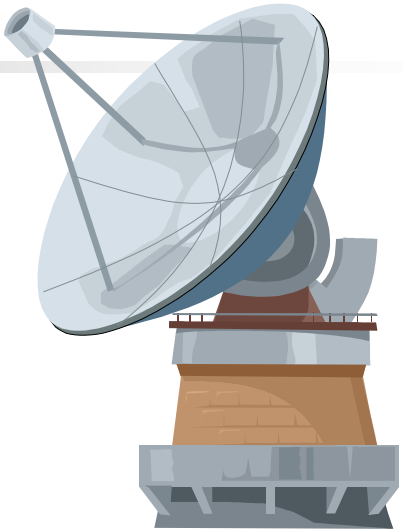
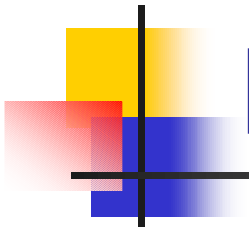
Système de Détection d'Intrusions (IDS)



Liyun LI *IR5*

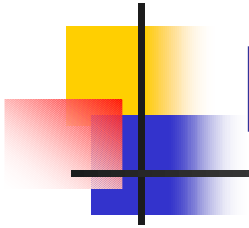
liyun@free.fr



Plan

Introduction

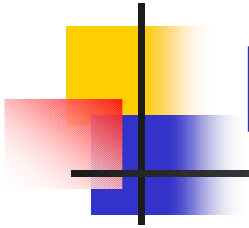
- Quelques chiffres sur le piratage
- But de la sécurité
- Définition d'une attaque et d'une intrusion
- 2 types de sécurité: active et passive



Plan (partie 2)

IDS

- Qu'est ce qu'un IDS ?
- L'utilité d'un IDS
- Types d'IDS: NIDS et HIDS
- Complémentarité des IDS
- Etude d'un NIDS basic: TCPDUMP
- Etude des fonctionnalités de Snort (NIDS)
- Etude d'un HIDS : Tripwire

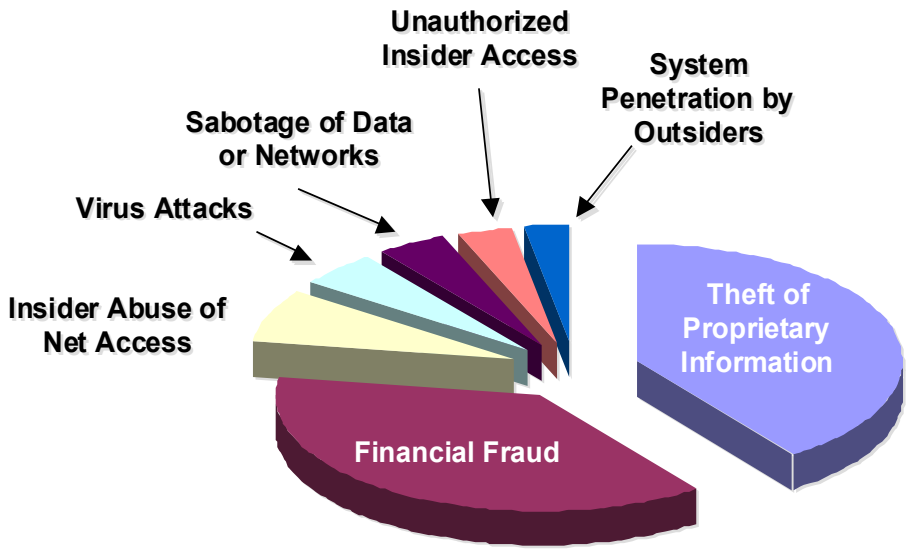


Plan (partie 3)

- Les types d’attaques
- Les Honeypots: les leurres

- Quelques bonnes habitudes
- Avenir des IDS
- Conclusion

Quelques chiffres

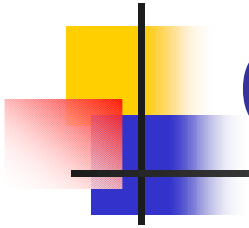


Type of Intrusion	$ Losses	%
Information Theft	42,496,000	**40%**
Financial fraud	39,706,000	**37%**
Abuse of net access	7,576,000	**7%**
Virus attacks	5,274,000	**5%**
Sabotage	4,421,000	**4%**
Insider misuse	3,567,000	**3%**
Outsider Penetration	2,885,000	**3%**
Total	$105,925,000	

Source: “1999 CSI/FBI Computer Crime and Security Survey” Computer Security Institute - www.gocsi.com/losses.htm

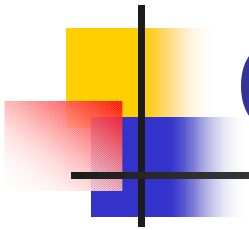
But la sécurité informatique

- Protéger un réseau qui est connecté à d'autres réseaux non sécurisés (ex: Internet)
- Autoriser l'accès à certains services **uniquement**. (Web, mail, ftp…)
- Se prémunir contre des attaques et intrusions



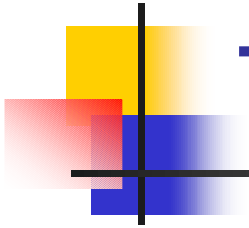
Qu’est ce qu’une attaque ?

- Découverte systématique d’**informations** du réseau par des **scans** de port et **balayage** du réseau.
- Tentative réelle d’intrusion dans un réseau



Qu’est ce qu’une intrusion ?

- Prise de contrôle à distance (totale ou partielle) d’un ou de plusieurs serveurs ou hôtes
- Dans 9 cas sur 10, une intrusion est précédée d’une attaque

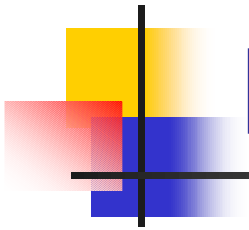


Type de sécurité

- Schématiquement il existe 2 types de sécurité:
- La sécurité active
  - Action sur sur les flux (autorisation , interdiction…)
  - Pare-feux, relais applicatifs, relayeur de messagerie…
- La sécurité passive
  - N'agit pas sur les flux entrants
  - Tente de reconnaître des flux hostiles
  - IDS

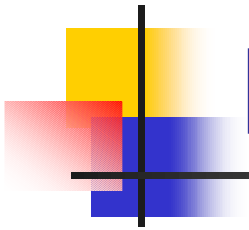
Qu'est un Internet Detection System (IDS) ?

- C'est un système qui détecte (tente de détecter) les intrusions
- C'est un processus de découverte et d'analyse de comportements hostiles dirigé contre un réseau



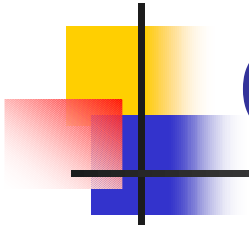
Pourquoi un IDS ?

- La sécurité active n'est pas suffisante
  - Le pare-feux ne contrent pas toutes les menaces.
  - Innovation constante des techniques de hacking
  - Faille potentielle selon les fonctionnalités des systèmes
  - Failles inhérentes de certains OS ;-)



Pourquoi un IDS (2)

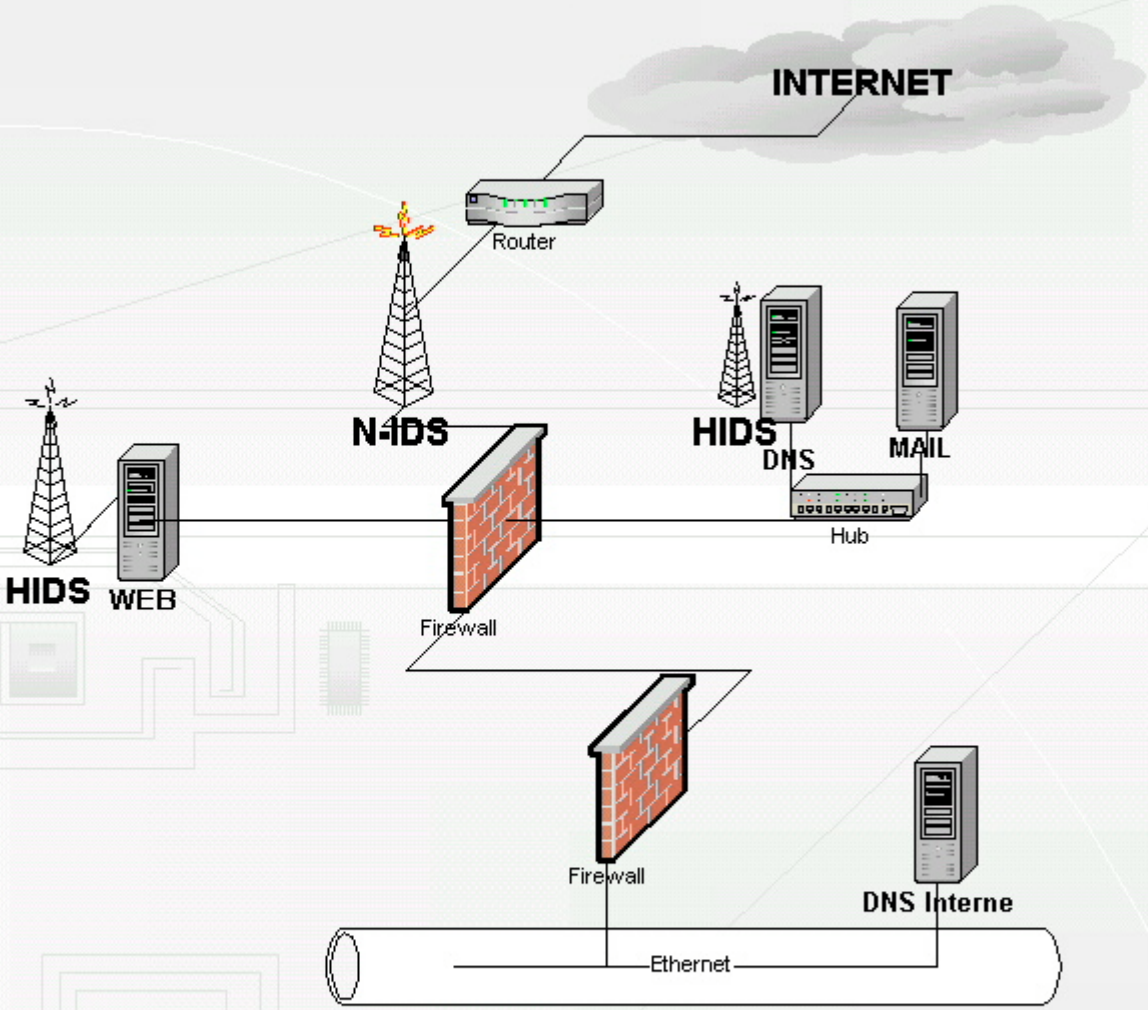
- Remonter la source de l'attaque
- Détecte les techniques employés
- En cas d'intrusion, les traces sont preuves tangibles

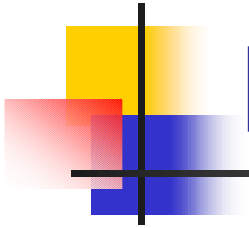


Complémentarité

- NIDS : détecte les (tentatives) d'intrusions grâce à une base de signatures
- Mais il n'ARRETE pas l'intrusion !!
- Capture les infos et les techniques de l'attaquant
- Aide indispensable pour se prémunir des intrusions en prenant les mesures de sécurité adéquates

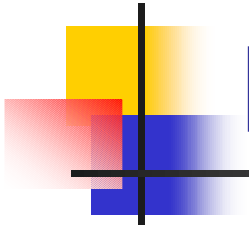
Place des IDS





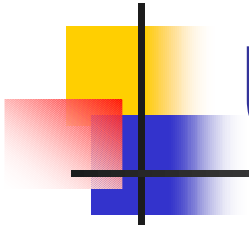
Plusieurs types d'IDS

- Les **NIDS** : Network Internet Detection System
- Les **HIDS** : Host Internet Detection System
- Les systèmes hybrides :mélange de HIDS et NIDS
- **Honeypots** : « pots de miel », leurres



NIDS et HIDS: généralités

- Les NIDS analysent des flux réseaux
- Les HIDS se basent sur la surveillance des hôtes par l'analyse des logs de l'hôte.
- Les 2 sont complémentaires



Un NIDS de base : Tcpdump

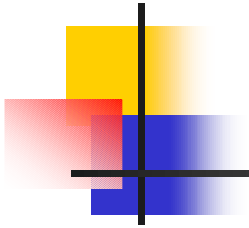
- Outil de base indispensable pour l'analyse réseau
- Disponible sur toutes les plateformes UNIX
- Permet l'écriture de filtres simples pour surveiller des types de traffic

- Exemple de mise en situation dans le scan suivant:

Exemple simple de scan

¦Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)

- ¦Interesting ports on (192.168.1.30):
- ¦Port State Service
- ¦53/udp open domain
- ¦
- ¦Nmap run completed -- 1 IP address (1 host up) scanned in 1 second



Exemple commande

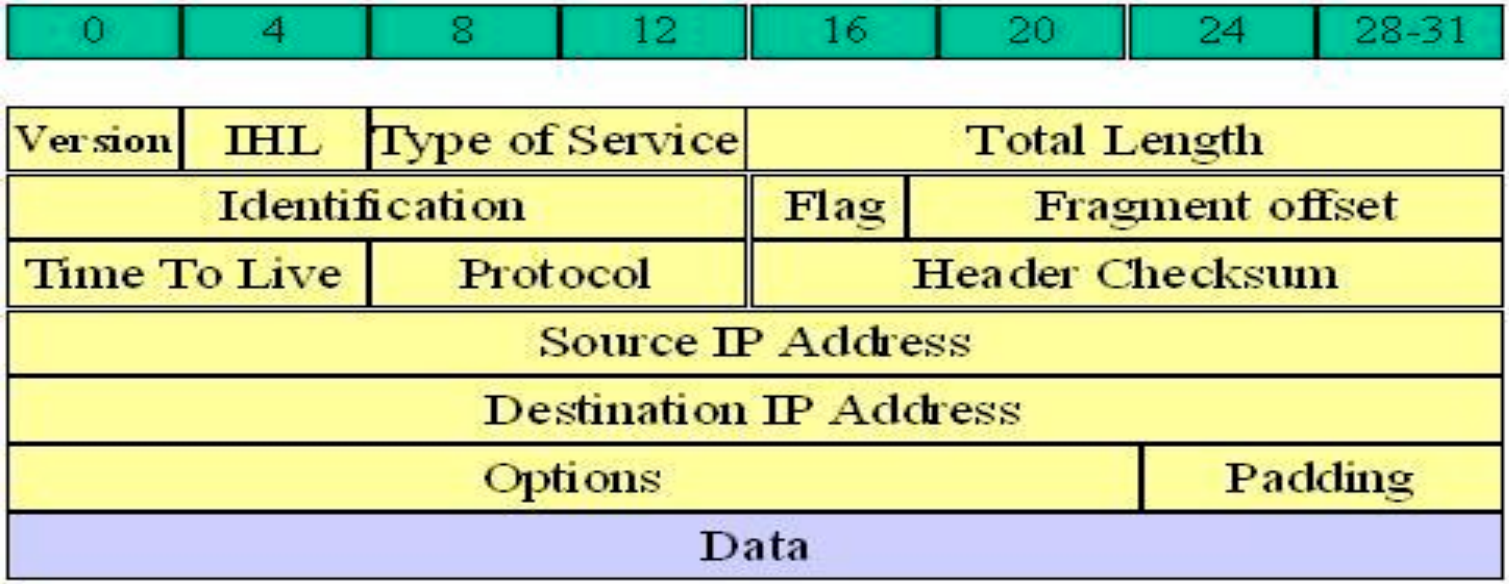
tcpdump host 192.168.1.30 and ip[9]=17,

qui signifie

« Affiche moi sur la sortie standard tous les datagrammes dont le 9ème octet est à 17, protocole UDP (cf Datagramme IP) »

Datagramme IP

Datagramme



Exemple de sortie tcpdump

Si sur la machine 192.168.1.30 ,root tape:

```
tcpdump host 192.168.1.30 and ip[9]=17 -n
tcpdump: listening on eth0
```

05:06:08.294790 192.168.1.1.43976 > 192.168.1.30.53: 0 [20484q] [43012n] (0)

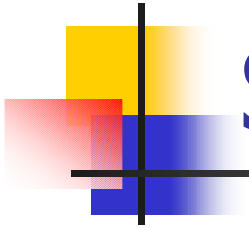
05:06:08.624790 192.168.1.1.43977 > 192.168.1.30.53: 0 [20484q] [43012n] (0)

Sur cette sortie, la cible verra que tous les datagrammes UDP sur le port domaine (53). Ici en 192.168.1.1 essaie de communiquer avec le port 53 de 192.168.1.1

Tcpdump est l 'outil de base pour le traffic résesau

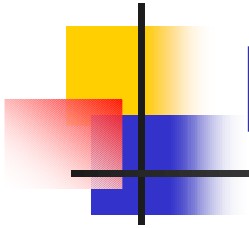
Snort : NIDS puissant

- Logiciel open source,modulaire et de petite taille
- Auteur : Martin Roesh
- Version actuelle 1.81
- Détection en temps réel
- **Gigantesque** bibliothèque de signatures d'attaques constamment mise à jour



Snort

- Fichier de configuration simple
- Langage de description simple et facile à utiliser
- Partie en-tête
  - spécifie les filtrages sur les adresses, les ports sources et destinations, ainsi que la direction et l'action (alert, pass, log)
- Partie configuration



Fonctionnalités

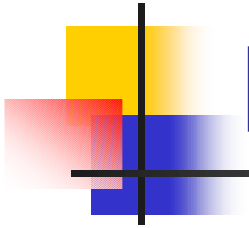
- Détecte la l'attaque par fragmentation IP
- Détecte de nombreux protocoles (IP, TCP, UDP, ICMP,…)
- Détecte les scans de ports initié par nmap

Extrait d'un exemple

- alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-ATTACKS chown command attempt"; flags:A+; content:"/usr/sbin/chown";nocase; sid:1338; rev:1; classtype:web-application-attack;)

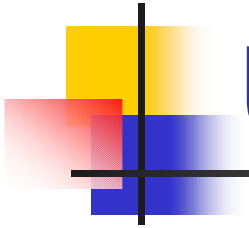
- **Explication:**

  Si Snort voit un paquet à destination du serveur Web port 80 avec un le drapeau ***ack*** positionné à 1 et contenant comme données « ***/usr/sbin/chown*** », alors une alerte est envoyé vers l'administrateur



HIDS

- Host IDS
- S’installe sur un serveur
- Avertit l’administrateur en cas de compromission de l’hôte
- Est basé sur l’intégrité du système

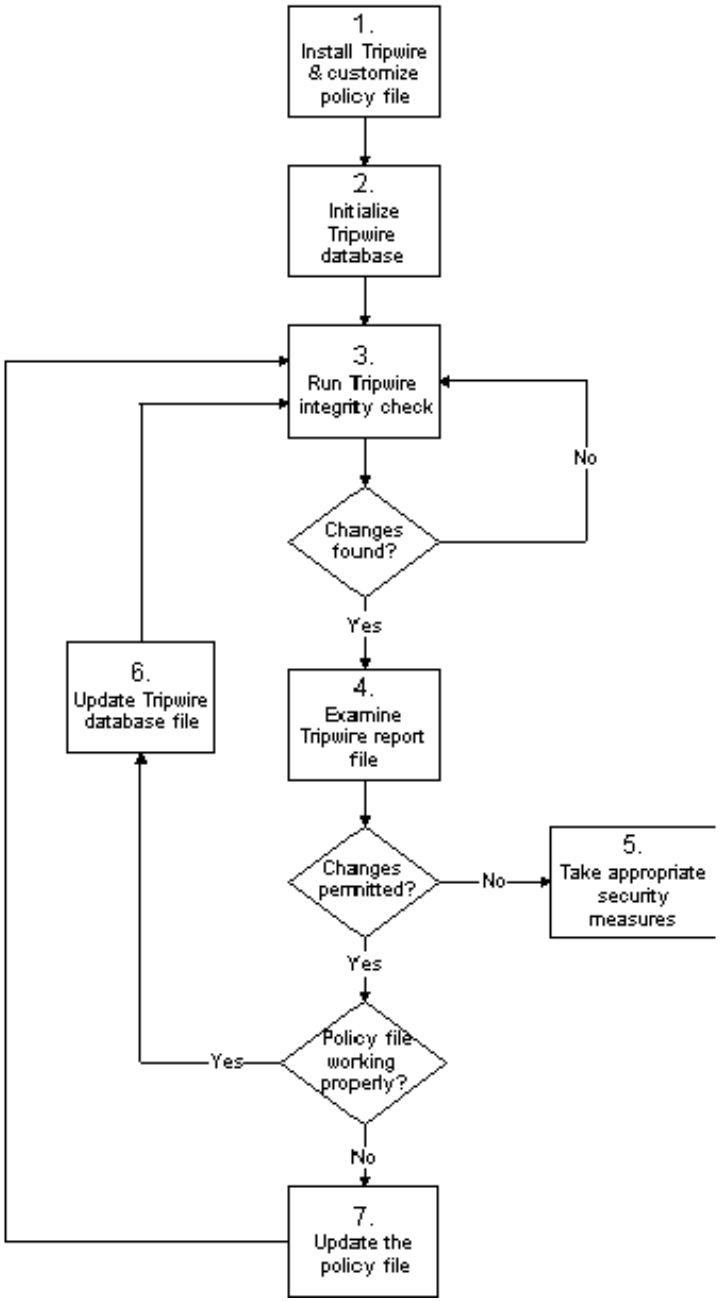


Un HIDS : Tripwire

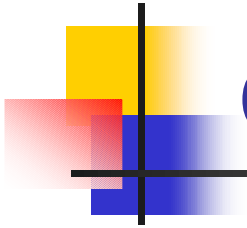
- Tripwire compare les résultats avec la base de référence générée préalablement (md5)
- *Parce que l'empreinte générée sur un fichier ne peut être reproduite deux fois à l'identique*

Tripwire

- Tripwire en schéma
- (source redhat)

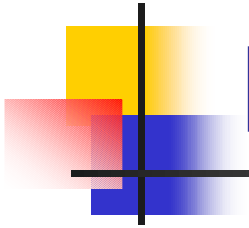


Tripwire :cas d'utilisation optimal



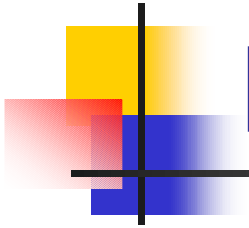
- Stocker les exécutables sur support amovible protégé en écriture (disquette, lecteur zip…)
- Vérifier quotidiennement (via cron) l'intégrité des fichiers systèmes critiques !

Exemple simple



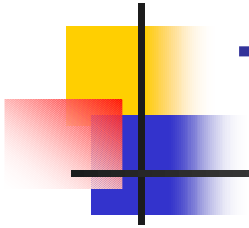
- Le fichier /etc/tripwire/twpol.txt liste la l'ensemble des fichiers à protéger pour lesquels il génère un checksum

- Exemple : supposons qu 'on ai réussit à modifier la commande « cat » en « cata »
- Envoie d'un mail à root lors de la prochaine vérification de l'intégrité



Faiblesse des NIDS

- Peu performants sur les réseaux Ethernet 100 Mb
- Ne détecte pas tout !
- Techniques pour contrer les NIDS évoluent
- Peu d'années d'expérience
- Demande du personnel paranoïaque ☺

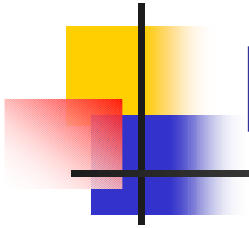


Types d’attaques

- Attaque Mitnick
- Attaque Teardrop
- Attaque Land
- Attaque DOS

Honeypots (Pots de miel)

- C'est un système pour leurrer le pirate
- Principes
  - Mise en place de faux serveurs avec peu de protection.
  - Simulation de l'activité d'un réseau
- But: récolter les traces et les techniques de l'attaquant



Portsentry: un IDS actif

- Logiciel libre
- Détection des scans de ports furtifs ou non
- Quant Portsentry détecte les scans de ports spécifiés dans /etc/portsentry/portsentry.conf, alors il agit

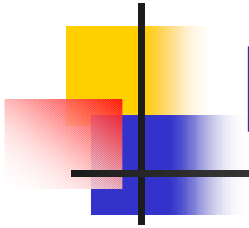
3 méthodes de **réaction dynamique**

Méthode 1

Si TCPWrapper est installé:

- Ajout dynamique dans /etc/hosts.deny de l'adresse IP de l'attaquant et lui interdit tous les services

ALL: $TARGET : DENY



Méthode 2 et 3

Méthode 2:

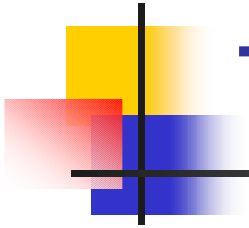
- Ajout d'une règle dynamique dans les règles du firewall

```
# iptables -I INPUT -s $TARGET -j DENY
```

Méthode 3 :

Refus de routage explicite vers l'agresseur qui se fait aussi dynamiquement

```
#route add -host $TARGET reject
```

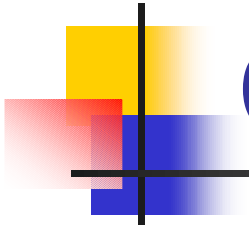


TCPWrapper

- TCPWrapper travaille main dans la main avec inetd.
- En fonction des services demandés, TCPWrapper peut les refuser ou les accepter
- L'idée est la suivante :

  Refuser tous les hosts par défaut à exploiter les services du serveur

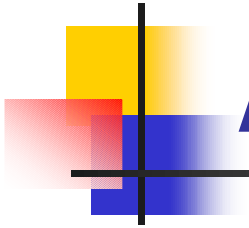
  Puis d'autoriser explicitement l'ip des hosts à accéder à aux services demandés



Quelques bonnes habitudes !

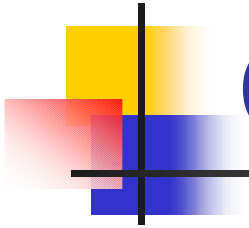
- Lors de l'installation d'un nouveau programme, tester la valeur de retour md5sum sur un programme pour vérifier son intégrité

- Banissez les rhost, rlogin, rexec, rsh rlogin, telnet ..!!!
- … car les mots de passe circulent en clair sur le réseau
- Utiliser ssh à partir des versions 2.9.x, (pensez à dsniff et l'attaque man-in-the-middle par Dug Song)



Avenir des IDS

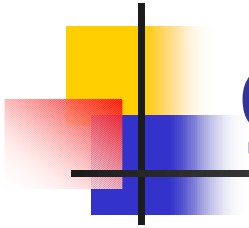
- LIDS (Linux IDS)
- Evolution de Snort
- Portsentry, Shadow



Conclusion

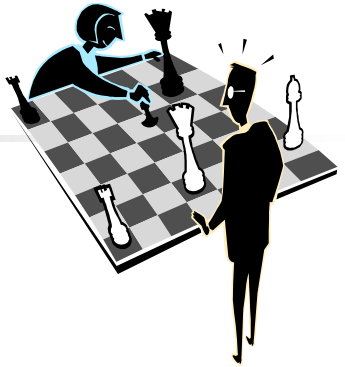
- Les HIDS et les NIDS sont des éléments qui contribuent à améliorer la sécurité des réseaux.
- Mettre à jour aussi souvent que possible les bases de signatures d'attaques (cf www.snort.org)
- Temps de réaction rapide pour rester efficace

Conclusion: le cocktail gagnant

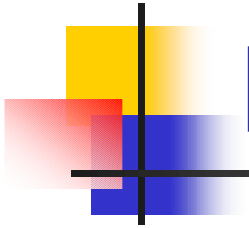


- Plus les données sont vitales, plus les mesures de précautions doivent être paranoïaques !
- Aussi, utilisez une package de logiciels libres composés de
- { Iptables, TCPWrapper, Snort, Portsenty }
- Et ……. **LIRE** les logs ☺

Le mot de la fin



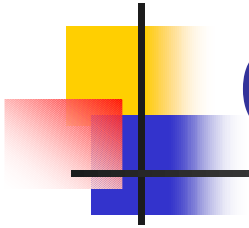
- La sécurité : c’est comme une partie d’échecs contre les pirates !!



Plus d'infos

- *Shadowconf*, Shadow Team

- *Détection des intrusions réseaux* Stephen Nortcutt, Judy Novak, Donald MacLahan editions Campus Press



Quelques sites

- www.snort.org
- www.linuxsecurity.com
- www.securityfocus.com
- http://www.robertgraham.com/pubs
- http://www.hsc.fr/ressources