Nmap

Question 1:

Votre tâche consiste à implémenter une analyse simple de découverte d'hôte à l'aide de l'outil Nmap et également à effectuer une analyse détaillée des ports sur un hôte spécifié qui prend une adresse IP cible et analyse les 1 000 premiers ports à l'aide d'une analyse TCP SYN (-sS). Imprimer les ports ouverts pour l'hôte spécifié.

Résultat:

Host: 192.168.1.1 is up
Host: 192.168.1.3 is up
Host: 192.168.1.7 is up
No open ports found for 192.168.1.3

Question 2:

Détection de version du service (-sV) et exécution de scripts NSE (Nmap Scripting Engine) par défaut (--script=default). Le but du code est d'analyser une cible spécifiée (donnée sous forme d'adresse ou de plage IP) et de fournir des informations détaillées sur les versions de service exécutées sur les ports ouverts de la cible, ainsi que les résultats de tous les scripts NSE exécutés.

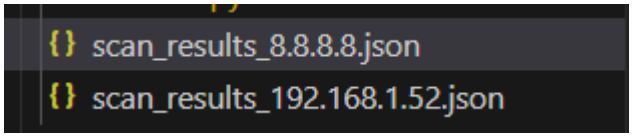
(Exemple 2)

Mettre à jour le code pour enregistrer les résultats de l'analyse au format JSON et permettre à l'utilisateur de saisir plusieurs adresses IP jusqu'à ce qu'il décide d'annuler avec Ctrl+C.

Résultat:

Enter target IP address or range (Ctrl+C to cancel): 8.8.8.8
Scan results saved to: scan_results_8.8.8.8.json
Enter target IP address or range (Ctrl+C to cancel): 192.168.1.52
Scan results saved to: scan_results_192.168.1.52.json
Enter target IP address or range (Ctrl+C to cancel):
Scan canceled. Exiting...

JSON files



Inside Json file of scan_results_8.8.8.8.json

Question 3:

Votre tâche consiste à effectuer une analyse TCP SYN pour identifier les ports ouverts, puis déterminer les ports fermés en fonction de l'analyse et enregistrer les résultats dans un format structuré (JSON). Il sert de point de départ pour créer des outils d'analyse réseau plus avancés.

Résultat:

Enter target IP address or range (Ctrl+C to exit): 127.0.0.1
Port Status:
Host: 127.0.0.1
  Port 22: open
  Port 135: open
  Port 445: open
  Port 2179: open
  Port 5357: open
  Port 7070: open
  Port 9000: open
  Port 9001: open
  Port 9002: open
  Port 9003: open
Scan results saved to: scan_results_127.0.0.1.json

Exemple résultat: