CONCOURS SÉSAME

Épreuve de Compétences Digitales

Partie : Sécurité Numérique

30 questions – Niveaux facile, moyen et difficile

Référentiels : DigComp 2.2 • PIX • ANSSI • OWASP • Programme NSI/SNT

● Facile	● Moyen	● Difficile

Question 1 [Facile] – *Mots de passe*

Parmi les mots de passe suivants, lequel est le plus robuste ?

a) 123456
b) motdepasse
c) T$9kL#2mXp!qR7
d) jean2005

Question 2 [Facile] – *Logiciels malveillants*

Qu'est-ce qu'un logiciel malveillant (malware) ?

a) Un logiciel gratuit téléchargé depuis Internet
b) Un programme conçu intentionnellement pour endommager, perturber ou accéder de manière non autorisée à un système informatique
c) Un logiciel qui consomme beaucoup de mémoire RAM
d) Un programme dont l'interface graphique est mal conçue

Question 3 [Facile] – *Phishing*

Le « phishing » (hameçonnage) est une technique qui consiste à :

a) Installer un antivirus sur l'ordinateur d'un ami sans son accord
b) Envoyer un message frauduleux imitant une entité de confiance (banque, administration, etc.) pour inciter la victime à communiquer des informations personnelles ou bancaires
c) Pêcher des informations sur Wikipédia pour un exposé scolaire
d) Télécharger des mises à jour officielles du système d'exploitation

Question 4 [Facile] – *Antivirus*

Quel est le rôle principal d'un logiciel antivirus ?

a) Accélérer la connexion Internet
b) Détecter, bloquer et supprimer les logiciels malveillants (virus, chevaux de Troie, ransomwares, etc.)
c) Sauvegarder automatiquement les fichiers dans le cloud
d) Mettre en page les documents texte

Question 5 [Facile] – *Mises à jour*

Pourquoi est-il essentiel de maintenir son système d'exploitation et ses logiciels à jour ?

a) Uniquement pour bénéficier de nouvelles fonctionnalités esthétiques
b) Parce que les mises à jour corrigent des failles de sécurité (vulnérabilités) qui pourraient être exploitées par des attaquants

c) Pour augmenter la taille du disque dur

d) Parce que les logiciels expirent automatiquement après 30 jours sans mise à jour

Question 6 [Facile] – *Sauvegarde de données*

La règle de sauvegarde « 3-2-1 » recommande de :

a) Sauvegarder ses données tous les 3 jours, sur 2 clés USB et 1 disque dur

b) Conserver 3 copies de ses données, sur 2 types de supports différents, dont 1 copie hors site (en dehors du lieu habituel)

c) Utiliser 3 mots de passe différents, changer 2 fois par mois, garder 1 copie papier

d) Posséder 3 ordinateurs, 2 imprimantes et 1 scanner

Question 7 [Facile] – *Réseaux Wi-Fi*

Pourquoi est-il risqué de se connecter à un réseau Wi-Fi public non sécurisé (par exemple dans un café ou un aéroport) ?

a) Parce que la connexion sera trop rapide et pourrait endommager l'appareil

b) Parce qu'un attaquant peut intercepter les données échangées sur le réseau (identifiants, mots de passe, données bancaires…)

c) Parce que le Wi-Fi public consomme plus de batterie que le Wi-Fi domestique

d) Parce que les réseaux publics sont toujours payants

Question 8 [Facile] – *RGPD – Consentement*

Selon le RGPD, avant de collecter des données personnelles, un site web doit :

a) Envoyer un courrier postal à l'utilisateur

b) Obtenir le consentement libre, éclairé, spécifique et univoque de l'utilisateur

c) Publier une annonce dans un journal national

d) Simplement mentionner le mot « RGPD » quelque part sur le site

Question 9 [Facile] – *Pare-feu*

Quel est le rôle d'un pare-feu (firewall) dans la sécurité informatique ?

a) Empêcher physiquement le feu de se propager aux câbles réseau

b) Filtrer et contrôler le trafic réseau entrant et sortant selon des règles de sécurité prédéfinies

c) Augmenter le débit de la connexion Internet

d) Compresser les e-mails pour qu'ils prennent moins de place

Question 10 [Facile] – *Verrouillage des appareils*

Quelle est la première mesure de sécurité à mettre en place sur un smartphone ?

a) Supprimer toutes les applications préinstallées

b) Activer un mécanisme de verrouillage de l'écran (code PIN, schéma, empreinte digitale ou reconnaissance faciale)

c) Désactiver la connexion Wi-Fi de manière permanente

d) Coller un film protecteur sur l'écran

Question 11 [Moyen] – *Authentification multifacteur*

L'authentification à deux facteurs (2FA) repose sur la combinaison de deux éléments parmi trois catégories. Lesquelles ?

a) Deux mots de passe différents saisis l'un après l'autre

b) Quelque chose que l'on sait (mot de passe), quelque chose que l'on possède (téléphone, clé de sécurité) et/ou quelque chose que l'on est (biométrie)

c) Un identifiant et une adresse e-mail

d) Un code PIN et le nom de son animal de compagnie

Question 12 [Moyen] – *Chiffrement*

Quelle est la différence entre le chiffrement symétrique et le chiffrement asymétrique ?

a) Le chiffrement symétrique utilise une seule clé partagée pour chiffrer et déchiffrer, tandis que le chiffrement asymétrique utilise une paire de clés (publique et privée)

b) Le chiffrement symétrique ne fonctionne qu'avec des fichiers texte, l'asymétrique qu'avec des images

c) Le chiffrement asymétrique est toujours plus rapide que le symétrique

d) Il n'y a aucune différence, ce sont deux noms pour la même technique

Question 13 [Moyen] – *Ransomware*

Qu'est-ce qu'un rançongiciel (ransomware) et quelle est la recommandation principale en cas d'infection ?

a) Un logiciel qui optimise les performances de l'ordinateur ; il faut le mettre à jour régulièrement

b) Un logiciel malveillant qui chiffre les fichiers de la victime et exige le paiement d'une rançon ; il est recommandé de ne pas payer et de porter plainte

c) Un outil de sauvegarde automatique ; il faut acheter la version premium

d) Un programme légitime de gestion financière ; il faut y entrer ses coordonnées bancaires

Question 14 [Moyen] – *VPN*

Quel est le rôle principal d'un VPN (Virtual Private Network) ?

a) Accélérer systématiquement la vitesse de navigation sur Internet

b) Créer un tunnel chiffré entre l'appareil de l'utilisateur et un serveur distant, protégeant ainsi les données en transit et masquant l'adresse IP réelle

c) Remplacer l'antivirus et le pare-feu de l'ordinateur

d) Permettre de se connecter simultanément à plusieurs réseaux Wi-Fi

Question 15 [Moyen] – *Ingénierie sociale*

L'ingénierie sociale (social engineering) en cybersécurité désigne :

a) La conception de logiciels respectant les normes sociales et éthiques

b) L'ensemble des techniques de manipulation psychologique visant à tromper des individus pour obtenir des informations confidentielles ou un accès non autorisé

c) Le travail des ingénieurs dans le secteur des réseaux sociaux

d) L'automatisation des publications sur les réseaux sociaux

Question 16 [Moyen] – *Cookies*

En matière de sécurité et de vie privée, que sont les cookies et quel type pose le plus de problèmes de traçage ?

a) Des virus informatiques dangereux qu'il faut systématiquement supprimer

b) De petits fichiers texte déposés par les sites web sur le navigateur ; les cookies tiers (déposés par des domaines différents du site visité) permettent le traçage publicitaire inter-sites

c) Des images cachées dans les pages web qui ralentissent la navigation

d) Des mises à jour obligatoires imposées par le navigateur

Question 17 [Moyen] – *HTTPS et certificats*

Comment un utilisateur peut-il vérifier qu'un site web est sécurisé par HTTPS avant de saisir des informations sensibles ?

a) En vérifiant que le site affiche des images de cadenas dans son contenu

b) En vérifiant la présence du cadenas dans la barre d'adresse du navigateur et que l'URL commence par « https:// », puis en inspectant le certificat pour confirmer l'identité du propriétaire

c) En vérifiant que le site contient le mot « sécurisé » dans son titre

d) En vérifiant que le site ne contient aucune publicité

Question 18 [Moyen] – *Droits d'accès*

Dans un système d'exploitation, que signifie le principe du « moindre privilège » ?

a) Tous les utilisateurs doivent avoir un accès administrateur pour simplifier l'utilisation

b) Chaque utilisateur ou programme ne doit disposer que des droits strictement nécessaires à l'accomplissement de ses tâches, et pas plus

c) Il faut limiter le nombre de fichiers créés par chaque utilisateur

d) Seul le propriétaire de l'ordinateur peut créer des comptes utilisateurs

Question 19 [Moyen] – *Empreinte numérique*

Quelle est la différence entre les traces numériques volontaires et involontaires ?

a) Les traces volontaires sont celles laissées par des robots, les involontaires par des humains

b) Les traces volontaires sont les informations que l'utilisateur publie délibérément (posts, commentaires, profil), tandis que les traces involontaires sont collectées automatiquement à son insu (adresse IP, cookies, historique de navigation, géolocalisation)

c) Les traces involontaires n'existent que sur les réseaux sociaux

d) Les traces volontaires sont illégales, les traces involontaires sont légales

Question 20 [Moyen] – *Sécurité des e-mails*

Quel est le risque principal lié à l'ouverture d'une pièce jointe provenant d'un expéditeur inconnu dans un e-mail ?

a) La pièce jointe va automatiquement remplir le disque dur

b) La pièce jointe peut contenir un logiciel malveillant (virus, cheval de Troie, ransomware) qui s'exécutera à l'ouverture et infectera le système

c) L'e-mail va être automatiquement transféré à tous les contacts

d) Le navigateur web va se désinstaller

Question 21 [Difficile] – *Fonctions de hachage*

En cryptographie, qu'est-ce qu'une fonction de hachage et quelles propriétés fondamentales doit-elle posséder ?

a) Un algorithme de compression de fichiers qui réduit leur taille de moitié

b) Une fonction mathématique qui transforme une entrée de taille quelconque en une empreinte de taille fixe, devant être déterministe, résistante aux collisions et irréversible (non inversible)

c) Un programme qui trie les fichiers par ordre alphabétique sur le disque dur

d) Un protocole réseau qui accélère le transfert de données volumineuses

Question 22 [Difficile] – *Attaque par force brute*

Un mot de passe composé uniquement de 4 chiffres décimaux (0-9) offre combien de combinaisons possibles, et pourquoi est-ce insuffisant face à une attaque par force brute ?

a) 40 combinaisons ; c'est insuffisant car un ordinateur peut tester plus vite

b) 10 000 combinaisons (10^4) ; c'est insuffisant car un ordinateur moderne peut tester des millions de combinaisons par seconde

c) 1 000 000 combinaisons ; c'est suffisant pour la plupart des usages

d) 4 combinaisons ; une pour chaque chiffre

Question 23 [Difficile] – *Injection SQL*

Qu'est-ce qu'une attaque par injection SQL et comment s'en protéger ?

a) Une technique pour accélérer les requêtes SQL en injectant des index ; on s'en protège en mettant à jour le serveur SQL

b) Une attaque où l'attaquant insère du code SQL malveillant dans un champ de saisie utilisateur pour manipuler la base de données ; la protection principale est l'utilisation de requêtes paramétrées (prepared statements)

c) Un type de virus qui détruit les bases de données SQL en supprimant les tables ; la seule protection est l'antivirus

d) Une méthode de sauvegarde de base de données par injection de copies ; la protection est le chiffrement du disque dur

Question 24 [Difficile] – *Protocole TLS*

Lors de l'établissement d'une connexion HTTPS, quel mécanisme le protocole TLS utilise-t-il pour sécuriser la communication ?

a) Il envoie le mot de passe de l'utilisateur au serveur en texte clair pour vérification

b) Un handshake combinant cryptographie asymétrique (pour l'échange de clés et l'authentification du serveur) puis cryptographie symétrique (pour le chiffrement des données échangées)

c) Il masque simplement l'URL dans la barre d'adresse du navigateur

d) Il compresse les données pour qu'elles soient illisibles sans décompression

Question 25 [Difficile] – *Attaque DDoS*

Qu'est-ce qu'une attaque par déni de service distribué (DDoS) et quel est son objectif ?

a) Un virus qui supprime tous les fichiers d'un serveur

b) Une attaque coordonnée depuis de multiples sources (souvent un botnet) qui submerge un serveur ou un réseau de requêtes pour le rendre indisponible aux utilisateurs légitimes

c) Une technique de phishing ciblant simultanément plusieurs employés d'une entreprise

d) Un logiciel qui distribue les ressources réseau équitablement entre les utilisateurs

Question 26 [Difficile] – *Zero-day*

Qu'est-ce qu'une vulnérabilité « zero-day » (0-day) et pourquoi est-elle particulièrement dangereuse ?

a) Une faille qui n'existe que pendant les premières 24 heures suivant l'installation d'un logiciel

b) Une vulnérabilité inconnue de l'éditeur du logiciel et pour laquelle aucun correctif n'existe encore, ce qui signifie que les systèmes affectés sont sans protection le jour de sa découverte ou de son exploitation

c) Un type de virus qui se déclenche à minuit (jour zéro)

d) Une mise à jour qui supprime toutes les données de l'utilisateur

Question 27 [Difficile] – *Sécurité des mots de passe*

Pourquoi les mots de passe ne doivent-ils jamais être stockés en clair dans une base de données, et quelle technique de protection est recommandée ?

a) Parce que les mots de passe en clair occupent trop d'espace disque ; on recommande la compression ZIP

b) Parce qu'en cas de compromission de la base, tous les mots de passe seraient directement lisibles ; on recommande le stockage du hash salé (hash + sel aléatoire unique par mot de passe) avec un algorithme lent comme bcrypt, scrypt ou Argon2

c) Parce que les mots de passe en clair ralentissent les requêtes ; on recommande de les raccourcir

d) Parce que la loi interdit de stocker plus de 100 mots de passe par base de données

Question 28 [Difficile] – *OWASP Top 10*

Le OWASP Top 10 est une référence en matière de sécurité des applications web. Que classe-t-il et quelle catégorie est apparue en tête de l'édition 2021 ?

a) Les 10 meilleurs langages de programmation pour le web ; le premier est JavaScript

b) Les 10 risques de sécurité les plus critiques pour les applications web ; la catégorie en tête de l'édition 2021 est « Broken Access Control » (contrôle d'accès défaillant)

c) Les 10 navigateurs web les plus sécurisés ; le premier est Google Chrome

d) Les 10 entreprises les plus performantes en cybersécurité ; la première est Microsoft

Question 29 [Difficile] – *Cryptographie à clé publique – Diffie-Hellman*

Le protocole d'échange de clés Diffie-Hellman permet à deux parties de :

a) S'envoyer mutuellement leurs mots de passe en clair de manière sécurisée

b) Établir un secret partagé (clé symétrique) en échangeant uniquement des informations publiques sur un canal non sécurisé, grâce à des opérations mathématiques dans un groupe cyclique

c) Compresser des fichiers volumineux pour les transférer plus rapidement

d) Créer un réseau privé virtuel (VPN) sans aucun logiciel

Question 30 [Difficile] – *Analyse de risques – Méthode EBIOS*

En matière de gestion de la sécurité des systèmes d'information, qu'est-ce que la méthode EBIOS Risk Manager ?

a) Un logiciel antivirus développé par l'État français

b) Une méthode d'analyse de risques numériques développée par l'ANSSI, qui permet d'identifier et d'évaluer les risques cyber en étudiant les sources de menaces, les événements redoutés et les scénarios d'attaque afin de définir des mesures de sécurité proportionnées

c) Un protocole de chiffrement utilisé par les administrations françaises

d) Un système d'exploitation sécurisé réservé au ministère de la Défense