BTS SIO · BLOC 3 CYBERSÉCURITÉ

Audit MedSecure — Identité numérique et ingénierie sociale

Durée conseillée : 1 h 30 · Évaluation sur 20 points

Nom : ..... **Note :** ..... / 20

Consigne : Répondez de manière rédigée et justifiez chaque réponse à partir du dossier documentaire. Utilisez le vocabulaire précis de l'identité numérique et des protocoles de sécurité.

Mission 1 — Noms de domaine et usurpation d'e-mail · 12 points

1. **En analysant le Document 1, expliquez le risque opérationnel majeur pour MedSecure si le nom de domaine n'est pas renouvelé à temps. Nommez l'attaque spécifique correspondante.** — 3 pts

2. **En observant les champs `From:` et `Return-Path:` du Document 2, expliquez la technique employée par l'attaquant pour tromper le destinataire. Comment qualifie-t-on l'utilisation du nom `med-secure.com` ?** — 3 pts

3. **Le courriel du Document 2 relève d'une tentative de hameçonnage (phishing). Relevez trois indices visuels ou techniques (en dehors des adresses d'expédition) confirmant cette hypothèse.** — 3 pts

Mission 2 — Interception réseau et qualification légale · 8 points

4. **Expliquez la signification des mentions `spf=softfail` et `dkim=none` présentes dans les en-têtes du Document 2. En quoi permettent-elles au serveur de messagerie de détecter la fraude ?** **3 pts**

5. **À partir du Document 3, expliquez comment l'attaquant a pu récupérer les identifiants du Dr Martin sans qu'aucun virus ne soit installé sur sa machine. Nommez précisément ce type d'attaque.** **3 pts**

6. **Indiquez quelle mesure technique élémentaire (au niveau du protocole web employé) aurait empêché cette interception en gare.** **2 pts**

7. **(Question CEJMA) Citez deux infractions pénales prévues par la loi qui peuvent être retenues contre l'auteur de ces attaques.** **3 pts**