Quiz sur les Vulnérabilités Réseau et Metasploit

Liens à consulter :

* <https://www.vumetric.com/fr/blogue/les-10-vulnerabilites-de-reseau-les-plus-courantes/>
* <https://www.linkedin.com/pulse/6-types-de-vuln%C3%A9rabilit%C3%A9s-informatiques-les-plus-twagirumukiza/>
* <https://drive.google.com/file/d/1qxgobH5T-YITI5x6tAiPPvpkeAE5R9sC/view>
* <https://www.oversoc.com/ressources/article/surface-dattaque-externe-les-10-vulnerabilites-les-plus-courantes>
* <https://drive.google.com/drive/folders/1gsPadbDaskjg_1HF8w2KTVVmXevX-LBi?usp=sharing>

C’est quoi le WEP ?

- <https://www.kaspersky.fr/resource-center/definitions/wep-vs-wpa>

- <https://www.netspotapp.com/fr/blog/wifi-security/wifi-encryption-and-security.html>

1. Qu'est-ce qu'une vulnérabilité de réseau ?

A. Un type de logiciel antivirus

B. Une faille ou faiblesse dans un réseau pouvant être exploitée pour obtenir un accès non autorisé

C. Une méthode de cryptage des données

D. Une politique de sécurité informatique

E. Un protocole de communication sécurisé

2. Quel protocole de sécurité sans fil est considéré comme le plus sécurisé parmi les suivants ?

A. WEP

B. WPA

C. WPA2 PSK

D. WPA2 avec authentification à deux facteurs

E. Aucun de ces protocoles

3. Quelle est la meilleure pratique pour éviter l'introduction de logiciels malveillants via des supports amovibles ?

A. Désactiver les fonctions d’exécution automatique

B. Analyser les supports avant de les connecter

C. Crypter les données sur les supports amovibles

D. Appliquer des règles strictes concernant leur utilisation

E. Toutes les réponses ci-dessus

4. Pourquoi les logiciels obsolètes représentent-ils une vulnérabilité ?

A. Ils ne sont plus compatibles avec les nouveaux matériels

B. Ils consomment plus de ressources système

C. Ils contiennent des failles de sécurité non corrigées

D. Ils sont plus lents à exécuter

E. Ils sont difficiles à installer

5. Quelle méthode d’authentification est la plus sûre pour réduire les vulnérabilités de réseau ?

A. Authentification à facteur unique

B. Utilisation de mots de passe par défaut

C. Authentification à deux facteurs (2FA)

D. Authentification à plusieurs facteurs (MFA)

E. Aucune méthode d’authentification

6. Quelles configurations de pare-feu peuvent mener à des failles de sécurité ?

A. Des règles trop strictes

B. Des configurations par défaut non modifiées

C. Des fautes de frappe dans les règles de pare-feu

D. Une maintenance régulière

E. Toutes les réponses ci-dessus

7. Quelle est l’importance de disposer de sauvegardes de données hors site ?

A. Prévenir la perte de données en cas de vol

B. Assurer une récupération rapide en cas d'attaque de ransomware

C. Faciliter le partage de fichiers

D. Améliorer les performances du réseau

E. Réduire les coûts de stockage

8. Comment les attaques par hameçonnage peuvent-elles être évitées ?

A. En cliquant sur tous les liens des emails

B. En supprimant tous les emails suspects

C. En offrant une formation de sensibilisation à la cybersécurité

D. En utilisant des mots de passe courts et simples

E. En désactivant l’antivirus

9. Quel risque est associé aux appareils mobiles connectés aux réseaux d'entreprise ?

A. Ils consomment trop de données

B. Ils peuvent être facilement perdus ou volés

C. Ils ne sont pas compatibles avec les logiciels d'entreprise

D. Ils ont une autonomie de batterie limitée

E. Ils sont difficiles à configurer

10. Qu'est-ce que l'informatique fantôme ?

A. Une technique de piratage avancée

B. Des systèmes installés sans autorisation du service informatique

C. Une méthode de sauvegarde des données

D. Un type de logiciel antivirus

E. Un protocole de sécurité réseau

11. Quel module Metasploit serait le plus approprié pour exploiter une vulnérabilité RCE dans vCenter Server ?

A. exploit/windows/smb/ms08\_067\_netapi

B. exploit/unix/ftp/vsftpd\_234\_backdoor

C. exploit/multi/http/vcenter\_rce

D. exploit/linux/local/udev\_netlink

E. exploit/windows/http/bluekeep\_rce

12. Quelle est la principale fonction de Metasploit ?

A. Scanner les réseaux pour les appareils connectés

B. Fournir une plateforme pour développer et exécuter des exploits

C. Gérer les sauvegardes de données

D. Créer des mots de passe forts

E. Configurer les pare-feu

13. Quel est le principal risque des réseaux sans fil non sécurisés ?

A. Débit Internet lent

B. Accès non autorisé par des attaquants

C. Incompatibilité avec certains appareils

D. Consommation d'énergie élevée

E. Délai de latence augmenté

14. Comment peut-on atténuer les risques liés à l'utilisation de logiciels obsolètes ?

A. Désactiver les mises à jour automatiques

B. Utiliser uniquement des logiciels open-source

C. Appliquer régulièrement les mises à jour et les correctifs

D. Limiter l'accès aux logiciels à un seul utilisateur

E. Installer un deuxième antivirus

15. Quel type de vulnérabilité est couramment exploité par les attaques par force brute ?

A. Mauvaise configuration du pare-feu

B. Logiciels obsolètes

C. Mots de passe faibles

D. Réseaux sans fil non sécurisés

E. Courriels entrants non sécurisés

16. Quelle pratique aide à sécuriser les courriels entrants ?

A. Cliquer sur tous les liens pour vérifier leur authenticité

B. Installer un logiciel de gestion des mots de passe

C. Former les employés à reconnaître les tentatives de phishing

D. Partager les mots de passe par courriel sécurisé

E. Utiliser uniquement des appareils mobiles

17. Quels sont les signes d'une mauvaise configuration du pare-feu ?

A. Faible vitesse de connexion

B. Accès bloqué à tous les services réseau

C. Accès non autorisé à des services réseau critiques

D. Messages d'erreur fréquents sur les appareils connectés

E. Problèmes de synchronisation du réseau

18. Quel est un exemple courant d'informatique fantôme ?

A. Utiliser un appareil non autorisé pour accéder au réseau

B. Installer un logiciel de sécurité sur tous les appareils

C. Configurer un VPN pour un accès distant sécurisé

D. Mettre en œuvre des sauvegardes régulières

E. Désactiver les mises à jour automatiques

19. Qu'est-ce que le module Metasploit "exploit/windows/smb/ms08\_067\_netapi" exploite ?

A. Une vulnérabilité dans le serveur vCenter

B. Une vulnérabilité dans les pare-feux mal configurés

C. Une vulnérabilité dans le protocole SMB de Windows

D. Une vulnérabilité dans les appareils mobiles

E. Une vulnérabilité dans les logiciels obsolètes

20. Quel outil peut être utilisé en conjonction avec Metasploit pour scanner les réseaux et détecter les vulnérabilités ?

A. Wireshark

B. Nmap

C. Wi-Fi Analyzer

D. SQLmap

E. John the Ripper

21. Pourquoi est-il important de crypter les données transmises sur un réseau sans fil ?

A. Pour augmenter la vitesse de connexion

B. Pour éviter les problèmes de compatibilité

C. Pour protéger les données contre les interceptions non autorisées

D. Pour améliorer la portée du signal Wi-Fi

E. Pour réduire la consommation d'énergie

22. Qu'est-ce que l'authentification multifactorielle (MFA) ?

A. Une méthode d'authentification qui nécessite plusieurs types de vérifications d'identité

B. Une méthode d'authentification basée uniquement sur des mots de passe forts

C. Une méthode de cryptage des données

D. Une méthode de sauvegarde des données hors site

E. Une méthode de configuration des pare-feu