2. Familles

Bas débit -> 56 kb/s

8kb = 1kB

ADSL 13380 kb/s

SDSL 1024 kb/s

ADSL2+ : 25mb/s

IDSL ( Numéris ) 2 \* 64 kb/s

4.Limites

ADSL 2 Mb/s

ADSL 2+ 3Mb/s

Télé 4-5 Mb/s

Télé HD 8-10 Mb/s

5. Fonctionnement

Ligne non-dégroupée

Télécom

Box

Filtre

Filtre

PBAX

DSLAM

Dégroupage total :

Box

Téléphone

DSLAM

+Liaison filaire et Wifi

1. Liaison filaire

Réseau local LAN

Ethernet 10 Mb/s

Fast Ethernet 100Mb/s

Gigabit 1Gb/s

1. Wifi

* Normes :5

|  |  |  |  |
| --- | --- | --- | --- |
| **Normes** | **Nom** | **Vitesse** | **Distance** |
| 802.11a | Wifi 5 | 27-54Mb/s | 10 m |
| 802.11b |  | 6-11Mb/s | 300m |
| 802.11g |  | 25-54Mb/s | 300m |
| 802.11n |  | 100-300Mb/s | 100m |
| 802.11ac |  | 433-1300Mb/s | >300m |

* Infrastructure

Connexion à un point d’accès ( antenne )

* Ad Hoc
* Pont ( Bridge )
* Répéteur

Chiffrement :

WEP 64-128 Bits

WPA > 128 bits

WPA2

Supervision et infogérance

3)Types d’infogérance

- TMA : support aux utilisateurs et maintenance / lié aux clients

- Gestion des infrastructures : Externalisation ou non de l’hébergement / lié au matériel

- BPO : Externalisation de certains processus de l’entreprise ( compatibilité, RH, page )

1) Superviseur, monitoring

Niveau 1

Service disponible ou non 🡪 alerte

Niveau 2

Interventions ponctuelle des techniciens

Niveau 3

Infogérance

MAJ, analyse de log, sauvegarde, audit

2) Infogérance et prestations

- Basculement en fail-over : Basculer automatiquement sur un équipement alternatif

2 modes :

* Equipement secondaire en veille
* Equilibrage de charge

Retour à la normale, fail-back

* Equilibrage de charge ou loud-balancing

Forme de serveurs, server cluster

Serveur maître distribue les tâches aux machines esclaves.

NAS Ethernet

SAN eSCSI

* Disponibilité

Temps de fonctionnement réel divisé par temps de fonctionnement théorique

1. Types d’attaques

5P :

* Probe ( Sonde )

Ping, traceroute, mslookup, scanner de port

* Penetrate ( intrusion )

Brute Force, dictionnaire

Failles des logiciels

* Persist ( persistant )

Créer un accès administrateur en fraude

Outil de contrôle à distance ( cheval de troie )

* Propagate

Sonder les failles du réseau local

Propager l’intrusion

* Paralyze

Endommager des systèmes ou des données.

Utiliser les machines pour attaquer d’autres systèmes

1. Securité

* Scan simple : Tentative de connexion
* Furtif

Tentative d’échange de données sans connexion

* Détournement des normes RFC
* Aveugle

Utiliser des machines intermédiaires

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

* Passif

1. Attaques réseaux

b.2 IP Spoofing

USURPER IP

1. ARP Spoofing

Usurper MAC

1. DNS Spoofing

Usurper DNS

1. Attaque par fragments

* Fragments overlooping, substition de fragments

1. Détournement session TCP

Ecouter le réseau et attendre l’authentification

Désynchroniser le client et le serveur en créant une latence

1. Attaquer sur les logiciels

Configuration par défaut

Bugs

Dépassement de pile

Script

Injection SQL

Homme du milieu

1. DOS /DDOS

Déni de service distribué

* Inonder le service de demandes d’échange de données
* Demandes de connexions sans suite
* Surcharger le service en demandes UDP ( UDP prioritaire sur TCP)
* Smurfling (envoyer un ping en broadcast puis usurper l’identité d’une machine et recommencer jusqu’à que le réseau sature)

1. Type de détection

-IDS système de détection d’intrusions

-Trier les connexions

- Filtrer les communication sur la passerelle/routeur

6. Méthode de détection

- Recherche de motifs (pattern matching)

-analyse de protocoles à la recherche d’abus connu

-analyse heuristique à la recherche de comportements inconnus

-approche probabiliste/statistique