3 – Attaques sur les logiciels

* Configuration par défaut
* Bugs
* Dépassement de pile
* Script
* Injection sql
* Homme du milieu

4) Dos/ddos

* Déni de service distribué
* Inonder le service de demandes
* Demande de connexino sans suite
* Surcharger le serveur en demande UDP
* Udp prioritaire tcp
* Smurfling/inonder de requetes ICMP (ping) en broadcast en usurpant l’identité de certaines machines
* Ddos (dos avec de nombreuses machines)

5) Types de détection

IDS (Système de détention d’intrusions

* Surveiller la mémoire et les processus
* Trier les connexions
* Filtrer les communications sur la passerelle / routeur

6) Méthodes de détention

Recherche de motifs (pattern matching)

Analyse de protocoles à la recherche d’abus connu

Analyse heuristique à la recherche de comportements inconnues

Approche probabiliste / statistiques

Demander une autorisation

Rédupérer le produit auprès du responsable des stocks

Transmissions de l’information au service comptable

QoS : Qualité de Service

1 – Objectif

Optimisation des ressources réseaux pour garantir les performances.

QoS selon les applications ou les utilisateurs

Mutualiser les ressources

2 – Principe

Filtrer les données sur le réseau

Couche 3 : IP

Critère de filtrage :

* Protocole, port source et destination
* Bande passante
* Source et destination
* Date et heure
* Etat du trafic réseau
* Itinéraire
* Distance
* Limitation de trafic

3) Limitation du trafic

Au moyen d’un algo, seau percé pour limiter le trafic.

4) Ordonnancement

Gestion de l’ordre de passage.

FIFO : First in first out