Exam Cybersécurité

Examen à réaliser par binôme.

Exercice 1

Etudier le schéma réseau et répondre aux questions ci-dessous. Une réponse argumentée est requise pour chaque question.

1. Quelle pourrait être l'adresse IP de l'interface eth0 du routeur 2 ?
2. Où le poste de l'auditeur doit-il être connecté afin de pouvoir auditer les réseaux LAN et DMZ, et quelle pourrait être son adresse IP ? Indiquer si des contraintes particulières sont nécessaires pour que tout fonctionne comme souhaité.
3. Comment réaliser la découverte des réseaux DMZ et LAN ? Indiquer les outils et commandes à utiliser.
4. Comment scanner les ports du serveur web (donner un exemple de commande et d'adresse IP possible) ?
5. Quels ports sont susceptibles d'être ouverts sur ce type de machine (serveur web) ?
6. Si l'on se place sur internet, quelle adresse IP doit-on scanner, et quel peut être le résultat du scan de ports ?
7. Sachant que le serveur web tourne sous Windows, quels ports sont susceptibles d'être ouverts, en plus des ports 80 et 443 ?
8. Le serveur Web n'a pas été mise à jour depuis 2016. Quelle(s) vulnérabilité(s) critique(s) peut-on trouver et exploiter (vulnérabilité Windows) ?
9. Comment vérifier si un transfert de zone est possible sur le serveur DNS, et qu'est-ce que le transfert de zone ?

Exercice 2

Choisissez une VM sur TryHackMe parmis la liste suivante :

- Relevant
- Watcher
- The Marketplace
- Wekor

Réaliser un audit de la machine virtuelle choisie, et rédiger un rapport d'audit intégrant la liste des vulnérabilités découvertes et les recommandations pour les corriger.

Envoi des rapports

Envoyer vos rapports et réponses à cjoliot@soteria-lab.com avant le 19 novembre 2021 à 23h59.