Supervision et infogérence

3 types d’infogérance :

* TMA
* Support des utilisateurs et de la maintenance
* Gestion des infrastructures
* Externalisation ou nom de de l’hébergement
* BPO
* Externalisation de certains processus de l’entreprise (compta, rh, paye)

1 – Supervision, monitoring

Niveau 1 :

Service disponible ou non -> alerte

Niveau 2 :

Interventions ponctuelle des techniciens

Niveau 3 :

Infogérence

Maj, analyse de log, sauvegarde, audit

2 – Infogérence et protections

* Basculement ou fail-over
* Basculer automatiquement sur un équipement alternatif
* 2 nodes :
  + Equipement secondaire en veille
  + Equilibrage de charge
* Equilibrage de charge ou load balancing
* Ferme de serveurs, server cluster
* Serveurs maître distribue les tâches aux machines esclaves
* DNS dynamiques

Equilibrage de charge

NAS – Ethernet

SAN – eSCSI / eSATA

* Disponibilité
  + Temps de fonctionnement réel divisé par le temps de fonctionnement théorique : 99% (3,65jours hors service/an)
  + 99.9 % = 8,75H / an
  + 99,99% = 5,2min
* Sécurité :
  + 1 : Types d’attaque :
  + 5 p :
    - Probe (Sonde)
      * Ping, traceroute,mslookup, scan de ports
    - Penetrate (Intrusion)
      * Brute force, dictionnaire, faille de logiciels
    - Persist (Persistant)
      * Créer un accès admin en frause
      * Outil de contrôle à distance (cheval de troie)
    - Propagate (propager)
      * Sonder les failles du réseau
      * Propager l’intrusion
    - Paralyze (paraliser)
      * Endommager des systèmes ou des données systèmes
      * Utiliser les machines pour attaquer d’autres systèmes
  + 2 – Sion
    - Simple (Tentative de connexion aux serveurs/seulement dtectable)
    - Furif (Tentative d’échange des données sous connexion)
    - Détournement des normes rfc
    - Aveugle
      * Utiliser des machines intermédiaire
      * Spoofing, usurper identité d’une machine ou d’un équipement
      * Passif (snifing, enregistrer et analyser les communications réseaux)
  + 2. Attaques réseaux
  + 2.2 IP Spoofing (usurper IP)
  + 2.3 APR spoofing
  + Usurper MAC
  + 2/4 DNS Spoofing
  + Usurper DNS
* 2.5 Attaque per fragments
* Fragments overlopping, substitution de fragments

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  | X |  |  |

* Tiny fragments

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  | X | **X** |  |  |

2. Attaques réseaux

2.6 Détournement de session TCP

Ecouter le réseau et attaque l’authentification

Désynchroniser le client et le serveur en créer une latence

Usurper le client (ou serveur)

3. Attaques sur les logiciels

Configuration par défaut

Bugs

Déparsement de piles

Script

Injection sql