B3_S1_INT01_20220922

Nom, prénom, groupe :

Répondez de manière précise, directe et concise. Les longues phrases bien construites ne sont ici pas nécessaires (contrairement à un partiel/examen). Gérez votre temps, apprenez à synthétiser même si vous en savez en réalité plus sur le sujet.

Considérez cet extrait d'un article de presse au sujet d'une cyberattaque:

> (…) Suite à l'attaque, un audit de sécurité a révélé que le système informatique de la société a été infecté par un malware de type « botnet », rendant indisponibles les serveurs web publics de l'organisation pendant plusieurs heures (…) Dans notre entrevue du mois dernier, le RSSI nous avait pourtant assuré avoir mis en place une solution anti-malware «de pointe», dont les clients doivent aujourd'hui se demander si elle est réellement efficace ou si elle a été déployée correctement (…)

01 . Relevez, dans cet extrait, une imprécision due à un manque de connaissances techniques du rédacteur (première phrase).

02 . Que pensez-vous alors de la critique énoncée (seconde phrase) ?

03 . Sur la base de cet extrait, quelle hypothèse faites-vous quant au **type d'attaque** dont a réellement été victime la société en question ?

Considérez le SMS ci-dessous, reçu par une employée de votre organisation, Éva N. :

> GOOGLE
>
> Google a bloqué une connexion suspecte sur votre compte alexandrexxxx@gmail.com. Veuillez changer votre mot de passe au plus vite pour éviter le blocage définitif de votre compte : https://securite.google.com.org/hUKnvb

04 . Comment s'appelle précisément cette attaque ?

05 . Dans quelle **grande catégorie** de techniques d'attaque classez-vous celle-ci ?

06 . Relevez, dans ce SMS, **deux techniques classiques** utilisées par l'auteur pour optimiser son attaque.

07 . Pourquoi cette attaque a-t-elle peu de chances d'aboutir sur notre employée ? Expliquez pourquoi cela peut pourtant être rentable pour un groupe de cybercriminels.

Un attaquant parvient à rentrer dans le bâtiment d'une organisation ciblée en se faisant passer pour un employé de nettoyage, pendant les heures de bureau. Il connaît suffisamment le fonctionnement de l'organisation pour savoir que sa présence ne sera pas jugée suspecte s'il n'interagit pas directement avec les employés.

08 . Énoncez **trois attaques ou techniques d'attaque** qu'il pourra néanmoins tenter sur les lieux, en expliquant très brièvement de quoi il s'agit.

Un attaquant ciblant l'entreprise ONVADIR SA à La Madeleine (Lille) parvient à constituer une liste de quelques dirigeants et managers de l'organisation. En utilisant des techniques d'OSINT, il se rend compte que certains d'entre eux sont adeptes des échecs: ils font partie du club de la ville et visitent souvent son site, `echecsalamadeleine.fr`, pour connaître les dates et résultats de tournois locaux.

09 . Une idée germe immédiatement dans le cerveau torturé de l'attaquant. Indiquez le nom de l'attaque potentielle et expliquez son fonctionnement.

10 . Expliquez le terme « OSINT ».

Le 22 août 2022, le code source et des informations techniques propriétaires de l'entreprise *LastPass* (concurrent de *DashLane* et *1Password* notamment) ont été volés. L'éditeur du fameux logiciel - qui compte 25 millions d'utilisateurs et 80000 entreprises clientes - a annoncé que des pirates se sont introduits dans le compte d'un de ses développeurs et l'ont utilisé pour accéder à des données exclusives. *LastPass* affirme que les pirates ont eu un accès interne à son système pendant quatre jours, mais qu'aucune donnée client (identifiants et mots de passe en particulier) n'a été compromise.

11 . Comment appelle-t-on une solution comme *LastPass* ?

12 . Énoncez **trois avantages** de ce type de solution, en comparant avec la façon dont un employé livré à lui-même gère habituellement ce problème.

Supposons que la compromission permette à terme aux attaquants de récupérer la liste de tous les **identifiants** (pseudos, emails…) enregistrés par les utilisateurs de *LastPass*.

13 . Comment pourraient-ils *immédiatement* gagner une somme conséquente grâce à cette liste ?

14 . Quel **type d'attaque** un pirate en possession de cette liste pourrait-il mettre en place ? **Expliquez** brièvement son fonctionnement.

Vous faites partie de la SSI (Sécurité des Systèmes d'Information) dans votre organisation, qui utilise le plan *Business* de *LastPass* pour ses employés. Suite aux révélations de ce nouvel incident (*LastPass* a déjà été victime de plusieurs attaques), votre RSSI (Responsable de la SSI) envisage de mettre un terme à ce contrat, et demande les avis de ses collaborateurs.

15 . Écrivez un email à destination du RSSI dans lequel vous formulerez **deux propositions *argumentées*** en réponse à sa demande *(pour cette dernière question uniquement, vous prendrez soin de **rédiger effectivement et correctement** cet email, tout en restant très synthétique)*

Last updated 2022-09-22 07:27:51 +0200