**Recherche Automatisée d'IoT avec Shodan**

**ATTENTION :** Ne communiquez pas directement avec les IOT utilisez uniquement Sodan pour collecter les résultats

Fonctionnalités SHODAN

Barre de Recherche : Utilisez la barre de recherche pour entrer des mots-clés, des adresses IP ou des noms de domaine. C'est ici que vous allez entrer les requêtes pour trouver des appareils IoT.

Filtres de Recherche : Juste en dessous de la barre de recherche, vous trouverez des filtres prédéfinis comme "Top Countries", "Top Cities", et "Top Organizations". Utilisez ces filtres pour voir les résultats de recherche les plus populaires par région ou organisation.

Recherche Avancée : Contient les opérateurs de recherche avancée tels que "port", "country", "org" (organisation), "has\_screenshot" (pour les appareils ayant des captures d'écran disponibles) et "product" (pour trouver des appareils d'un certain type ou marques).

Visualisation des Données : Shodan offre des options de visualisation des données telles que des cartes, des graphiques et des histogrammes. Utilisez ces outils pour obtenir une vue d'ensemble des distributions géographiques des appareils ou des tendances dans les données.

Détails de l'Appareil : En cliquant sur un résultat spécifique, vous pouvez voir les détails de l'appareil tels que l'adresse IP, le port, les services exécutés, les vulnérabilités connues et les métadonnées comme les versions de logiciel ou les en-têtes de serveur.

Recherche sauvegardée : Shodan vous permet de sauvegarder vos recherches pour les réutiliser ou les suivre ultérieurement. C'est une fonctionnalité utile pour les recherches récurrentes ou pour garder une trace de configurations spécifiques d'appareils.

API et Outils de Ligne de Commande (voir le script fourni et pip install shodan) : Shodan propose une API ainsi que des outils de ligne de commande pour automatiser et intégrer des recherches dans vos propres outils ou scripts.

Étape 1 : Création d'un Compte et Exploration de Shodan

* Inscrivez-vous sur Shodan (avec votre email étudiant)
* Lisez le document fourni : shodan.pdf
* Prenez connaissance du script shodan-exemple.py
* Récupérez votre clef d’API shodan

Introduction aux Mots-Clés et Filtres de Shodan :

Les mots-clés dans Shodan sont utilisés pour rechercher des informations spécifiques dans les données des appareils connectés à Internet. Par exemple, en cherchant "webcam", vous trouverez des appareils qui ont le terme "webcam" dans leurs données.

Filtres de Recherche :

1. title:"webcam" : Recherche des appareils ayant le mot "webcam" dans le titre de leur page web. Utile pour trouver des caméras de surveillance connectées.
2. http.title:"router" : Trouve des appareils avec le mot "router" dans le titre de leur page web. Cible spécifiquement les routeurs.
3. port:21 : Filtre les appareils ayant le port 21 (FTP) ouvert. Peut révéler des serveurs FTP accessibles.
4. default password : cherche des appareils qui pourraient avoir des mots de passe par défaut, indiquant une potentielle vulnérabilité.
5. title:"HP LaserJet" port:9100 : Recherche des imprimantes HP LaserJet avec le port 9100 ouvert, souvent utilisé pour l'impression réseau.
6. "Server: gSOAP/2.8" "GeoVision Inc." : Trouve des appareils utilisant le serveur gSOAP version 2.8 de GeoVision, potentiellement des caméras de surveillance.
7. title:"Epson" "port:80" : Cherche des imprimantes ou des scanners Epson accessibles via le port 80 (HTTP).
8. "Server: IP Webcam Server" "200 OK" : Identifie des serveurs de webcams IP, souvent des caméras de surveillance connectées.
9. html:"DVR\_H264 ActiveX" : Détecte des enregistreurs vidéo numériques (DVR) utilisant ActiveX pour le streaming vidéo, indiquant potentiellement un accès ouvert.
10. title:"VNC viewer for Java" : Recherche des interfaces VNC (contrôle à distance) accessibles via une application Java, indiquant une possible vulnérabilité.

TODO :

* Pour les mots clef ci-dessus choisissiez en 5 sur les 10 proposés en exemple ci-dessus (de 1 A 10)
  + Modifiez légèrement la recherche (ne pas faire juste un copier-coller des mot clefs SVP) et prenez une capture d’écran du résultant
  + Expliquer chaque résultat, expliquez ce que vous avez trouvé
  + Expliquer pourquoi votre résultat est sensible
  + Expliquer pourquoi ce périphérique ne devrait pas être sur internet (oui car le but est de trouver des IOT sensibles)
  + Mettez les résultats dans la partie résultats
* Utilisez Sodan pour rechercher au moins 5 autres appareils ou services IoT en utilisant des mots-clés ou des combinaisons de filtres différents.
  + Expliquer chaque résultat, expliquez ce que vous avez trouvé
  + Expliquer pourquoi votre résultat est sensible
  + Expliquer pourquoi ce périphérique ne devrait pas être sur internet (oui car le but est de trouver des IOT sensibles)
* Conclusion : J’attends donc bien 10 résultats de recherche avec leurs détails et explications.
* Documentez chaque recherche, en indiquant les mots-clés/filtres utilisés et en expliquant les résultats obtenus.

Résultats :

Requette 1 (Exemple à modifier): Mots **Clés** utilisés « ***title :webcam country:fr port:80*** »

* Explication de la pertinence du mot clé, pourquoi il a été choisi et pourquoi c’est sensible
* Capture d’écran du résultat
* Commentaire sur la capture
* Explication de pourquoi cette IOT ne devrait pas être la
* Conclusion

Partie 2 : Automatisation de la Recherche avec un Script Python

TODO : Développez un Script Python pour automatiser la Recherche :

* Utilisez la librairie Shodan pour créer un script qui automatise les recherches de mots-clés.
* Le script doit pouvoir saisir des mots-clés, exécuter la recherche et enregistrer les résultats dans un fichier.
* Utilisez une lib python de visualisation statistique, comme matplotlib ou seaborn, pour créer des graphiques représentant les données recueillies. (les marques, les ports ouverts, et toues les infro(s) importtantes)

Bonne chance ! Merci !!