Supervision et infogérance

3 types d’infogérance :

* TMA

Support utilisateur et maintenance

* Gestion des infrastructure

Externalisation ou non de l’hébergement

* BPO

Externalisation de certains processeurs de l’entreprise(comptabilité, Ressource humaine, paye)

1. Supervision, monitoring

Niveau 1 :

Service disponible ou non 🡪 alerte

Niveau 2 :

Intervention ponctuelle des technicien

Niveau 3 :

Infogérance

Maj/Analyse de log/ sauvegarde/audit

1. Infogérance et protections

* Basculement on fail-over

Basculer automatiquement sur un equipement alternatif

2 modes

* Equipement secondaire en veille
* Equilibrage de charge

Retour à la normal, fail back

* Equilibrage de charge ou load-balancing
* Ferme de serveurs/server cluster
* Serveur maître distribue les taches au membre
* Equilibrage de charge

NAS Ethernet

SAN eSCSI

eSATA

* Disponibilité

Temps de fonctionnement réel\_\_\_\_\_

Temps de fonctionnement théorique

|  |  |  |
| --- | --- | --- |
| 99% | 3.65 jours | Hors service/an |
| 99.9% | 8.75 h | ///////////////////////////////// |
| 99 .999% | 5.2min | ///////////////////////////////// |

Sécurité

1. Type d’attaque

5point :

* probe(sonde)

Ping, traceroute, malookup

Scanner de port

* Penetrate(intrusion)

Brute force, dictionnaire

Failles des logiciel

* Persit(persistent)

Créer un accès administrateur en fraude

Outil de contrôle à distance (cheval de troie)

* Propagate(propager)

Sonder les failles du réseau local

Propager l’intrusion

* Paralyze(paraliser)

Endommager des systèmes ou des données

Utiliser les machines pour attaquer d’autre systèmes

1. Attaque réseau

* Simple

Tentative de connexion aux service

Facilement détectable

* Furtif

Tentative d’échange des donnés sans connexion

* Détournement des normes RFC
* Aveugle

Utiliser des machines intermédiaires

Spoofing, usurper l’identité d’une machine ou d’un équipement

* Passif

Spifing, enregistrer et analyser les communications réseaux

* 1. IP Spoofing

Usurper IP

* 1. ARP spoofing

Usurper MAC

* 1. DNS spoofing

Usurper DNS

2.4 Attaque par fragment

* Fragments overlopping, substitution de fragments

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | xxxxxxxxxxxxxx |  |  |

* Tiny fragments

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | |  |  | | --- | --- | |  |  | |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | |  | | --- | |  | |  |  |

* 1. Détournement de session tcp

Ecouter le réseu et attendre l’authentification

Désynchroniser le client et le serveur en criant une latence

Usurper client(ou serveur)

1. Attaque sur les logiciels

Configuration par défaut

Bug

Dépassement de pile

Script

Injection SQL

Homme du milieu(midle man)

SELECT \*   
FROM users   
WHERE nom =...

AND Mdp = ... ;(« password ; drop table user »)

1. DOS/DDOS

Déni de service distribué

* Inonder le service de demande d’échange de données
* Demandes de connexion sans suite
* Surcharger le service en demandes UDP

UDP prioritaire TCP

* Snurfling/ innonder de requêtes icmp(ping) en broadcast en usurpant l’identité de machines
* DDOS

DOS avec de nombreuse machines

1. Type de detection

IDS système de détection d’intrusion

Surveiller la mémoire et les procéssus

Trier les connexions  
Filtrer les communications sur la passerelle/routeur

1. Méthodes de detection

* Recherche de motif(pattern matching)
* Analyse de protocole à la recherche d’abus connus.
* Annalyse heuristique à la recherche de comportement inconnus
* Apporte probabilité/statistique