Sécurité

4 mots clés

Authenticité: Qui communique avec qui
Confidentialité: Sécurité des données confidentiel, en transmission et en stockage
Intégrité: Donné envoyer = donné reçu
Disponibilité: Service accessible

Un concept

Non répudiation:

Comment sécuriser le réseau d'une entreprise? diapo 3

Objectif de la sécurité: Qu'est ce qu'on sécurise
Moyens: Définir une politique de sécurité, surveillance des systèmes
Technique: Chiffrement, protocoles sécurisés, ...

Sécurité d'un système isolé diapo 4

Segmentation des différentes application (compte, droits), verrouillage de certain processus (chmod sur unix), ...

Sécurité d'un système appartenant à un réseau diapo 5

Configuration des services: Qu'elle sont les services nécessaires, qu'elle sont les droits, choix des implémentations, maintenir le système a jours, ...
Contrôle des services actifs: examiner les services en attente, de l'intérieur (netstat) ou de l'extérieur (nmap)

Sécurisé un réseau diapo 6

Au niveau Réseau (pour un réseau isolé par un équipement)

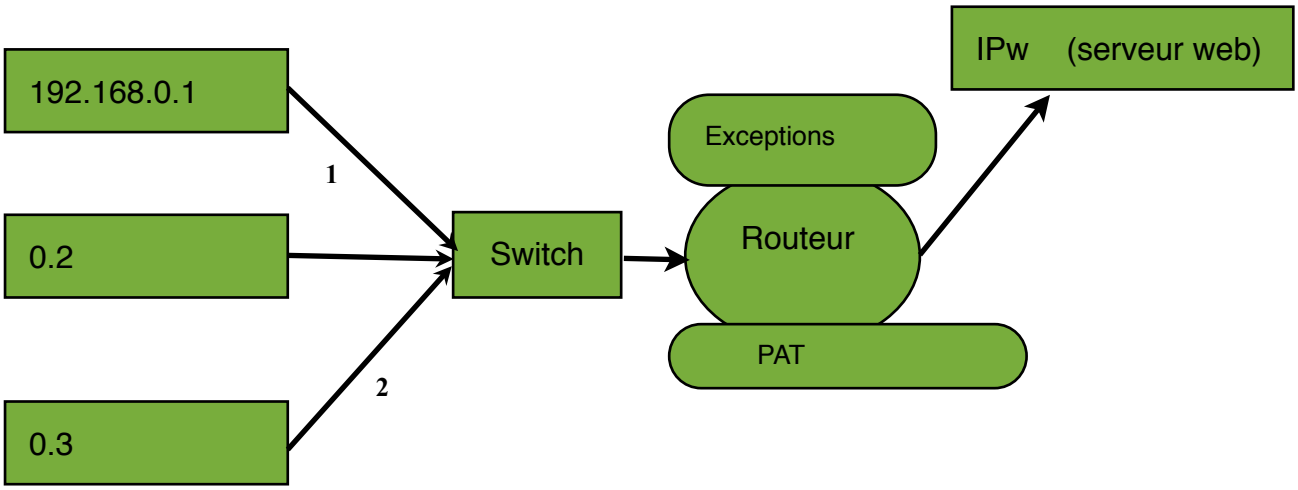
- identification du réseau et des systèmes qui le composent
- Utilisation d'adresse privées (RFC 1918)
    - Classe A: 10.0.0.0
    - Classe B: 172.168.0.0 à 192.168.255.0
    - Classe C: 192.168.0.0 à 192.168.255.0

- Protection par le routeur
    - NAT
    - PAT Port Address translation
    - Pare-feu
    - ....

Le NAT statique: diapo 7
Le NAT Dynamique: diapo 7, 8, 9, 10

IP masquerading => N adresse IP vers l'extérieur, limitation du nombre de connexion simultané à ces N adresse, une adresse de sortir pour une station

PAT => une adresse ip vers l'extérieur



PAT

entré @IP	entré n° port	sortie @IP	sortie n°port
IP1	4000	IPw	4000
IP2	4000	IPr	4001
IP10	21	IPr	20
IP10	8080	IPr	80

Excepti
ons

1

IP source	IP dest	Port Source	Port dest	header
IP1	IPw	4000	80	H

2

IP source	IP dest	Port Source	Port dest	header
IP2	IPw	4000	80	H

Sécurité d'un ensemble diapo 12

deux solutions:

- **Médiums privée:** le plus fiable, problème c'est cher !!
- **VPN:** communication encapsulé et crypté, moins onéreux

Chiffrement diapo 13
Chiffrement: principes diapo 14,15
Chiffrement: utilisation diapo 16
Exemple diapo 17
Protocole SSL diapo 18
Sécurité WIFI diapo 19

WPA -> remplacent du wep, il s'inspire du Wep, en introduisant des changement de vecteurd d'initialisation, ... toutes les 2 minutes (TKIP)

WPA 2 -> serveur radius qui contient les login et le mot de passe (comm en AES avec ce serveur)

Protocole Kerberos diapo 20, 21

IPODAH à voir !