Travaux pratiques – Ingénierie sociale (version de l'instructeur)

**Remarque à l'intention de l'instructeur**: le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

1. Objectifs

Rechercher et identifier les attaques par ingénierie sociale

1. Contexte/scénario

Le but d'une attaque par ingénierie sociale est d'inciter une victime à révéler des informations personnelles ou sensibles. Le hacker peut utiliser un enregistreur de frappe ou un message de phishing ou alors rencontrer en personne l'individu ciblé. Dans le cadre de ces travaux pratiques, vous devez déterminer ce qu'est l'ingénierie sociale et identifier les moyens de reconnaître ce type d'attaque et de l'empêcher.

1. Ressources requises

* Ordinateur personnel ou terminal mobile avec accès Internet
  1. Lisez l'article suivant.

Accédez au site web suivant et lisez-le attentivement afin de répondre aux questions suivantes à l'étape 2.

<https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972>

* 1. Répondez aux questions suivantes.
     1. Quelles sont les trois méthodes utilisées dans le cadre d'une attaque d'ingénierie sociale pour accéder à des informations ?

1. ****Accès électronique :** Cela implique l'utilisation de techniques en ligne, telles que le phishing par e-mail, pour tromper les individus et les inciter à divulguer des informations sensibles.**
2. ****Accès physique :** Cette méthode implique une interaction directe avec la victime, par exemple, en se faisant passer pour un employé ou un prestataire de services, afin d'obtenir des informations ou un accès non autorisé à des locaux.**
3. ****Médias sociaux :** Les attaquants exploitent les informations disponibles sur les réseaux sociaux pour cibler leurs victimes. Les données partagées, comme les centres d'intérêt, les relations, ou les informations personnelles, peuvent être utilisées pour personnaliser les attaques et tromper les individus.**

Les réponses doivent inclure un accès électronique, un accès physique et les médias sociaux.

* + 1. Donnez trois exemples d'attaque par ingénierie sociale selon les deux premières méthodes définies à l'étape 2a ?

1. ****Phishing par e-mail (Accès Électronique) :** Les attaquants envoient des e-mails frauduleux se faisant passer pour des institutions légitimes, tels que des banques ou des services en ligne. Ces e-mails contiennent souvent des liens malveillants ou des pièces jointes infectées. Lorsque les victimes cliquent sur ces liens ou ouvrent les pièces jointes, leurs informations sensibles, telles que les identifiants de connexion, peuvent être volées.**
2. ****Ingénierie sociale sur les réseaux sociaux (Accès Électronique) :** Les attaquants peuvent utiliser des informations disponibles publiquement sur les réseaux sociaux pour créer des messages ou des profils trompeurs. Ils peuvent créer de faux profils pour établir une connexion avec la victime, puis utiliser ces connexions pour obtenir des informations personnelles.**
3. ****Talonnage (Accès Physique) :** L'attaquant se présente physiquement à un lieu, par exemple, en se faisant passer pour un employé de maintenance ou de livraison. En utilisant cette fausse identité, l'attaquant peut gagner l'accès à des locaux sensibles ou convaincre les employés de divulguer des informations confidentielles.**

Les réponses varient, mais peuvent inclure le « spear phishing » par e-mail, des leurres avec le contenu souhaité ou le talonnage.

* + 1. Pourquoi les réseaux sociaux présentent-ils un risque d'attaque par ingénierie sociale ?

1. ****Partage d'informations personnelles :** Les utilisateurs ont tendance à partager des détails personnels tels que leur nom, prénom, date de naissance, lieu de résidence, centres d'intérêt, et relations. Ces informations peuvent être exploitées par des attaquants pour personnaliser leurs attaques et gagner la confiance des victimes.**
2. ****Habitudes et routines :** Les activités quotidiennes, les routines, et même les déplacements peuvent être déduits à partir des publications sur les réseaux sociaux. Les attaquants peuvent utiliser ces informations pour planifier des attaques qui coïncident avec les moments où les victimes sont plus vulnérables.**
3. ****Relations en ligne :** Les connexions en ligne peuvent être utilisées pour créer des attaques plus crédibles. Les attaquants peuvent se faire passer pour des amis, des collègues ou des connaissances en exploitant les relations établies sur les réseaux sociaux pour inciter les victimes à divulguer des informations sensibles.**

Les réponses doivent inclure que les réseaux sociaux encouragent généralement les internautes à partager les informations personnelles en plus de leurs centres d'intérêt et de leurs habitudes. (Nom et prénom, date de naissance, ville, etc.).

* + 1. Comment une entreprise peut-elle se défendre contre les attaques par ingénierie sociale ?

**Formations de Sensibilisation à la Sécurité.**

**Simulation d'Attaques.**

**Politiques de Sécurité Clair.**

**Systèmes de Détection Précoce.**

**Contrôles d'Accès Renforcés.**

**Sensibilisation Continue.**

Les réponses doivent inclure la création et la participation à des formations de sensibilisation à la sécurité.

* + 1. Qu'est-ce que l'organisme SANS Institute qui a rédigé cet article ?

L'organisme SANS Institute, qui a rédigé l'article, est un fournisseur de formation et de certification en matière de sécurité de l'information. Il est reconnu pour offrir des programmes de formation de haute qualité dans le domaine de la cybersécurité. Le site web [https://www.sans.org](https://www.sans.org/) est la plateforme où SANS fournit des ressources, des cours et des informations sur la sécurité de l'information pour les professionnels de la sécurité et les personnes cherchant à améliorer leurs compétences dans ce domaine. Le SANS Institute joue un rôle important dans l'éducation et la sensibilisation à la sécurité informatique.

Les réponses varient selon le site web https://www.sans.org et le contenu affiché. La réponse doit inclure qu'il s'agit d'un fournisseur de formation et de certification en matière de sécurité de l'information.