Université Batna-2 **2019/2020**
Département informatique
3ème Année Licence (SI)

Module : Sécurité Informatique

TD 3 : Les types d'attaques

Exercice1 :

1- Donnez dans un tableau pour chacun des 5 services de sécurité un type d'attaque qui lui correspond ?
2- Donnez un moyen permettant de réaliser : l'authentification, la confidentialité, la non-répudiation et la fraicheur de donnée?

Exercice2 :

1- Qu'est-ce qu'un Déni de Service ? Donnez une attaque qui puisse le causer dans un réseau local filaire? une autre pour un réseau sans fil ?
2- Dans l'entête d'un paquet TCP on trouve le numéro de séquence du paquet. Comment cette information peut-elle être exploitée pour une attaque ? de quel type sera donc cette attaque ?
3- Tout réseau possède une adresse de diffusion. Les messages envoyés à cette adresse de diffusion sont envoyés à tous les ordinateurs du réseau. Par exemple, si je veux connaître les autres ordinateurs de mon réseau, je peux pinguer l'adresse de diffusion et tous les ordinateurs connectés répondront à mon *ping*. Pourquoi serait-ce une mauvaise idée que les hôtes répondent aux pings de diffusion (c'est-à-dire les echorequests d'ICMP, envoyées à l'adresse de diffusion) ? Quel type de problème cela pourrait-il causer ?
4- Une autre attaque classique de Déni de Service est l'attaque SYN. Dans une attaque SYN, un attaquant envoie à une victime un flot de paquets SYN avec des adresses sources usurpées. La victime initialise des états de connexion et essaie de répondre aux adresses spoofées. Si suffisamment de paquets SYN sont envoyés, la table de connexions d'un serveurpeut être remplie, et les nouvelles requêtes seront refusées. Proposez des solutions pourrésoudre ce problème ?

Exercice3:

1- Qu'est ce que la cyber-criminalité ? qui vise-t-elle en premier ?
2- Quelles sont les solutions les plus utilisées dans les entreprises pour contrer la cybercriminalité ?

Réponses :

Exercice1 :

1- Authentification, confidentialité, integrité, diponibilité et non répudiation.

2-

Service	Type attaque visant ce service
Authentification	Usurpation d'identité
Confidentialité	Sniffing, interception de messages,
Intégrité	Modification du message, brouillage
Non Répudiation	Modification du journal , Répudiation
Disponibilité	DoS, bombardement et saturation du réseau

Rq : il y a une différence entre « une attaque qui vise un service » et « une attaque qui casse un service » : une attaque qui vise un service peut le casser ou pas suivant sa robustesse.

3- Donnez pour chaque service un moyen permettant de le réaliser ?
Authentification : Login/mot de passe, Certificat…
Confidentialité : Chiffrement
Non-répudiation : Signature numérique
Fraicheur : Time-stamp (date, heure) (dans les paquets RTP par exemple)

Exercice2 :

1- Un Dos : est une attaque ou un objectif d'attaques qui vise à mettre à plat une partie ou tout le système informatique.

DoS réseau local filaire : ex : Sniffer DoS réseau sans fil : Jamming

2-

- Le numéro de séquence indique le numéro du premier octet de données contenu dans le datagramme.

- Le numéro d'acquittement fournit un d'accusé de réception, et indique le numéro du prochain octet de données attendu par la machine.

*Si tout se passe bien (pas de perte de données, de retransmission, etc.), le numéro d'acquittement du récepteur est identique au numéro de séquence du prochain datagramme envoyé par l'émetteur.

Donc, il suffit d'intercepter un ACK et l'attaquant connait le prochain SEQ (num de séquence). Il pourra alors l'exploiter pour confectionner de faux paquets et les injecter dans le réseau et ils seront bien acceptés par le récepteur, ça pourra être une attaque d'injection de fausses infos, ou pourra aller jusqu'à un DoS si l'envoi est intensif.

3- Cela pourrait facilement être exploité pour générer un trafic très intensif et donc une attaque par inondation indirecte. Cela peut donc causer un DoS.

4- Reprenons : Une attaque par déni de services SYN flood est une technique visant à saturer un serveur en envoyant une multitude de paquets TCP, avec le flag SYN. Les connexions sont alors établies vers la machine, mais restent à moitié ouvertes, car le client malveillant (hacker) ne renvoie pas de confirmation (ACK).Le serveur attend pendant un certain délai la réponse et la connexion semi-ouverte consomme alors un certain nombre de ressources. En multipliant ce type de connexions, le hacker peut arriver à créer un déni de service qui rendra la machine inopérante.

Solutions :

- attendre pendant un certain temps, si pas d'ACK, l'entrée dans la table sera supprimée

- limiter le nombre d'entrées initiées pour éviter que la table ne déborde

- le Firewall doit bloquer une @IP qui envoie un nombre important de SYN.

Exercice3:

1- La cybercriminalité représente tout acte malveillant commis sur le réseau Internet (ou sous réseau en général) (espionnage d'informations confidentielles, mise à plat d'un réseau, accès illégitime au machines, harcèlement ou détournement de personnes spécialement mineurs par internet, vente de produits non autorisés, appels à la haine, au terrorisme, ….

Les statistiques ont prouvé que la cybercriminalité touche en premier lieu les entreprises.

2- Quelles sont les solutions les plus utilisées dans les entreprises pour contrer la cybercriminalité ?

L'utilisation de firewall (pares-feu) : Un **pare-feu**(*firewall*), est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets.