MANUEL D’INSTALLATION ET D’UTILISATION

Sommaire

Sommaire 2
Prérequis 3
Matériel et OS *3*
Logiciels *3*
Bibliothèques Python *3*
Installation 4
Utilisation – Mode interactif 4
Importer un CSV existant *5*
Afficher les résultats *5*
Générer des rapports *5*
Quitter *6*
Emplacement des artefacts 6

Prérequis

Avant l'installation, assurez-vous que la machine respecte les conditions suivantes :

Matériel et OS

- Machine standard sous Windows ou Linux
- Accès administrateur (Windows) ou droits pour setcap (Linux)

Logiciels

- **Python 3.6** ou supérieur
- **Nmap** installé et accessible dans le PATH
- Sur Windows : droit administrateur nécessaire pour le scan OS
- Sur Linux : pour exécuter le script sans root, appliquer la commande :

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

puis

chmod +x nom_scriptaudit

- Connexion internet pour accéder à l'API **endoflife.date**

Bibliothèques Python

Toutes les bibliothèques utilisées sont natives :

import subprocess
import xml.etree.ElementTree as ET
import json
import csv
from datetime import datetime, timedelta
from urllib.request import urlopen
import os
import re
import ssl

Aucun pip install n'est requis.

Installation

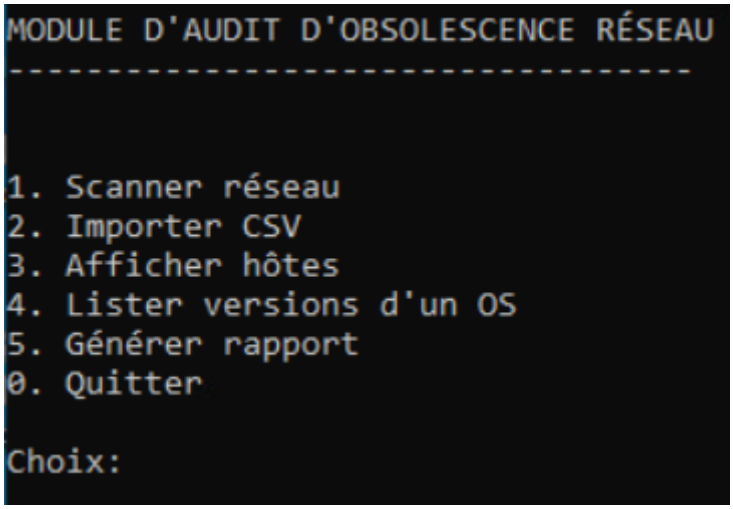
- Télécharger le script .py sur la machine.
- Vérifier que Python et Nmap sont installés et fonctionnels.
- Pour Linux, appliquer la commande setcap afin de permettre l'exécution du script par un utilisateur standard (optionnel si l'utilisateur est root).

Utilisation – Mode interactif

Lancer le script :

Python3 audit_os.py

Un menu interactif apparaît :



Scanner un réseau

Choisir l'option : 1
Entrer la plage réseau à scanner (exemple) : 192.168.1.0/24
Le script effectue :

- Scan Nmap avec détection OS
- Analyse du fichier XML généré
- Interrogation de l'API endoflife.date (avec correction SSL)
- Affichage des résultats dans la console

Importer un CSV existant

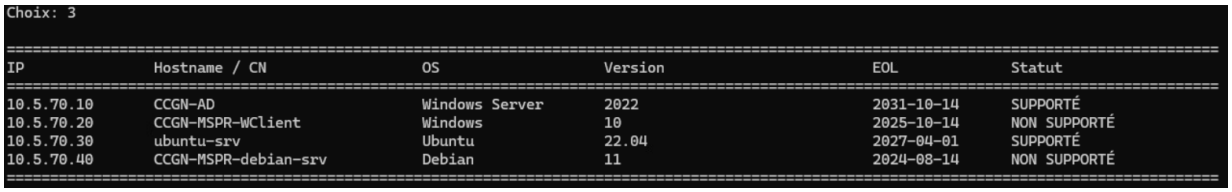
1. Choisir l'option : 2
2. Fournir le nom du fichier CSV (exemple : inventaire.csv)
3. Format attendu :

IPs	Hostname	OS_Name	OS_Version
192.168.1.10	SRV-DC01	Windows Server	2012 R2
192.168.1.20	SRV-WEB	Ubuntu	20.04

4. Le script lit le fichier et affiche les hôtes importés.

Afficher les résultats

1. Choisir l'option : 3
2. Le script affiche un tableau formaté :



```
Choix: 3

================================================================================================================================
IP              Hostname / CN                OS                  Version                   EOL             Statut
================================================================================================================================
10.5.70.10      CCGN-AD                      Windows Server      2022                      2031-10-14      SUPPORTÉ
10.5.70.20      CCGN-MSPR-WClient            Windows             10                        2025-10-14      NON SUPPORTÉ
10.5.70.30      ubuntu-srv                   Ubuntu              22.04                     2027-04-01      SUPPORTÉ
10.5.70.40      CCGN-MSPR-debian-srv         Debian              11                        2024-08-14      NON SUPPORTÉ
================================================================================================================================
```

Générer des rapports

1. Choisir l'option : 5

2. Fournir un nom de base pour les rapports (sans extension), exemple : audit_janvier_2026

3. Les fichiers sont générés dans le dossier configuré (par défaut : C:\Users\Administrateur\module3_audit\ sur Windows ou ~/audit_rapports sur Linux) :

- audit_janvier_2026.csv
- audit_janvier_2026.json
- audit_janvier_2026.html

Quitter

Choisir l’option : 0 pour fermer le script.

Emplacement des artefacts

CSV	C:\Users\Administrateur\module3_audit\ (Windows) ~/audit_rapports (Linux)
JSON	C:\Users\Administrateur\module3_audit\ (Windows) ~/audit_rapports (Linux)
HTML	C:\Users\Administrateur\module3_audit\ (Windows) ~/audit_rapports (Linux)