Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique et Technologie de l'Information
2iéme Master Administration et supervision des réseaux
Examen du module Sécurité 2

Nom :
Prénoms :

Répondez aux questions suivantes :

- Quel type d'attaque permet de masquer l'identité (l'adresse IP) du hacker ?
- **Les attaques indirectes par rebond**
- Dans quel type d'attaque le hacker attaque directement sa victime à partir de son ordinateur ?
- **Les attaques directes**
- Dans quel type d'attaque le hacker utilise les ressources de l'ordinateur intermédiaire (CPU, bande passante...) pour attaquer.
- **Les attaques indirectes par rebond**
- Quelle attaque permet le cassage d'un mot de passe en testant tous les mots de passe possibles
- **Attaque par force brute**
- Quelle attaque consiste à remplacer l'adresse IP de l'expéditeur d'un paquet par l'adresse IP d'une autre machine
- **L'usurpation d'adresse IP (spoofing IP)**
- Quelle technique permet à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage
- **L'usurpation d'adresse IP (spoofing IP)**
- Quel type d'attaque vise à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation
- **Une attaque par déni de service (DoS, Denial of Service)**
- Quel type d'attaque est basée sur l'utilisation de serveurs de diffusion
- **Attaque par réflexion**
- Quel type d'attaque (par réponse) consiste à utiliser des serveurs dont la réponse à une requête renvoie bien plus de données que la requête originale.
- **Attaque par amplification**
- Quelle sont les deux sous-protocoles utilisés par IPSec
- **ESP et AH**
- Quelle sont les deux modes d'association possibles dans IPSec (Mode)
- **Transport et Tunel**
- Quel protocole d'authentification réseau repose sur l'utilisation de tickets
- Kerberos

- Quel protocole agis comme relais de l'authentification vers d'autres serveurs d'authentification
- **Radius/Tacacs/ Kerberos**
- Lequel de ces deux protocoles (TCD ou UDP) est utilisé par :
  - Tacacs : UDP
  - Tacacs + : TCP
  - Radius : UDP

Lors d'une attaque on distingue différentes étapes, dans quelle étape :

- L'attaquant pénètre des réseaux privilégiés auxquels la machine compromise a accès. Compromission
- L'attaquant emploie des scanneurs de vulnérabilité.
- Repérage des failles
- L'attaquant scanne les adresses IP et les ports ouverts.
- Balayage du réseau
- Consiste à récupérer le maximum d'informations sur l'architecture du réseau
- Collecte d'informations

Veuilles indiquer si ces affirmations sont vraies ou fausses :

1. L'utilisation des protocoles chiffrés permets de se prémunir des snifers
2. L'acquisition active consiste à analyser les datagrammes IP circulant sur un réseau
3. Lors de la phase de nettoyage des traces, le pirate installe une application afin de créer artificiellement une faille de sécurité
4. Le virus polymorphe modifie les signatures de l'antivirus afin de les rendre inopérants
5. Le vers est un programme ouvrant une porte dérobée (backdoor) dans un système
6. Le rétrovirus se déclenche à un moment déterminé en exploitant la date du système
7. Le ransomware est chargé d'enregistrer les frappes de touches du clavier
8. Les keyloggers est l'envoi massif de courrier électronique
9. Les DoS par exploitation de vulnérabilités submerge une machine de requêtes
10. Dans une attaque par fragmentation, l'attaquant demande au serveur d'utiliser une version d'un protocole plus ancienne afin d'exploiter les failles qu'elle comporte.
11. Les attaques par rejeu (replay attaque) sont des attaques de type man in the middle
12. SET (Secure Electronic Transaction) est un protocole de sécurisation des transactions électroniques mis au point par Visa et MasterCard, et s'appuyant sur le standard SSL
13. IPSec permet de combiner les associations de sécurité
14. Les politiques de sécurité IPsec sont définies dans une base de données de politiques de sécurité
15. Le protocole IKE (Internet Key Exchange) a pour objectif de fournir des mécanismes d'authentification et d'échange de clés.
16. Dans IPSec, le Quick Mode permet de négocier les paramètres de sécurité des protocoles sous-jacents.
17. SSH utilise des Biclé asymétrique, créée par l'administrateur du serveur lors de l'installation et de la configuration.
18. SSH utilise des modes d'authentification par challenge
19. Le protocole Tacacs utilise le protocole TCP et le port 49 pour son transport
20. Les transactions entre un client TACACS+ et un serveur TACACS+ sont authentifiées par le biais d'un secret partagé