Correction du challenge 054 Zenmap

Pour rappel :
Ce tutoriel n'utilise pas de Docker et de Docker-compose.

L'utilisateur doit impérativement installer Zenmap sur sa machine (cf Tutoriel Zenmap ou sur le site officiel : https://nmap.org/download).

Challenge :
→ Nous allons utiliser Zenmap sur le nom de domaine : scanme.nmap.org
Celui-ci est utilisé spécifiquement pour les tests et la formation sur Nmap.
Il est généralement destiné à être utilisé à des fins d'apprentissage et de formation pour se familiariser avec Nmap sans violer les politiques de sécurité ou les lois applicables.

L'utilisateur doit remplir un formulaire pour réussir ce challenge.

Voici les questions/réponses :

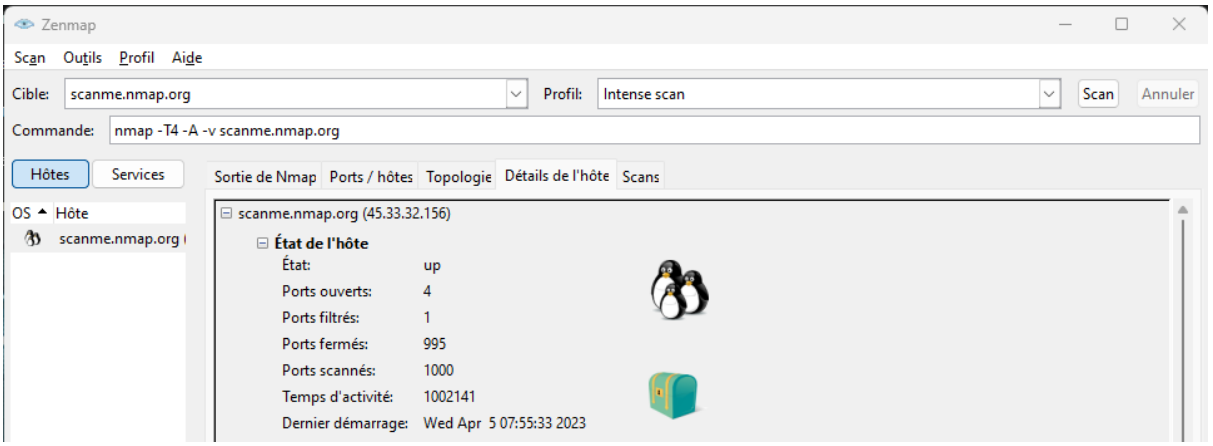
1. Quel est le nom de domaine avez-vous renseigné ?

→ scanme.nmap.org

2. Combien de types de scan (pré-enregistrés) sont disponibles dans l'outil Zenmap ?

→ 10

Pour les questions 3 à 12 : Effectuez un scan intense.



3. Quelle est la 3ème option de la commande associée à ce type de scan ? (indiquer la lettre)

→ v

4. Quelle est l'adresse IP de scanme.nmap.org ?

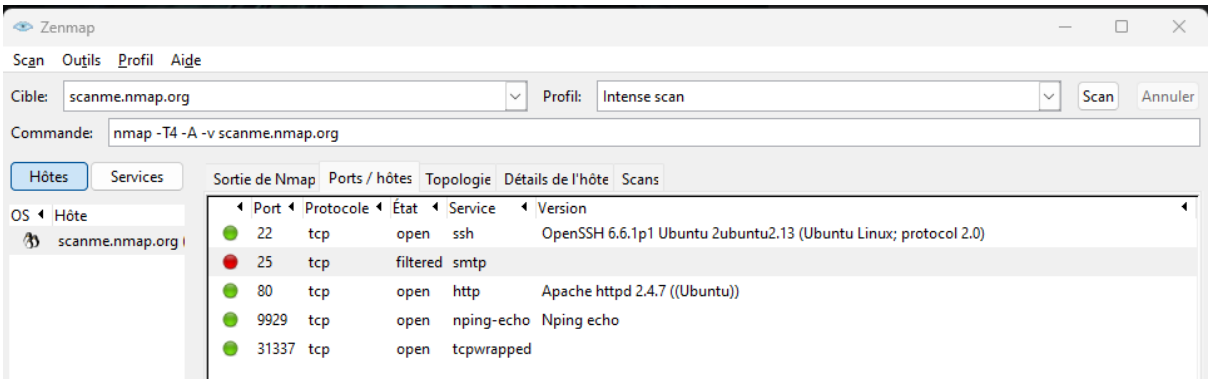
→ 45.33.32.156

5. Combien de ports sont scannés ?

→ 1000

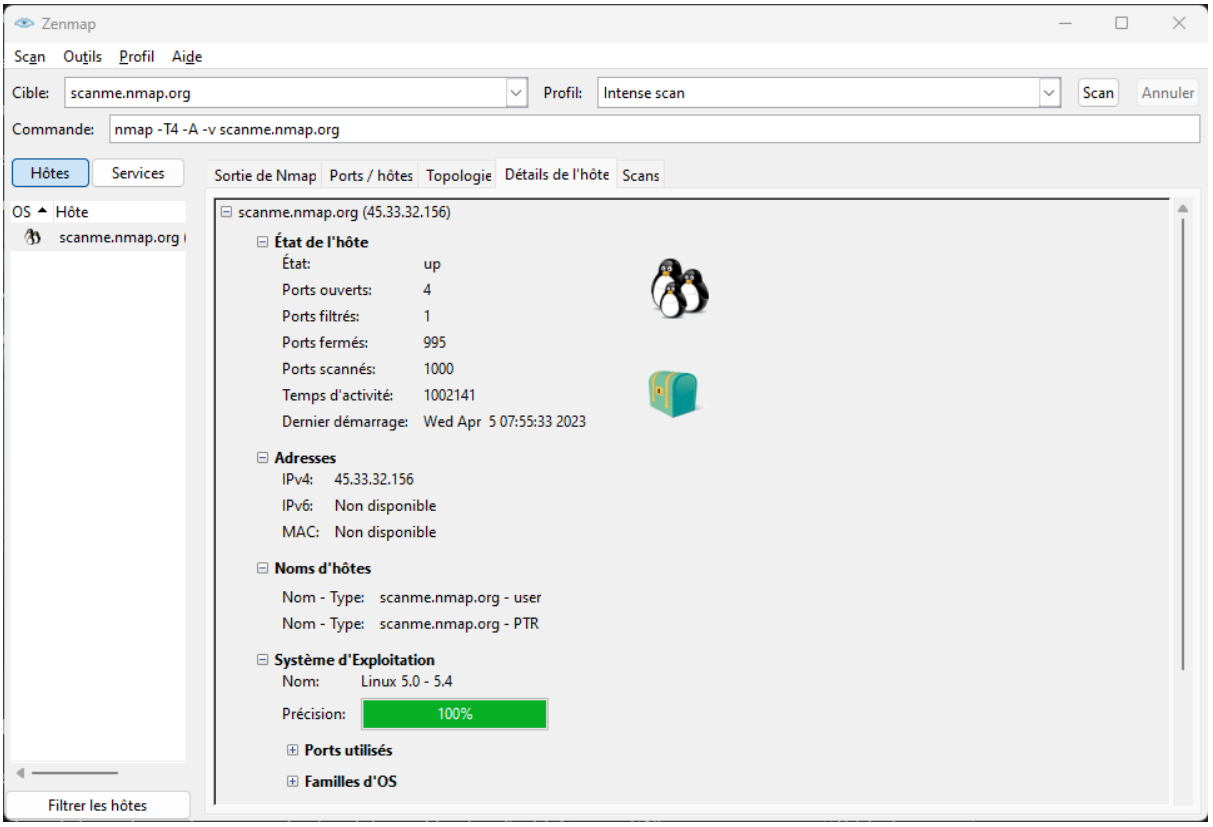
6. Combien sont ouverts ?

→ 4



7. Quelle service utilise le port 9929 ?

→ nping-echo



8. Quel est l'image associé à la cible ?

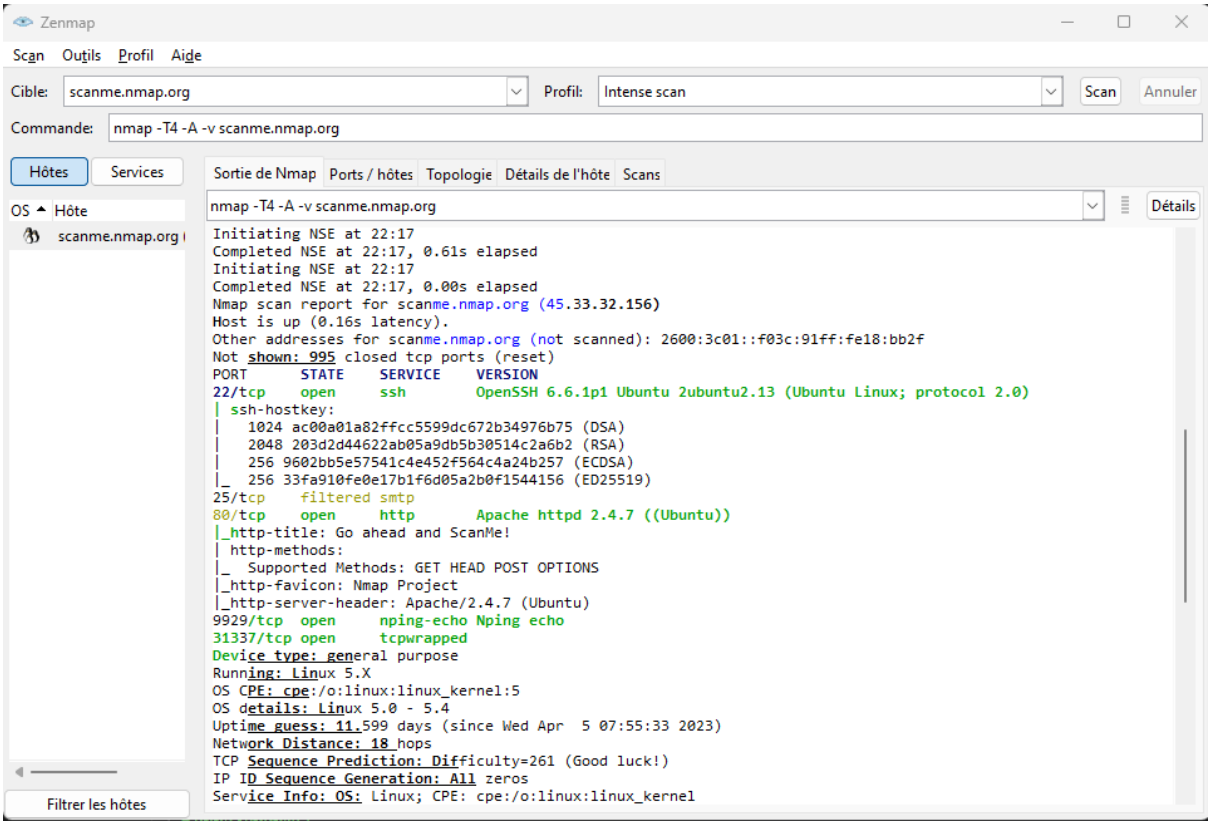
→ 3 pingouins

9. Quel OS ? (forme : xxxxxx X.X-X.X)

l→ linux 5.0-5.4

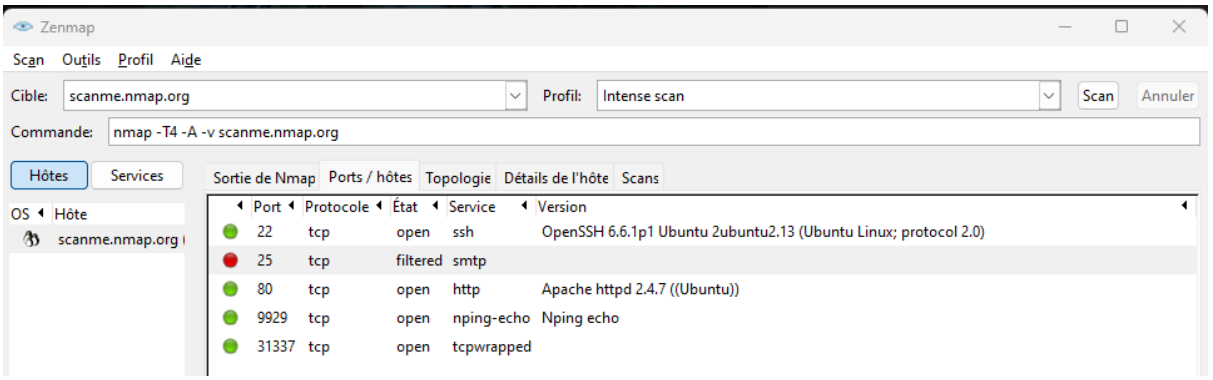
10. Quelle est le pourcentage de précision sur la détermination de l'OS ?

→ 100%



11. HTTP-TITLE du serveur Apache ? (en minuscule et sans ponctuation)

→ go ahead and scanme



12. Quel est l'état du service smtp ?

→ filtered

On obtient le flag : zenmapchallenge054

Apercçu utilisateur final :