FIREWALLS

-

Brice FOURNIER
Pierre KILLY
Vincent JAQUES

Firewall à filtrage de paquets

- Deux catégories :
  - Firewall stateless
  - Firewall stateful
- Filtrage de niveau 4 (voir niveau 5)
  - Adresse ip source et destination
  - Port TCP / UDP source et destination

- Exemple de firewall statefull avec NetFilter
  - Quatre états de paquets
    - New
    - Established
    - Related
    - Invalid
  - Module de suivi de protocole
    - Filtrage niveau 4, couche transport
      - Suivi de TCP
      - Suivi de UDP
      - Suivi de ICMP

- Module de suivi applicatif
  - Filtrage niveau 5, couche session
  - Exemple FTP :

    IPTABLES -A FORWARD -m state **–state ESTABLISHED** -j ACCEPT

    IPTABLES -A FORWARD -m state **–state NEW -p tcp –sport 1024: -d $FTP_SRV –dport 21** -j ACCEPT

    IPTABLES -A FORWARD -m state **–state RELATED -p tcp -d $FTP_SERV –sport 20 –dport 1024:** -J ACCEPT

    IPTABLES -A FORWARD -m state **–state RELATED -p tcp –sport 1024: -d $FTP_SRV –dport 1024:** -J ACCEPT

- **Limites**

  - Tout bloquer est inutile (sinon bah, autant rester chez soi, hein non mais ho, allez faire l'hermite ailleurs !).

  - Pas d'analyse des données : l'accès aux services accordé peut être utilisé pour passer les attaques (ex: port 80, voir la démonstration en fin d'exposé).

Les bridges firewallant

La solution discrète ...

- Fonctionnement proche d'un commutateur
- Transmet les paquets en fonction de l'adresse MAC
- Interface réseau d'administration

Les bridges firewallant

... Mais efficace !

- Firewalling par filtrage de paquets
- Sous Linux : iptables
- Filtrage sur la règle FORWARD
- Malgré tout détectable

Les firewalls mandataire

- Filtrage applicatif
- Fonctionne avec des agents spécifiques
- Filtrage en sortie ou en entrée

Filtrage en sortie

- Notion d'authentification
- Filtrage par adresse via une base
- Mode proxy ou mode transparent

Filtrage en entrée

- Protège les serveurs de l'extérieur
- Spécifie les fichiers accessibles
- Filtre les requètes potentiellement dangereuses

Firewalls Personnels

- Utilisation essentiellement cliente
- Nouvelle approche : Filtrage par application
- Liste blanche, liste noire, comportement par défaut
- Poste de travail ou portable en réseau d'entreprise ou directement relié a Internet

- **Atouts**

  - Identification de l'application :
    - Nom de l'application
    - Chemin dans le système de fichiers
    - Somme MD5 de l'exécutable

  - Configuration par :
    - Jeu de règles par défaut
    - Méthode intéractive d'autorisation des applications et flux
    - Configuration simple et remontée d'alerte

- Deux classes de produits :
  - Simples : oui / non
  - Evolués : oui / non avec restriction de flux
  - Tous proposent un suivi de niveau 4 pour TCP

- **Limites**
  - Utilisateur non compétent
  - Signalisation peu explicite et rébarbative
  - Jeu de règle par défaut faible
  - Difficulté de limiter certaines applications
  - OS mal configuré (FAT32, comptes superutilisateurs)

Références

- Linux Magasines Hors Série n°12 et n°13, Le Firewall, votre meilleur ennemi, Acte I et Acte II

- Atouts et limites des pares-feu personnels de Cédric Blancher, http://www.sstic.org/SSTIC03/presentations/Firewalls_personnels___C._Blancher/SSTIC03-Blancher-Firewalls_personnels.pdf