Examen Final d'introduction à la sécurité informatique
Le 13/01/2025. Durée : 1h30

Nom et Prénom :……..……..……..

Partie 02 :Choisir la bonne réponse (il ya une seule réponse correcte)

1) L'objectif principal de l'énumération des services actifs est de :
A. Exploiter directement les failles
B. Identifier la surface d'attaque
C. Installer des backdoors
D. Créer des comptes utilisateurs

✅**Réponse : B**

2) Quel outil est le plus adapté pour identifier rapidement les ports ouverts sur une très grande plage IP ?
A. Nmap
B. Netstat
C. Masscan
D. Enum4linux

✅**Réponse : C**

3) Enum4linux cible principalement les services :
A. HTTP
B. FTP
C. SMB
D. DNS

✅**Réponse : C**

4) Pourquoi une mauvaise configuration de service actif représente-t-elle un risque critique ?
A. Elle ralentit le réseau
B. Elle augmente la charge CPU
C. Elle peut permettre une exploitation sans vulnérabilité logicielle
D. Elle empêche la journalisation

✅**Réponse : C**

5)Quelle option Nmap permet d'identifier à la fois les services, leurs versions et le système cible ?
A. `-sS`
B. `-O`
C. `-sV -O`
D. `-sU`

✅**Réponse : C**

6) SNMPwalk devient dangereux lorsqu'il est combiné avec :
A. Un IDS
B. Une communauté SNMP publique
C. Un VPN
D. Un pare-feu

✅**Réponse : B**

7) Netcat est particulièrement utile pour :
A. L'exploitation automatisée
B. La détection d'OS
C. La validation manuelle d'un service découvert
D. Le sniffing réseau

✅**Réponse : C**

8) Pourquoi Masscan n'est-il pas suffisant seul dans une phase d'audit ?
A. Il est trop lent
B. Il ne détecte pas les ports
C. Il ne fournit pas d'analyse fine des services
D. Il est obsolète

✅**Réponse : C**

9) L'énumération SMB permet à un attaquant de préparer :
A. Une attaque DoS
B. Une élévation de privilèges ou un mouvement latéral
C. Une attaque DNS
D. Une attaque physique

✅**Réponse : B**

10) Du point de vue défensif, la réduction de la surface d'attaque passe en priorité par :
A. L'ajout d'outils de scan
B. La désactivation des services inutiles
C. L'augmentation de la bande passante
D. Le chiffrement SSL uniquement

✅**Réponse : B**

11) Une vulnérabilité devient réellement dangereuse lorsqu'elle :
A. Est récente
B. Possède un exploit fonctionnel
C. Est classée faible
D. Est documentée

✅**Réponse : B**

12) Le rôle principal des bases CVE est de :
A. Fournir des correctifs
B. Standardiser l'identification des vulnérabilités
C. Lancer des exploits
D. Bloquer les attaques

✅**Réponse : B**

13) Metasploit est utilisé à la fois par :
A. Les développeurs uniquement
B. Les attaquants et les pentesters
C. Les utilisateurs finaux
D. Les antivirus

✅**Réponse : B**

14) Pourquoi l'analyse des bannières de services est-elle critique ?
A. Elle améliore la performance
B. Elle révèle parfois des versions vulnérables
C. Elle empêche l'exploitation
D. Elle chiffre les échanges

✅**Réponse : B**

15) Quel critère est le plus important pour prioriser une vulnérabilité en audit ?
A. Sa date
B. Son score CVSS uniquement
C. Son impact potentiel sur le système
D. Le langage utilisé

✅**Réponse : C**

16) Un scan actif peut être détecté car il :
A. Est passif
B. Génère du trafic identifiable
C. Ne laisse aucune trace
D. Est chiffré

✅**Réponse : B**

17) Pourquoi les correctifs réguliers réduisent-ils fortement le risque ?
A. Ils suppriment les utilisateurs
B. Ils neutralisent les exploits publics
C. Ils bloquent Internet
D. Ils empêchent les scans

✅**Réponse : B**

18) La segmentation réseau limite principalement :
A. Les attaques BIOS
B. Les attaques locales
C. Les mouvements latéraux après compromission
D. Les attaques physiques

✅**Réponse : C**

19) Une vulnérabilité sans exploit public est :
A. Sans danger
B. Impossible à exploiter
C. Potentiellement exploitable mais plus complexe
D. Déjà corrigée

✅**Réponse : C**

10) Du point de vue défensif, IDS et correctifs réguliers agissent surtout sur :
A. La prévention physique
B. La réduction de la surface d'attaque et la détection
C. Le chiffrement
D. La sauvegarde

✅**Réponse : B**

21)Une attaque BIOS/UEFI est critique car elle agit :
A. Après l'OS
B. Avant le chargement de l'OS
C. Après l'antivirus
D. Au niveau applicatif

✅**Réponse : B**

22)Un mot de passe n'est jamais stocké en clair mais sous forme de :
A. Clé privée
B. Hash
C. Certificat
D. Token

✅**Réponse : B**

23) Un keylogger logiciel permet principalement :
A. L'élévation de privilèges
B. La capture des identifiants
C. Le chiffrement
D. Le scan réseau

✅**Réponse : B**

24)Pourquoi les rainbow tables sont inefficaces contre les mots de passe salés ?
A. Elles sont lentes
B. Le sel modifie le hash final
C. Elles utilisent MD5
D. Elles nécessitent Internet

✅**Réponse : B**

25)Une attaque locale devient critique lorsque :
A. Le réseau est lent
B. Le disque n'est pas chiffré
C. Le mot de passe est long
D. Le système est à jour

✅**Réponse : B**

26) Le sniffing réseau est particulièrement dangereux si :
A. Les connexions sont chiffrées
B. Les données transitent en clair

C. Le réseau est segmenté
D. Un VPN est utilisé

☑**Réponse : B**

27)L'extraction de la base SAM sous Windows permet :
A. La mise à jour de l'OS
B. Le cracking des mots de passe
C. Le chiffrement du disque
D. La détection d'intrusions

☑**Réponse : B**

28) Pourquoi une attaque firmware est-elle difficile à éradiquer ?
A. Elle est visible
B. Elle persiste indépendamment de l'OS
C. Elle nécessite Internet
D. Elle est limitée dans le temps

☑**Réponse : B**

29) La combinaison la plus efficace contre les attaques systèmes est :
A. Antivirus seul
B. Mot de passe fort seul
C. Sécurité en couches (physique, firmware, OS, utilisateur)
D. Sauvegarde uniquement

☑**Réponse : C**

30) Du point de vue M1, l'attaque système se distingue car elle :
A. Cible uniquement les applications
B. Cible les mécanismes fondamentaux de confiance
C. Est toujours distante
D. Est facile à détecter

☑**Réponse : B**

Partie 02

Exercice 01 :(2.5 pts)

On considère le **chiffrement affine** défini sur l'alphabet de 26 lettres, avec la correspondance :

A→0, B→1, …, Z→25

1) En utilisant la clé (a = 5,; b = 8) , déchiffrer le mot **UCSEPWZY**.

Réponse

m=… $X_1^{-1}(c - X_2) \bmod 26$
……..

X_1^{-1}=……5^{-1}=21…….

U	C	S	E	P	W	Z	Y
S	**E**	**C**	**U**	**R**	**I**	**T**	**Y**

Exercice 02 :(2.5 pts)
Alice enverra une message à Bob qui a été chiffré par le chiffre de Hill dont le message chiffré est "YZPIYFKBYX"

avec la clef de cryptage la matrice $\begin{pmatrix}3 & 6\\9 & 13\end{pmatrix}$. Donnez la matrice inverse puis complétez le tableau:

$\begin{pmatrix}3 & 6\\9 & 13\end{pmatrix}^{-1} = \begin{pmatrix}13 & 16\\11 & 5\end{pmatrix}$

chiffré	Y	Z	P	I	Y	F	K	B	Y	X
claire	M	O	N	M	E	S	S	A	G	E