# CONCOURS SÉSAME

# Épreuve de Compétences Digitales

## Partie : Sécurité Numérique

30 questions corrigées – 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

✅ **Réponse correcte : c)**

**Explication :**
Un mot de passe robuste doit être long (au moins 12 caractères selon les recommandations de l'ANSSI), complexe (mélange de majuscules, minuscules, chiffres et caractères spéciaux) et imprévisible (ne contenant ni mot du dictionnaire, ni information personnelle). Le choix (c) « T$9kL#2mXp!qR7 » remplit tous ces critères : 14 caractères, mélange de 4 types de caractères, aucun mot identifiable. Les choix (a) et (b) figurent dans le top 10 des mots de passe les plus piratés au monde. Le choix (d) contient un prénom et une année de naissance, facilement devinables par ingénierie sociale. Référence : ANSSI, guide des bonnes pratiques ; DigComp 2.2, compétence 4.1 « Protéger les appareils » ; PIX domaine 4.

---

### 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

✅ **Réponse correcte : b)**

**Explication :**
Un logiciel malveillant (malware, contraction de « malicious software ») est un programme informatique développé dans le but de nuire : voler des données, endommager des fichiers, espionner l'utilisateur, prendre le contrôle du système, etc. Les principales catégories incluent : les virus (se propagent en infectant d'autres fichiers), les vers (se propagent via le réseau sans fichier hôte), les chevaux de Troie (se déguisent en logiciel légitime), les rançongiciels (chiffrent les données et demandent une rançon), les logiciels espions (spyware), les enregistreurs de frappe (keyloggers) et les adwares. Un logiciel gratuit (a) n'est pas forcément malveillant. La consommation de RAM (c) et une mauvaise interface (d) ne caractérisent pas un malware. Référence : ANSSI ; DigComp 2.2, compétence 4.1 ; PIX domaine 4, compétence 4.1.

---

### 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

✅ **Réponse correcte : b)**

**Explication :**
Le phishing (hameçonnage) est une technique d'ingénierie sociale très répandue. L'attaquant envoie un e-mail, un SMS (« smishing ») ou un message vocal (« vishing ») imitant une organisation légitime (banque, impôts, assurance maladie, opérateur téléphonique, plateforme en ligne…). Le message contient généralement un lien vers un faux site web copiant l'apparence du site officiel, où la victime est invitée à saisir ses identifiants, mots de passe ou coordonnées bancaires. Les indices permettant de détecter un phishing incluent : adresse d'expéditeur suspecte, fautes d'orthographe, ton urgent ou menaçant, URL ne correspondant pas au domaine officiel. Référence : ANSSI ; cybermalveillance.gouv.fr ; DigComp 2.2, compétence 4.2 « Protéger les données personnelles et la vie privée » ; PIX domaine 4.

---

### 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

**Réponse correcte : b)**

**Explication :**
Un logiciel antivirus (ou solution de sécurité endpoint) a pour fonction principale de protéger un système informatique contre les logiciels malveillants. Il fonctionne selon plusieurs mécanismes : la détection par signatures (comparaison des fichiers avec une base de données de malwares connus), l'analyse heuristique (détection de comportements suspects), l'analyse comportementale en temps réel et, de plus en plus, l'intelligence artificielle. Un antivirus moderne protège contre les virus, les chevaux de Troie, les rançongiciels, les logiciels espions, les rootkits, etc. Il n'accélère pas Internet (a), ne gère pas les sauvegardes cloud (c) et ne met pas en page les documents (d). Référence : ANSSI ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

### 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

✅ **Réponse correcte : b)**

**Explication :**
Les mises à jour logicielles (patches) sont essentielles principalement pour corriger les failles de sécurité (vulnérabilités) découvertes après la publication du logiciel. Les cybercriminels exploitent activement ces vulnérabilités pour s'infiltrer dans les systèmes. Les mises à jour « zero-day patches » corrigent des failles déjà exploitées. En retardant les mises à jour, on laisse une fenêtre d'attaque ouverte. Les mises à jour apportent aussi des corrections de bugs et parfois de nouvelles fonctionnalités, mais la sécurité est la raison primordiale. Elles n'augmentent pas le disque dur (c) et les logiciels n'expirent pas automatiquement (d). Référence : ANSSI, guide d'hygiène informatique ; DigComp 2.2, compétence 4.1 ; PIX domaine 4, compétence 4.1.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**
La règle de sauvegarde 3-2-1 est une bonne pratique fondamentale en matière de protection des données. Elle préconise de conserver au moins 3 copies de chaque fichier important (l'original et 2 sauvegardes), de stocker ces copies sur au moins 2 types de supports différents (par exemple, disque dur interne + disque dur externe, ou disque dur + cloud), et de garder au moins 1 copie hors site (dans un lieu géographiquement distinct, par exemple dans le cloud ou chez un tiers) pour se protéger contre les catastrophes locales (incendie, inondation, vol). Cette stratégie minimise considérablement le risque de perte définitive de données. Référence : US-CERT ; ANSSI ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**
Les réseaux Wi-Fi publics ouverts (sans mot de passe ou avec un mot de passe partagé) sont vulnérables à plusieurs types d'attaques. L'attaque de type « man-in-the-middle » (MITM) permet à un attaquant de se positionner entre l'utilisateur et le point d'accès pour intercepter les données transitant en clair (identifiants, mots de passe, e-mails, données bancaires). Un attaquant peut aussi créer un faux point d'accès (« evil twin ») portant un nom similaire au réseau légitime. Les bonnes pratiques incluent : utiliser un VPN (réseau privé virtuel), vérifier que les sites visités sont en HTTPS, éviter les transactions sensibles, et désactiver le Wi-Fi quand il n'est pas utilisé. La vitesse (a) et la batterie (c) ne sont pas les risques principaux. Les réseaux publics sont souvent gratuits (d). Référence : ANSSI ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

## 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

✅ **Réponse correcte : b)**

**Explication :**
Le RGPD (Règlement Général sur la Protection des Données, règlement UE 2016/679) impose que le consentement au traitement des données personnelles soit libre (sans contrainte), éclairé (l'utilisateur comprend ce à quoi il consent), spécifique (pour chaque finalité distincte) et univoque (par un acte positif clair, comme cocher une case non pré-cochée). L'utilisateur doit pouvoir retirer son consentement aussi facilement qu'il l'a donné. Les bandeaux de cookies « accepter tout » sans alternative facile de refus sont d'ailleurs régulièrement sanctionnés par la CNIL. Un courrier postal (a), une annonce presse (c) ou la simple mention du RGPD (d) ne constituent pas un consentement valide. Référence : RGPD, articles 6 et 7 ; CNIL ; DigComp 2.2, compétence 4.2 ; PIX domaine 4.

## 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

✅ **Réponse correcte : b)**

**Explication :**
Un pare-feu (firewall) est un dispositif de sécurité réseau (matériel et/ou logiciel) qui surveille et filtre le trafic réseau entrant et sortant en fonction de règles de sécurité prédéfinies. Il constitue une barrière entre un réseau de confiance (par exemple le réseau local) et un réseau non fiable (par exemple Internet). Le pare-feu peut autoriser, bloquer ou journaliser les connexions selon des critères comme l'adresse IP source/destination, le port, le protocole ou le contenu. Il existe des pare-feux à filtrage de paquets, à inspection d'état (stateful), de niveau applicatif (proxy) et de nouvelle génération (NGFW). Le nom est métaphorique (a), il ne modifie pas le débit (c) ni ne compresse les e-mails (d). Référence : ANSSI ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

## 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

✅ **Réponse correcte : b)**

**Explication :**
Le verrouillage de l'écran est la première barrière de sécurité d'un smartphone. En cas de perte ou de vol, il empêche un tiers d'accéder aux données personnelles (contacts, messages, e-mails, photos, comptes bancaires, etc.). Les mécanismes incluent : le code PIN (4-6 chiffres minimum), le mot de passe, le schéma de déverrouillage, l'empreinte digitale (biométrie) et la reconnaissance faciale. L'ANSSI recommande un code d'au moins 6 chiffres ou un mot de passe. Supprimer les applications (a) n'est pas la priorité sécuritaire. Désactiver le Wi-Fi (c) est excessif. Le film protecteur (d) protège l'écran physiquement, pas les données. Référence : ANSSI, guide de sécurité mobile ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

**Réponse correcte : b)**

**Explication :**
L'authentification multifacteur (MFA), dont la 2FA est le cas le plus courant, repose sur la combinaison d'au moins deux facteurs appartenant à des catégories distinctes : (1) Facteur de connaissance (« ce que je sais ») : mot de passe, code PIN, réponse secrète ; (2) Facteur de possession (« ce que je possède ») : smartphone recevant un code SMS ou une notification, clé de sécurité physique (FIDO2/U2F), token matériel ; (3) Facteur d'inhérence (« ce que je suis ») : empreinte digitale, reconnaissance faciale ou vocale, scan rétinien. Deux mots de passe (a) appartiennent à la même catégorie (connaissance) et ne constituent pas du 2FA. Un identifiant + e-mail (c) ne sont pas deux facteurs distincts. Un PIN + nom d'animal (d) sont deux facteurs de connaissance. Référence : NIST SP 800-63 ; ANSSI ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : a)**

**Explication :**
Le chiffrement symétrique utilise la même clé secrète (partagée entre les parties) pour chiffrer et déchiffrer les données. Algorithmes courants : AES (Advanced Encryption Standard, clés de 128/192/256 bits), ChaCha20. Avantage : très rapide. Inconvénient : la distribution sécurisée de la clé entre les parties est un défi. Le chiffrement asymétrique utilise une paire de clés mathématiquement liées : une clé publique (diffusée) pour chiffrer et une clé privée (secrète) pour

déchiffrer (ou l'inverse pour la signature). Algorithmes courants : RSA, ECC (Elliptic Curve Cryptography). Avantage : résout le problème de distribution des clés. Inconvénient : plus lent que le symétrique (c est faux). En pratique, les deux sont combinés (protocole TLS/HTTPS) : l'asymétrique échange une clé de session symétrique, qui chiffre ensuite les données. Référence : ANSSI ; PIX domaine 4 ; DigComp 2.2, compétence 4.1.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**
Un rançongiciel (ransomware) est un logiciel malveillant qui chiffre les fichiers de la victime (documents, photos, bases de données…) à l'aide d'algorithmes cryptographiques puissants, les rendant inaccessibles, puis affiche un message exigeant le paiement d'une rançon (généralement en cryptomonnaie) en échange de la clé de déchiffrement. Les recommandations de l'ANSSI et de cybermalveillance.gouv.fr sont formelles : ne pas payer la rançon (cela finance les criminels et ne garantit pas la récupération des données), déconnecter immédiatement l'appareil du réseau, conserver les preuves, porter plainte et contacter cybermalveillance.gouv.fr. La meilleure protection reste la prévention : sauvegardes régulières (règle 3-2-1), mises à jour, sensibilisation. Référence : ANSSI ; cybermalveillance.gouv.fr ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**
Un VPN (réseau privé virtuel) établit un tunnel chiffré entre l'appareil de l'utilisateur et un serveur VPN distant. Tout le trafic Internet transite par ce tunnel de manière chiffrée, ce qui offre deux avantages principaux : la confidentialité (les données sont illisibles pour quiconque intercepte le trafic, notamment sur un Wi-Fi public) et l'anonymisation partielle (l'adresse IP visible par les sites web est celle du serveur VPN, pas celle de l'utilisateur). Les protocoles VPN courants incluent OpenVPN, WireGuard et IKEv2/IPSec. Un VPN ne garantit pas une accélération (a) – il peut même légèrement ralentir la connexion. Il ne remplace ni l'antivirus ni le pare-feu (c), ce sont des protections complémentaires. Il ne connecte pas à plusieurs Wi-Fi (d). Référence : ANSSI ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

## 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

✅ **Réponse correcte : b)**

**Explication :**

L'ingénierie sociale est une catégorie d'attaques qui exploite les failles humaines plutôt que les failles techniques. L'attaquant manipule psychologiquement sa cible en exploitant la confiance, la peur, l'urgence, la curiosité ou la complaisance pour obtenir des informations sensibles (identifiants, mots de passe, accès physiques). Les principales techniques incluent : le phishing (e-mail frauduleux), le spear phishing (phishing ciblé), le pretexting (usurpation d'identité avec un prétexte), le baiting (appât physique comme une clé USB piégée), le tailgating (entrer dans un bâtiment sécurisé en suivant un employé), le vishing (phishing vocal). Le facteur humain est considéré comme le maillon le plus faible de la sécurité. Référence : Kevin Mitnick, The Art of Deception ; ANSSI ; DigComp 2.2, compétence 4.2 ; PIX domaine 4.

## 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

✅ **Réponse correcte : b)**

**Explication :**

Les cookies sont de petits fichiers texte stockés par le navigateur à la demande des sites web visités. Les cookies « first-party » (déposés par le site visité) sont souvent nécessaires au bon fonctionnement (session, panier d'achat, préférences). Les cookies « third-party » (tiers), déposés par des domaines différents du site visité (régies publicitaires, trackers), permettent de suivre l'utilisateur d'un site à l'autre et de constituer un profil de navigation détaillé à des fins de publicité ciblée. Ce sont ces derniers qui posent le plus de problèmes de vie privée. Le RGPD et la directive ePrivacy imposent le recueil du consentement avant le dépôt de cookies non essentiels. Les cookies ne sont pas des virus (a), ni des images (c), ni des mises à jour (d). Les navigateurs modernes bloquent de plus en plus les cookies tiers (Firefox, Safari, et Chrome progressivement). Référence : CNIL ; directive ePrivacy ; RGPD ; DigComp 2.2, compétence 4.2 ; PIX domaine 4.

## 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

✅ **Réponse correcte : b)**

**Explication :**

Pour vérifier la sécurité d'une connexion HTTPS, l'utilisateur doit examiner la barre d'adresse du navigateur : l'URL doit commencer par « https:// » (et non « http:// »), et un cadenas doit apparaître à gauche de l'URL (dans la barre d'adresse du navigateur, pas dans le contenu de la page). En cliquant sur ce cadenas, on peut inspecter le certificat numérique X.509 du site : nom du propriétaire, autorité de certification émettrice, date de validité. Attention : HTTPS garantit que la connexion est chiffrée, mais ne garantit pas que le site lui-même est légitime (un site de phishing peut très bien utiliser HTTPS). Il ne faut pas se fier à des images de cadenas dans le contenu de la page (a), au titre du site (c) ou à l'absence de publicités (d). Référence : ANSSI ; DigComp 2.2, compétences 4.1 et 4.2 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**

Le principe du moindre privilège (Principle of Least Privilege, PoLP) est un concept fondamental de la sécurité informatique. Il stipule que chaque utilisateur, programme ou processus ne doit disposer que des permissions minimales nécessaires pour accomplir sa tâche. Par exemple, un utilisateur standard n'a pas besoin des droits administrateur pour naviguer sur le web ou lire ses e-mails. Ce principe limite l'impact potentiel d'une compromission : si un compte utilisateur avec des droits limités est piraté, les dégâts sont contenus. Donner des droits administrateur à tous (a) est une grave erreur de sécurité. Limiter les fichiers (c) et restreindre la création de comptes (d) ne définissent pas ce principe. Référence : ANSSI, guide d'hygiène informatique (règle 12) ; NIST ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**

Les traces numériques se divisent en deux catégories principales. Les traces volontaires (ou actives) sont les informations que l'utilisateur diffuse délibérément : publications sur les réseaux sociaux, commentaires, avis, profils en ligne, e-mails envoyés, photos partagées. Les traces involontaires (ou passives) sont collectées automatiquement, souvent sans que l'utilisateur en ait conscience : adresse IP, cookies de traçage, historique de navigation, données de géolocalisation, métadonnées des fichiers, empreinte de navigateur (fingerprinting), logs de connexion. Il existe aussi les traces héritées : les informations publiées par d'autres à notre sujet. Ce ne sont pas des traces de robots vs humains (a), elles existent partout en ligne (c), et les deux peuvent être légales ou non selon le contexte (d). Référence : CNIL ; DigComp 2.2, compétence 4.2 ; PIX domaine 4.

---

## 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

**Réponse correcte : b)**

**Explication :**

Les pièces jointes malveillantes sont l'un des principaux vecteurs d'infection. Elles peuvent contenir des virus, des chevaux de Troie, des ransomwares ou des macros malveillantes (dans les fichiers Office). Les formats à risque incluent : les exécutables (.exe, .bat, .cmd, .scr), les fichiers Office avec macros (.docm, .xlsm), les archives (.zip, .rar contenant des exécutables), les scripts (.js, .vbs, .ps1) et même certains PDF piégés. Les bonnes pratiques sont : ne jamais ouvrir une pièce jointe d'un expéditeur inconnu ou inattendu, vérifier l'identité de l'expéditeur, scanner les pièces jointes avec un antivirus, désactiver l'exécution automatique des macros. La pièce jointe ne remplit pas le disque (a), ne transfère pas l'e-mail (c) et ne désinstalle pas le navigateur (d). Référence : ANSSI ; cybermalveillance.gouv.fr ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**

Une fonction de hachage cryptographique transforme une entrée (message) de taille arbitraire en une empreinte (hash/digest) de taille fixe. Exemples : SHA-256 produit un hash de 256 bits (64 caractères hexadécimaux), SHA-3, BLAKE2. Trois propriétés fondamentales : (1) Déterminisme :

la même entrée produit toujours le même hash. (2) Résistance aux collisions : il doit être computationnellement infaisable de trouver deux entrées différentes produisant le même hash. (3) Résistance à la préimage (irréversibilité) : il doit être impossible de retrouver l'entrée à partir du hash. Applications : vérification d'intégrité de fichiers, stockage sécurisé de mots de passe (hash + sel), signatures numériques, blockchain (chaque bloc contient le hash du précédent). Ce n'est pas de la compression (a), du tri (c) ou un protocole réseau (d). Référence : NIST ; ANSSI ; PIX domaine 4 ; programme de NSI.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**

Un mot de passe de 4 chiffres décimaux offre $10^4$ = 10 000 combinaisons possibles (de 0000 à 9999). Une attaque par force brute (brute force) teste systématiquement toutes les combinaisons possibles jusqu'à trouver la bonne. Un ordinateur moderne peut tester des millions, voire des milliards de combinaisons par seconde (selon l'algorithme de hachage utilisé). 10 000 combinaisons seraient donc testées en une fraction de seconde. C'est pourquoi les experts recommandent des mots de passe d'au moins 12 caractères mélangeant lettres, chiffres et symboles, ce qui augmente exponentiellement l'espace de combinaisons (par exemple, 12 caractères parmi 95 symboles = $95^{12} \approx 5{,}4 \times 10^{23}$ combinaisons). Le nombre de combinaisons n'est pas 40 (a), ni 1 000 000 (c), ni 4 (d). Référence : ANSSI ; NIST SP 800-63B ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**

L'injection SQL (SQLi) est l'une des vulnérabilités web les plus critiques (classée dans le Top 10 OWASP). L'attaquant insère du code SQL malveillant dans un champ de saisie (formulaire de connexion, barre de recherche, URL) qui est transmis directement à la base de données. Exemple : dans un formulaire de connexion, au lieu d'un nom d'utilisateur, l'attaquant saisit : ' OR '1'='1' -- ce qui modifie la requête SQL et peut contourner l'authentification. Les conséquences

peuvent inclure : accès non autorisé, vol de données, modification ou suppression de données, voire prise de contrôle du serveur. Protection principale : les requêtes paramétrées (prepared statements / parameterized queries) qui séparent le code SQL des données utilisateur. Autres mesures : validation des entrées, principe du moindre privilège pour les comptes BDD, WAF (Web Application Firewall). Référence : OWASP Top 10 ; ANSSI ; PIX domaine 4 ; programme de NSI.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**

Le protocole TLS (Transport Layer Security, successeur de SSL) sécurise les communications HTTPS via un processus appelé « handshake TLS ». En TLS 1.3 (version actuelle), le processus est : (1) Le client envoie un « ClientHello » avec les suites cryptographiques supportées et des paramètres de clé ; (2) Le serveur répond avec son certificat numérique (authentification) et les paramètres de clé ; (3) Les deux parties calculent un secret partagé via un échange de clés Diffie-Hellman éphémère (ECDHE) – c'est la partie asymétrique ; (4) Ce secret partagé dérive des clés de session symétriques (AES-GCM ou ChaCha20-Poly1305) utilisées pour chiffrer toutes les données échangées – c'est la partie symétrique, beaucoup plus rapide. TLS n'envoie jamais de mot de passe en clair (a), ne masque pas l'URL (c) et ne se limite pas à la compression (d). Référence : RFC 8446 (TLS 1.3) ; ANSSI ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**

Une attaque DDoS (Distributed Denial of Service) vise à rendre un service (site web, application, serveur) indisponible en le submergeant d'un volume massif de requêtes provenant de multiples sources simultanées. L'attaquant utilise généralement un botnet : un réseau de milliers ou millions d'appareils compromis (ordinateurs, objets connectés IoT) contrôlés à distance. Les principales catégories sont : les attaques volumétriques (saturation de la bande passante, ex. : UDP flood), les attaques protocolaires (exploitation des protocoles réseau, ex. : SYN flood), et les attaques applicatives (ciblage de la couche application, ex. : HTTP flood). L'objectif n'est pas de voler des données mais de perturber la disponibilité du service. Les protections incluent les CDN, les services anti-DDoS (Cloudflare, AWS Shield), le filtrage de trafic. Ce n'est pas un virus (a), ni du

phishing (c), ni un outil de répartition (d). Référence : ANSSI ; OWASP ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**
Une vulnérabilité zero-day (ou 0-day) est une faille de sécurité dans un logiciel qui est inconnue de son éditeur (et donc non corrigée) au moment de sa découverte ou de son exploitation par des attaquants. Le terme « zero-day » signifie que l'éditeur a eu « zéro jour » pour développer et déployer un correctif. C'est l'une des menaces les plus redoutées en cybersécurité car : (1) aucun patch n'est disponible ; (2) les antivirus basés sur des signatures ne détectent pas l'attaque (elle est inédite) ; (3) les systèmes de détection d'intrusion n'ont pas de règles pour l'identifier. Les zero-days se vendent sur des marchés spécialisés (légaux comme Zerodium ou clandestins sur le dark web) pour des sommes considérables (jusqu'à plusieurs millions de dollars pour les plus critiques). Exemples célèbres : Stuxnet, EternalBlue. Référence : ANSSI ; MITRE CVE ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.

---

## 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

✅ **Réponse correcte : b)**

**Explication :**
Si une base de données stockant des mots de passe en clair est compromise (piratage, fuite, accès non autorisé), tous les mots de passe sont immédiatement exposés. La pratique recommandée est le hachage salé : (1) On génère un sel (salt) : une chaîne aléatoire unique pour chaque utilisateur. (2) On concatène le mot de passe avec le sel. (3) On applique une fonction de hachage spécialement conçue pour le stockage de mots de passe : bcrypt, scrypt ou Argon2 (recommandé par l'OWASP). Ces algorithmes sont intentionnellement lents (key stretching) pour résister aux attaques par force brute. Le sel empêche les attaques par tables arc-en-ciel (rainbow tables) qui contiennent des correspondances hash/mot de passe pré-calculées. On ne stocke

jamais le mot de passe, seulement le hash salé. Ce n'est pas un problème d'espace (a), de vitesse (c) ou de quota légal (d). Référence : OWASP ; ANSSI ; NIST SP 800-63B ; PIX domaine 4.

---

### 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

✅ **Réponse correcte : b)**

**Explication :**
L'OWASP (Open Web Application Security Project) publie régulièrement le « Top 10 », un document de sensibilisation qui identifie et classe les 10 risques de sécurité les plus critiques pour les applications web, basé sur l'analyse de données réelles de vulnérabilités. L'édition 2021 classe en première position « A01:2021 – Broken Access Control » (contrôle d'accès défaillant) : les mécanismes d'autorisation ne fonctionnent pas correctement, permettant à des utilisateurs d'accéder à des ressources ou fonctionnalités qui devraient leur être interdites. Suivent notamment : les défaillances cryptographiques (A02), les injections (A03, incluant SQL injection et XSS), la conception non sécurisée (A04), la mauvaise configuration de sécurité (A05). L'OWASP Top 10 est une référence utilisée par les développeurs, les auditeurs et les réglementations (PCI-DSS). Référence : owasp.org ; ANSSI ; PIX domaine 4.

---

### 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

✅ **Réponse correcte : b)**

**Explication :**
Le protocole d'échange de clés Diffie-Hellman (DH), inventé par Whitfield Diffie et Martin Hellman en 1976, permet à deux parties (traditionnellement Alice et Bob) d'établir un secret partagé en n'échangeant que des informations publiques sur un canal de communication non sécurisé. Le principe repose sur l'arithmétique modulaire dans un groupe cyclique : chaque partie choisit un secret privé, calcule une valeur publique (exponentiation modulaire) et l'envoie à l'autre. Chaque partie combine la valeur publique reçue avec son propre secret privé pour obtenir le même secret partagé. La sécurité repose sur la difficulté du problème du logarithme discret. Ce secret partagé est ensuite utilisé comme clé pour un chiffrement symétrique rapide. La variante moderne ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) est utilisée dans TLS 1.3 pour sécuriser HTTPS. Ce n'est pas un transfert de mots de passe (a), ni de la compression (c), ni un VPN automatique (d). Référence : Diffie & Hellman (1976) ; RFC 7748 ; ANSSI ; PIX domaine 4.

## 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

✅ **Réponse correcte : b)**

**Explication :**
EBIOS Risk Manager (Expression des Besoins et Identification des Objectifs de Sécurité) est la méthode de référence française pour l'analyse de risques numériques, développée et maintenue par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Publiée en 2018, elle succède à EBIOS 2010. La méthode se déroule en 5 ateliers : (1) Cadrage et socle de sécurité – définition du périmètre et des mesures de base ; (2) Sources de risque – identification des attaquants potentiels et de leurs objectifs ; (3) Scénarios stratégiques – chemins d'attaque haut niveau via l'écosystème ; (4) Scénarios opérationnels – modes opératoires techniques des attaques ; (5) Traitement du risque – définition des mesures de sécurité proportionnées. EBIOS est conforme aux normes ISO 27005 et ISO 31000. Ce n'est pas un antivirus (a), ni un protocole de chiffrement (c), ni un OS (d). Référence : ANSSI, EBIOS Risk Manager (2018) ; ISO 27005 ; DigComp 2.2, compétence 4.1 ; PIX domaine 4.