

Examen S1 Master 2 Sécurité Informatique

Module : Audit et Sécurité Informatique

Type : QCM (20 questions)

Q1. Selon la norme ISO/IEC 27001, un audit de sécurité est :

- A. Une attaque informatique simulée sans autorisation
- B. Un processus systématique, indépendant et documenté
- C. Une simple vérification technique des serveurs
- D. Un test automatique réalisé par des outils uniquement

✓ **Réponse : B**

Q2. Quel est l'objectif principal d'un audit de sécurité ?

- A. Pirater le système pour tester sa résistance
- B. Supprimer toutes les vulnérabilités
- C. Évaluer la conformité et l'efficacité des mesures de sécurité
- D. Installer des outils de protection

✓ **Réponse : C**

Q3. Lequel des éléments suivants relève d'un audit organisationnel ?

- A. Scan de ports avec Nmap
- B. Analyse des politiques de mots de passe
- C. Injection SQL
- D. Exploitation d'un service vulnérable

✓ **Réponse : B**

Q4. Un PenTest de type *boîte noire* signifie que :

- A. Le testeur a un accès administrateur
- B. Le testeur dispose d'informations partielles
- C. Le testeur n'a aucune information préalable
- D. Le test est limité au code source

✓ **Réponse : C**

Q5. Quel référentiel est principalement utilisé pour les vulnérabilités Web ?

- A. ISO 27001
- B. NIST CSF
- C. OWASP Top 10
- D. ITIL

✓ **Réponse : C**

Q6. Le modèle PDCA signifie :

- A. Protect – Detect – Correct – Analyze
- B. Plan – Do – Check – Act
- C. Prevent – Deploy – Control – Audit
- D. Prepare – Detect – Counter – Attack

☒ **Réponse : B**

Q7. Quelle phase du PenTest consiste à collecter des informations sur la cible ?

- A. Exploitation
- B. Élévation de privilèges
- C. Prise d'information (reconnaissance)
- D. Maintien d'accès

☒ **Réponse : C**

Q8. Quel outil est principalement utilisé pour le scan de ports réseau ?

- A. Wireshark
- B. Burp Suite
- C. Nmap
- D. Metasploit

☒ **Réponse : C**

Q9. L'ouverture du port FTP (21) représente un risque car :

- A. Il est trop lent
- B. Il transmet les données en clair
- C. Il bloque les pare-feux
- D. Il empêche la journalisation

☒ **Réponse : B**

Q10. Quelle vulnérabilité permet l'exécution de code côté serveur ?

- A. XSS
- B. CSRF
- C. RCE
- D. Clickjacking

☒ **Réponse : C**

Q11. Dans un audit, le périmètre permet de :

- A. Choisir les outils
- B. Définir ce qui est inclus ou exclu de l'audit
- C. Fixer le budget
- D. Classer les vulnérabilités

☒ **Réponse : B**

Q12. Quel rôle est responsable de la coordination globale de l'audit ?

- A. Auditeur technique
- B. Rédacteur
- C. Chef de mission
- D. Référent interne

☒ **Réponse : C**

Q13. L'analyse *Impact* × *Probabilité* permet de :

- A. Détecter les failles
- B. Mesurer la maturité
- C. Évaluer le niveau de risque
- D. Générer des correctifs

☒ **Réponse : C**

Q14. Quelle information doit obligatoirement accompagner une vulnérabilité dans le rapport ?

- A. Une estimation financière
- B. Une preuve (capture, log, scan)
- C. Une signature numérique
- D. Un correctif automatique

☒ **Réponse : B**

Q15. Le score CVSS sert à :

- A. Chiffrer les données
- B. Évaluer la criticité d'une vulnérabilité
- C. Détecter les attaques réseau
- D. Planifier les audits

☒ **Réponse : B**

Q16. Quel outil est utilisé pour analyser le trafic réseau ?

- A. Nessus
- B. Wireshark
- C. Gobuster
- D. Sqlmap

☒ **Réponse : B**

Q17. Une vulnérabilité XSS permet principalement :

- A. L'accès au système d'exploitation
- B. Le vol de sessions utilisateur
- C. L'arrêt du serveur
- D. Le chiffrement des données

☒ **Réponse : B**

Q18. Le résumé exécutif du rapport d'audit est destiné :

- A. Aux développeurs
- B. Aux auditeurs techniques
- C. À la direction
- D. Aux utilisateurs

☒ **Réponse : C**

Q19. Quelle recommandation est prioritaire face à une vulnérabilité critique ?

- A. Sensibilisation des employés
- B. Correction immédiate
- C. Audit annuel
- D. Documentation

☒ **Réponse : B**

Q20. Un audit de sécurité doit être :

- A. Ponctuel et non documenté
- B. Réalisé uniquement après une attaque
- C. Continu et intégré dans une démarche d'amélioration
- D. Automatique uniquement

✅ **Réponse : C**