à l'outil global en fournissant l'analyse de conformité vis-à-vis des dates de fin de support éditeur.

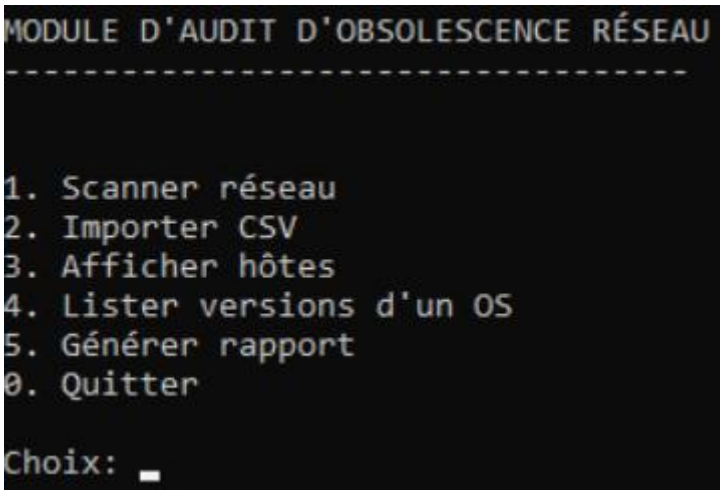
Configuration et gestion des secrets

Le module ne nécessite aucune clé API ni authentification spécifique.
L'API endoflife.date utilisée est publique et accessible sans authentification.
Les rapports générés sont automatiquement stockés dans un dossier dédié :

- Linux : ~/audit_rapports
- Windows : Documents/audit_rapports

Ergonomie du menu interactif

Le menu interactif a été conçu pour être simple et pédagogique :
1 – Scanner un réseau
2 – Importer un CSV
3 – Afficher les hôtes détectés
4 – Lister les versions d'un OS
5 – Générer un rapport
0 – Quitter



Cette approche évite l'utilisation de paramètres complexes en ligne de commande et rend l'outil accessible à un technicien système.

Démarche retenue pour l’audit d’obsolescence

La source de référence retenue est l’API publique endoflife.date. Les dates de support et de fin de vie sont récupérées dynamiquement afin de garantir une mise à jour continue des informations.
Les statuts calculés sont : SUPPORTÉ, EOL < 1 AN, EOL IMMINENT, NON SUPPORTÉ.

Compromis techniques assumés

• La détection OS via Nmap peut être imprécise. Une mention 'Vérification manuelle requise' est prévue lorsque la version n’est pas détectée.

• Dépendance à une API externe : si indisponible, les données EOL ne peuvent être récupérées.

• Le périmètre est limité aux systèmes d’exploitation et n’inclut pas les versions applicatives.

• Le rapport HTML est statique afin de privilégier portabilité et simplicité.