Les IDS / IPS

Intrusion Detection/Prevention Systems

CIKALA Frédéric
LATAIX Rémy
MARMECHE Samuel
Ingénieurs 2000 - IR3

Plan de l'exposé

I) La sécurité, à l'heure actuelle

II) Les différentes attaques

II) La solution « passive », l'IDS

IV) La solution « active », l'IPS

V) Limites des IDS/IPS

VI) Bilan et conclusion

La sécurité, à l'heure actuelle

- Les entreprise sont de plus en plus dépendantes de la santé de leur Système d'Information (SI)
- Paradoxe :
  - 60% des gens interrogés se disent confiants en leur SI
  - ¼ des entreprises ont appliqué une réelle politique de sécurité

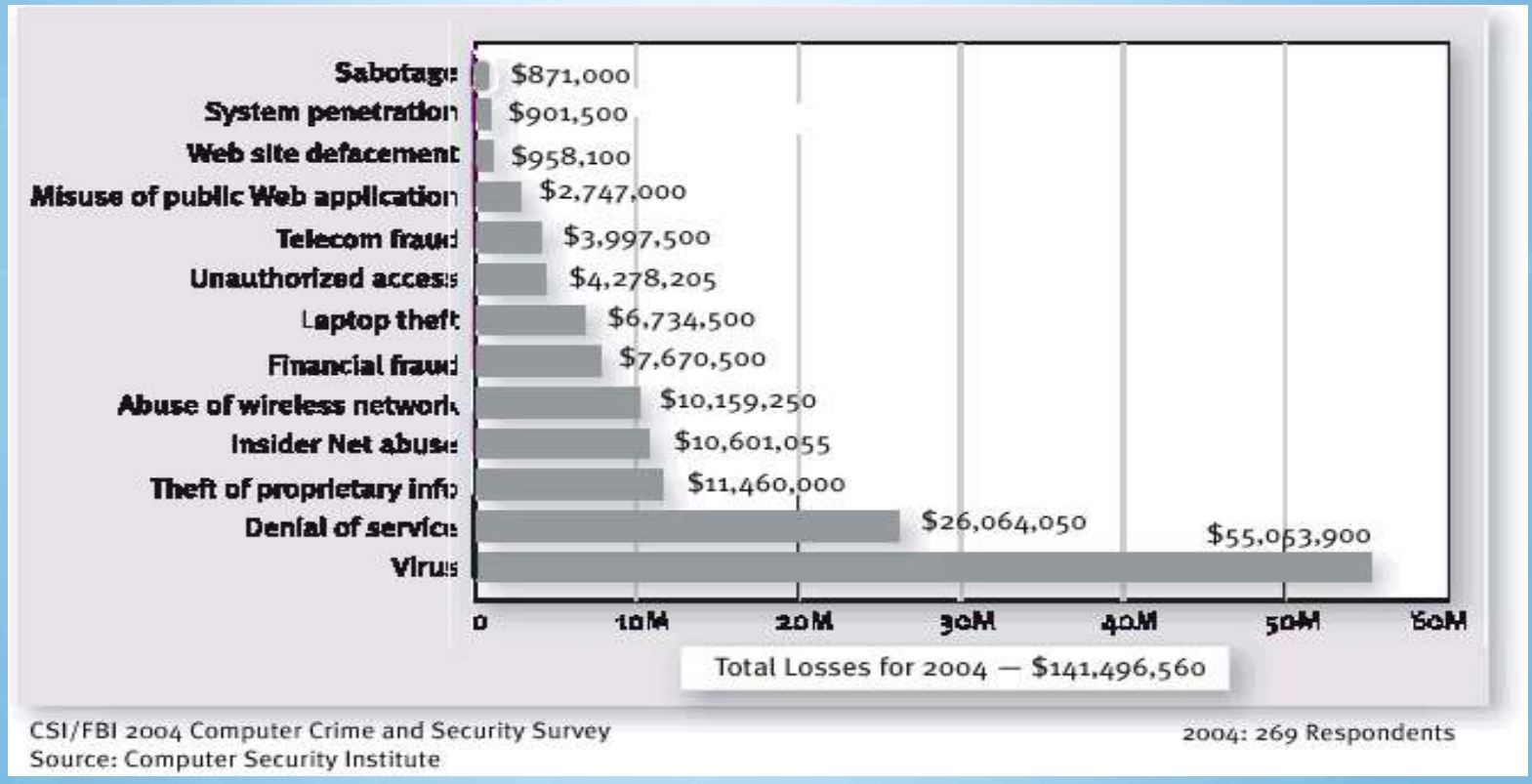
  -> Manque de moyens et de sensibilisation au sein des entreprises

Des risques bien réels

- Les faits marquants de vols de sources de données:
  - Microsoft, fuite de 600 Mo de code source sur les SP de NT 4 et 2000, Mainsoft à l'origine de la fuite
  - Cisco, 800 Mo de l'IOS 12.3 en téléchargement sur un site russe
  - Vol des codes sources du Firewall PIX 6.3.1 et mis en vente sur des newsgroups

(source : CERIF)

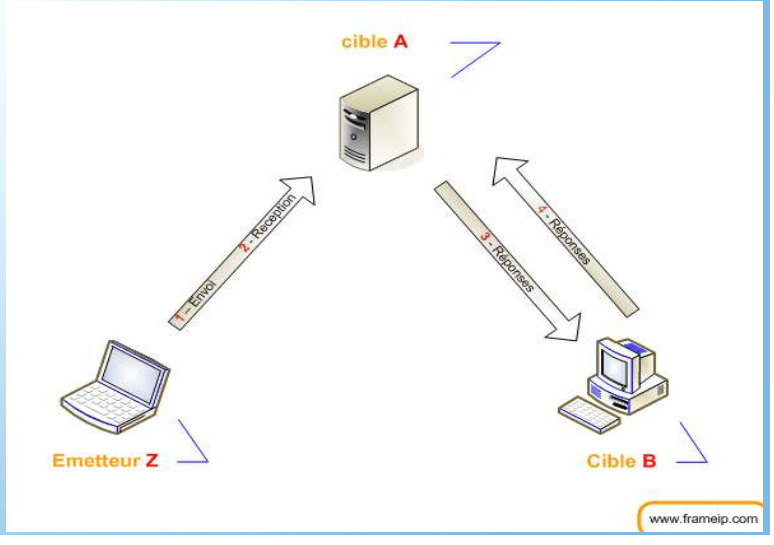
Des chiffres évocateurs



Les différents types d'attaques

Plusieurs types d'attaques

- ►Le scanning :
  - Le balayage de connexion TCP/UDP
  - TCP/IP Stack Fingerprinting
- ►Le spoofing :
  - Usurpation d'identité
  - ARP, DNS
- ►Le flooding :
  - SYN Flooding



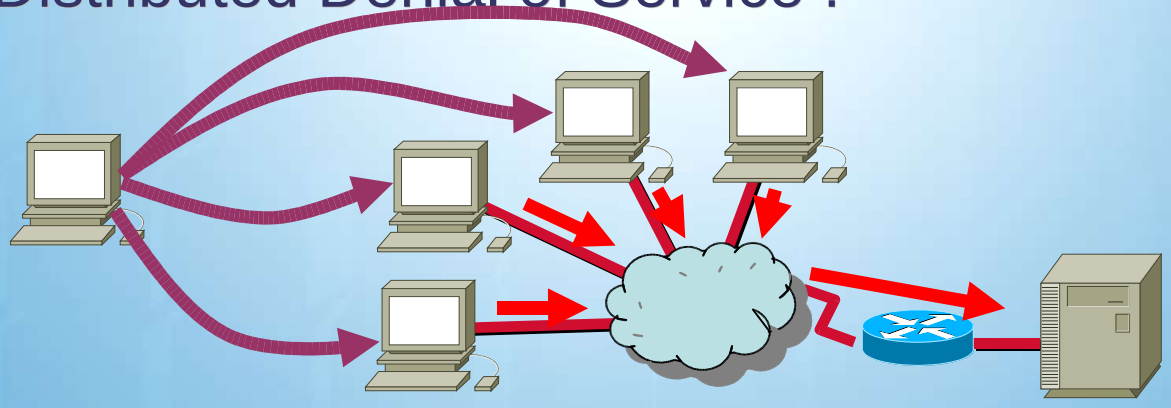
Les différents types d'attaques

- Failles TCP:

  TCP Hi-Jacking

  TCP Sequence Number Guessing

- Le Distributed Denial of Service :



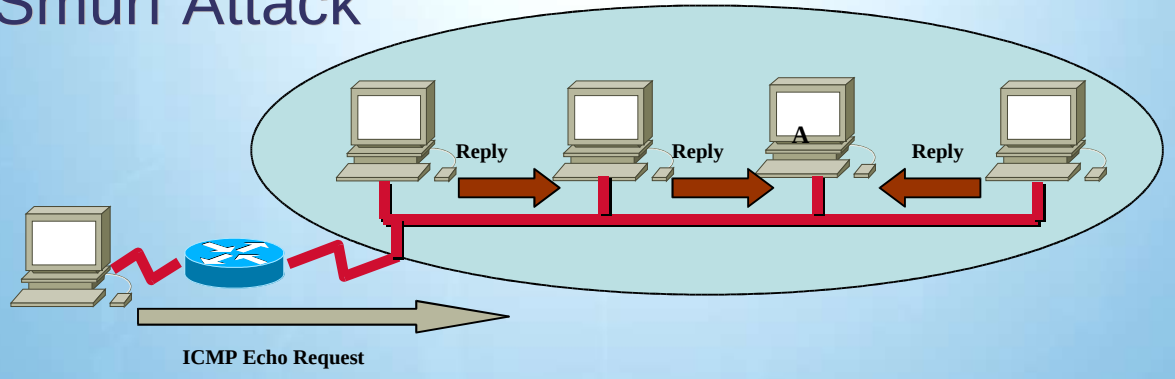
Les différents types d'attaques

- Failles ICMP :

  ICMP-Redirect

  Ping of the Death

  Smurf Attack



La solution « passive » : Les IDS

- Deux principes de détection d'intrusion :

  - Systèmes neuronaux : se basent sur la détection d'anomalies, après une période d'apprentissage d'un flux normal

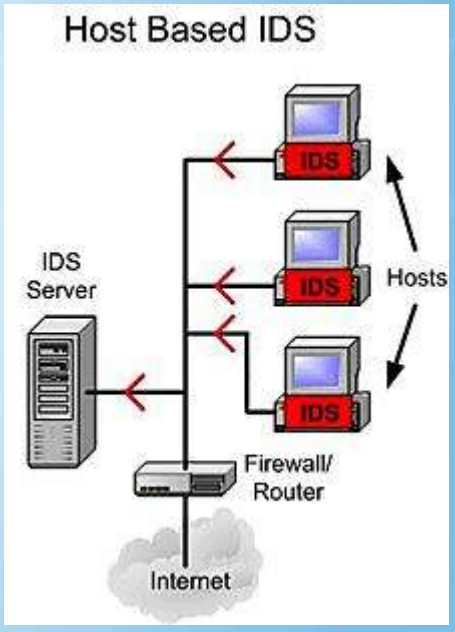
  - Systèmes à base de signatures : s'appuient sur des empruntes d'attaques afin de détecter l'intrusion (pattern matching, approche par scénarii).

La solution « passive » : Les IDS

- Deux niveaux de détection d'intrusion :
  - Niveau système (log, historique , ressources),

    Il s'agit d' « Host IDS »,

    Passe par les daemons syslogs, par exemple.



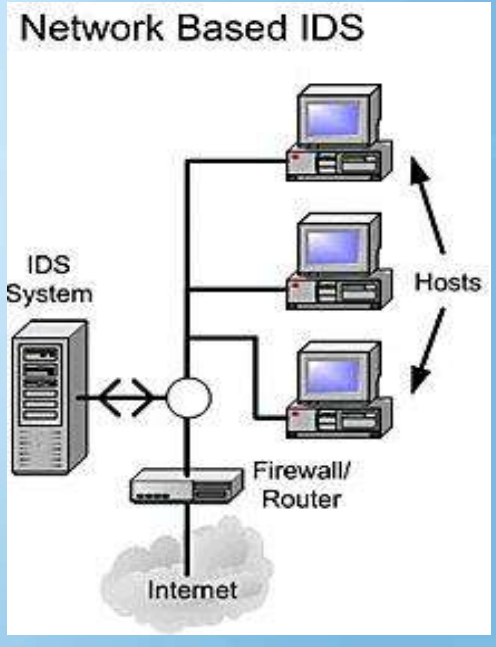
La solution « passive » : Les IDS

- Niveau réseau (paquets véhiculés),

  Il s'agit de « Network IDS »,

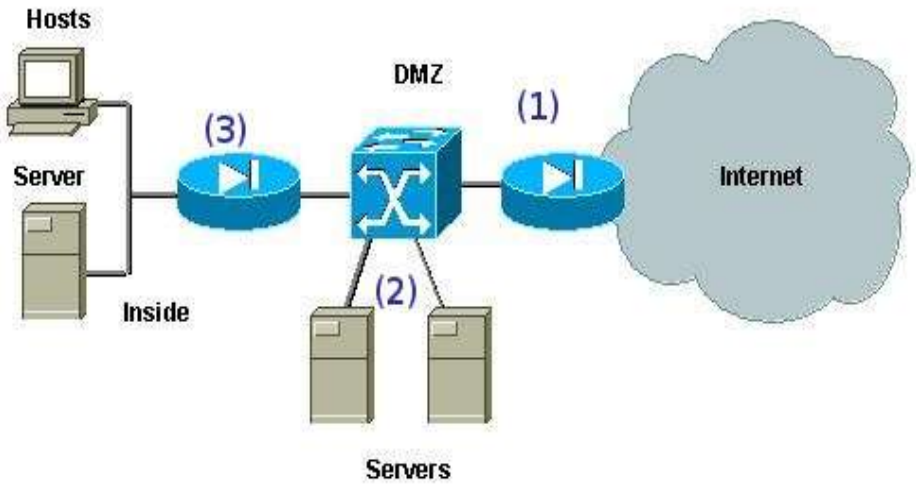
  Carte réseau en mode promiscuous,

  Positionnement stratégique.



La solution « passive » : Les IDS

- Où positionner un IDS ?



1) Capte toutes les attaques, très verbeux,

2) Capte les attaques filtrées par le firewall, d'un certain niveau,

3) Capte les attaques provenant de l'intérieur.

La solution « active » : les IPS

Ensemble de technologies de sécurité

- But

  Anticiper et stopper les attaques

- Principe de fonctionnement

  Symétrie avec IDS -> Host IPS & Network IPS,
  Analyse des contextes de connexion,
  Automatisation d'analyse des logs,
  Coupure des connexions suspectes,

La solution « active » : les IPS

- Fonctionnalités :
  - Compréhension des réseaux IP (architecture, protocoles...)
  - Maitrise des sondes réseau / Analyse des logs
  - Défense des fonctions vitales du réseau
  - Vitesse d'analyse
  - Mode 'statefull Inspection'

La solution « active » : les IPS

- Concept commercial,

  Cisco – « Des réseaux capables de se défendre tout seuls ».
  Le moteur ASQ de NetAsq
  Symantec

- Technologies hétérogènes mises en interaction :
  pare-feu, VPN, IDS, anti-virus, anti-spam, ...

Limites & Contraintes - IDS

- Limites humaines : mise à jour de la liste des signatures,
- implémentation sur le réseau, utilisation du mode promiscuous -> 1 sonde par réseau commuté
- pour le comportemental : changement de la configuration du réseau
- pertinence de l'information, false-positive

Limites & Contraintes - IDS

- 6 catégories principales de techniques de contournement:
  - insertion : ajouter des données aux flux présents
  - élimination : rendre l'IDS inutile ou inexploitable
  - substitution : échange tout ou une partie du contenu incriminable

Limites & Contraintes - IDS

- fragmentation : découpé un contenu ou des opérations
- distribution : répartition des sources
- confusion, : rendre le contenu incompréhensible

Limites & Contraintes - IPS

- Mise en place délicate,
- Administration rebutante,
- Possibilité de bloquer tout le réseau dans le cas de fausse alertes
- Pas de standard, assimillé à un concept marketing (« buzzword »)

Bilan et conclusion

- Les IDS/IPS apportent un plus indéniable aux réseaux dans lesquels ils sont placés.

- Cependant, leur limites ne permettent pas de garantir une sécurité à 100%, impossible à obtenir. Il faut alors y tendre ....

- Le futur de ces outils permettra de combler ces lacunes en évitant les « faux positifs » (pour les IDS) et en affinant les restrictions d'accès (pour les IPS)

Merci de votre attention ^^

Si vous avez des questions ...