Sécurité des Réseaux et d'internet

Yves Laloum

CNAM

1. Menaces et vulnérabilités sur l'Internet

- Connaître et comprendre les vulnérabilités et les menaces
  - ⇨ niveau réseau : sniffers / scanners / pb protocole IP (smurfing, flooding, etc) / pb switches et routeurs
  - ⇨ niveau système : identification / chevaux de troie / rootkits / mots de passe / DoS / attaques locales / bogues et trous de sécurité / scripts / virus / vers
- Les expérimenter par la prise en main des outils du pirate et par des tests d'intrusion

Qui sont les attaquants ?

- Amateurs (sensations fortes)
- Employés (vengeance, colère)
- Concurrents et opportunistes (banques, e-commerce)
- Crime organisé / terroristes (argent)
- Gouvernements / Espionnage international (politique / militaire)

Quelques mythes et idées reçues

- “Nous sommes protégés par un firewall”
- “Notre site ne risque rien : pas assez intéressant”
- “Achetez ce produit : vous serez en sécurité”
- “Nous avons un système de détection d’intrusion infaillible”
- “Le paiement en-ligne est sécurisé et sans risque”
- “Le chiffrement est LA solution à la sécurité”

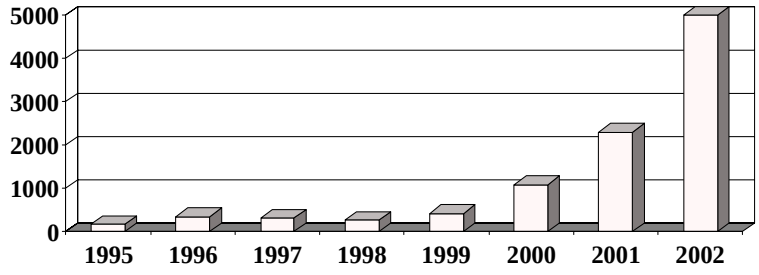
$\Rightarrow$ FAUX

Evénements marquants

- Attaques des sites CNN, Yahoo, Amazon, e*trade
- Virus “I LOVE YOU”
- Vol de 55000 numéros de cartes bancaires par un Russe
- Vol de fichiers médicaux (5000 patients)
- Faux communiqué de presse fait perdre 40% aux actions d’une société
- Nouvelle forme d’attaque : DDoS

Quelques chiffres

Nombre de vulnérabilités découvertes par an
(tous OS confondus. Source : CERT)



Exemple : www.doj.gov
(Department Of Justice)

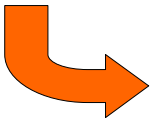
Conséquences

⇨ perte de temps, donc d'argent (sites en-ligne)
⇨ perte de réputation (chantage financier)
⇨ mise hors service des serveurs (DoS)
⇨ corruption possible du système / perte de données
⇨ vols de numéros de cartes bancaires : sans commentaire
⇨ vol d'informations personnelles : le site peut être poursuivi
⇨ publications d'infos intox : conséquences graves
⇨ et les centrales nucléaires … !

Evolution des types d'intrusion

1988 :

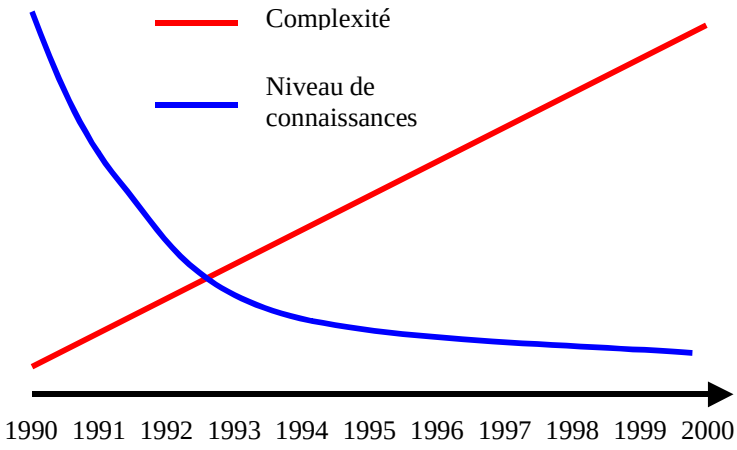
- attaques sur mots de passe
- exploitation manuelle de vulnérabilités



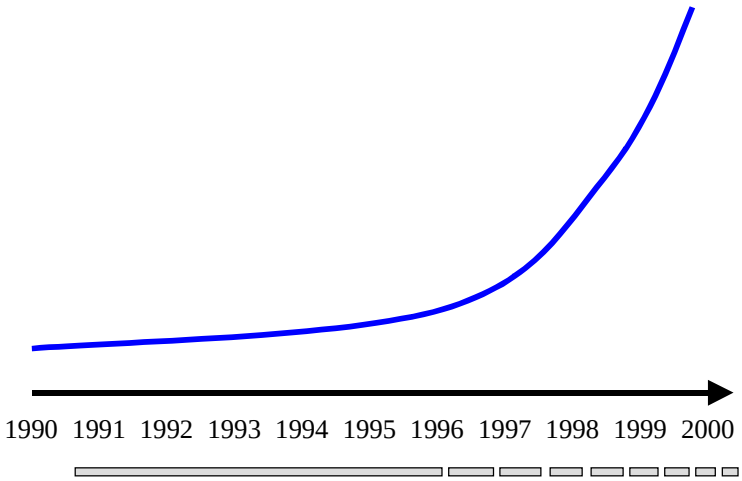
Aujourd'hui :

- attaques sur mots de passe
- exploitation de vulnérabilités sous forme automatique
- trous dans les protocoles
- examen des sources
- attaques http, ftp, mail
- installation de sniffers
- falsification d'adresse IP
- refus de service
- scanning à grande échelle
- attaques distribuées

Complexité des attaques / Niveau de connaissance requis

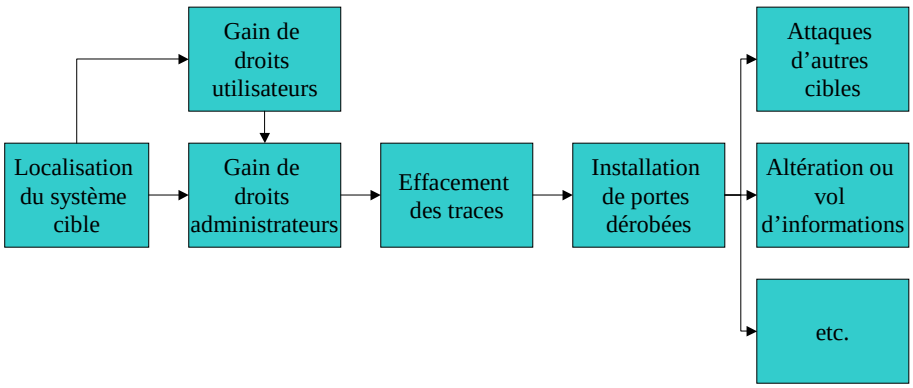


Quantité d'intrus potentiels



Page 11

Anatomie d'une attaque standard



Page 12

Que risque une machine non sécurisée ? (1/2)

- Expérience au SDSC de San Diego
- Une machine Linux RedHat 5.2 simple
- Un outil de visualisation du trafic Internet
- La machine est dédiée à l'expérience

Que risque une machine non sécurisée ? (2/2)

- 8 heures après installation
  - ⇨ sondée pour une vulnérabilité Solaris ss conséquence
- 21 jours après installation
  - ⇨ 20 tentatives d'intrusion sur POP, IMAP, RPC, telnet et mountd
  - ⇨ échec car les "exploits" étaient pour RedHat 6.x
- 40 jours après installation
  - ⇨ serveur POP compromis
  - ⇨ fichiers log "nettoyés"
  - ⇨ sniffer et rootkit installés

CEPENDANT

- Selon le CERT :

”Plus de **99%** des intrusions résultent de l’exploitation de vulnérabilités connues ou d’erreurs de configuration, contre lesquelles des mesures sont disponibles”

Tendances actuelles (1/3)

La communauté Internet évolue et doit faire face aux aspects suivants :

- le nombre d’intrus/pirates et d’intrusions augmente
- la sophistication des attaques et l’efficacité des outils augmente
- le nombre d’entreprises et d’utilisateurs reliés à l’internet augmente
- la complexité des protocoles et des applications client/serveur sur l’internet augmente

Tendances actuelles (2/3)

- la complexité de l'internet en tant que réseau augmente
- les infrastructures ont des problèmes conceptuels de sécurité qui ne peuvent être rapidement résolus
- la quantité de spécialistes en sécurité augmente mais à un taux inférieur à l'augmentation du nombre d'usagers
- le nombre d'outils de sécurité augmente mais moins vite que la complexité des logiciels, systèmes et réseaux

Tendances actuelles (3/3)

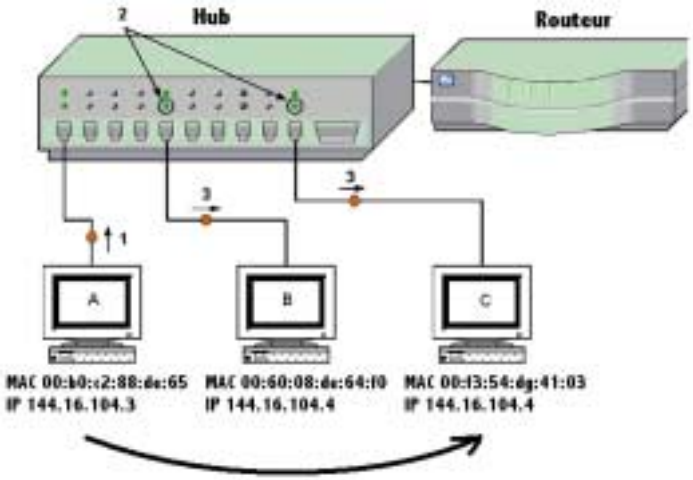
- le temps alloué au développement et aux tests des produits diminue
- les éditeurs continuent à produire des logiciels avec des vulnérabilités, incluant certaines pour lesquelles une prévention existe (ex. buffer overflow)

1.2. Attaques des équipements réseaux

Sniffers en environnement non commuté (1/3)

- Adresses MAC et adresses IP
  - ⇨ A IP 144.16.103.3 MAC 00:b0:c2:88:de:65
  - ⇨ C IP 144.16.103.2 MAC 00:60:8:de:64:f0
  - ⇨ L'envoi d'un paquet nécessite de connaître l'adresse MAC
- Le paquet parvient à tous les composants du réseau
- Les composants ignorent les paquets qui ne leurs sont pas destinés (adresse MAC différente)

Sniffers en environnement non commuté (2/3)



Sniffers en environnement non commuté (3/3)

- Une machine dotée d'un sniffer ne respecte pas cette règle
  - ⇨ Mode « promiscuous »
  - ⇨ Peut écouter TOUT le trafic du réseau, donc les mots de passe en clair (telnet, ftp, http, pop, imap, SNMP, SQL Server, etc.)
- Solutions
  - ⇨ Anti-sniffers détectant les interfaces en mode « promiscuous »
  - ⇨ Cryptographie
  - ⇨ Réseaux commutés, cependant ...

Routeurs

- Portes dérobées
  - ⇨ comptes par défaut pour les fabricants
  - ⇨ tous niveaux y compris administrateur
  - ⇨ présents sur tous types de routeurs
  - ⇨ mots de passe sur l'Internet !!!

ex :

Routeurs	*Login*	*Password*
3Com	admin	synnet
3Com	manager	manager
Cisco	enable	cisco
Bay Networks	Manager	<null>

1.3. Attaques des protocoles réseaux

Deny of Service (DoS)

- But : mettre hors service un système ou un réseau
- Utilise généralement l'IP spoofing pour cacher la vraie source = fausse adresse source
- Nombreux type de DoS :
  - ⇨ SYN Flooding
  - ⇨ UDP Flooding
  - ⇨ Ping of Death

◆SYN Flooding

⇨Anatomie d'une connection TCP = poignée de main

C ⇒ S SYN(Seq_C)
S ⇒ C ACK(Seq_C), SYN(Seq_S)
C ⇒ S ACK(Seq_S)
…échange de données...

Deny of Service (DoS)

- SYN Flooding (suite)

  ⇨ Nombreuses demandes de connection TCP
  ⇨ Mais la “poignée de main” n’est pas terminée
  ⇨ Stockage dans une pile en attente

  ⇨ Débordement de la pile = crash de la machine

  ⇨ Parade : filtrer les adresses IP source (par exemple par firewall)

Deny of Service (DoS)

- Ping of Death

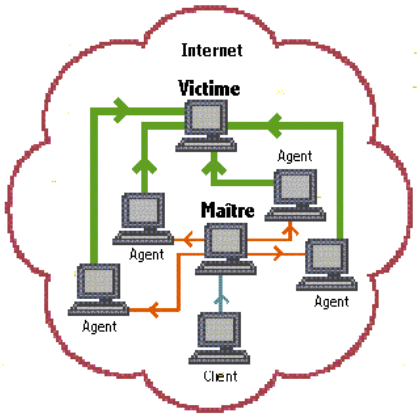
  ⇨ exploite un bug dans les implémentations du service ping
  ⇨ principe : envoi d’un ping plus gros que prévu (>64ko)
  ⇨ simple : crash de la machine réceptrice

  ⇨ assez vieille vulnérabilité = presque disparue

  ⇨ Parade : mise à jour du système d’exploitation

Distributed Deny of Service (DDoS)

- Beaucoup plus récent (2000)
  - ⇨ Nécessite plusieurs machines “infectées”
  - ⇨ Commandé par un “maître”, depuis un client
  - ⇨ Effet DoS démultiplié
  - ⇨ Plus dur à filtrer
  - ⇨ Solution ?? Pas de prévention individuelle



TCP Session Hijacking

- Détournement de session TCP
  - ⇨ Possible si l’attaquant B renifle tout le trafic entre A et C
  - ⇨ Après l’ouverture de la connexion
    - il suit l’évolution des numéros de séquence TCP
    - peut se substituer au client pour envoyer une commande exécutée sur C avec les droits de A
- Parade :
  - ⇨ d’abord supprimer la possibilité de sniffeurs
  - ⇨ préférer des communications cryptées (SSH)

1.4 Attaques des systèmes

- Une machine en libre service n'est pas en sécurité
  - ⇨ démontable
  - ⇨ attaquable par les lecteurs (disquette, CD-ROM)
    - ☞ accès fichiers / modifications mots de passe / etc.
  - ⇨ portes dérobées dans les BIOS
- Installations par défaut
  - ⇨ installent également les vulnérabilités par défaut
  - ⇨ installent trop de choses
  - ⇨ sont standard

standard = risque maximum

Erreurs d'administration

- Mots de passe
  - ⇨ trop simples
  - ⇨ jamais changés
  - ⇨ mal cachés / mal cryptés
- Il existe des programmes de recherche de mots de passe
  - ⇨ énumération par "force brute"
  - ⇨ énumération par dictionnaire
  - ⇨ vitesse actuelle Pentium 3-500 (dépend de l'algo de cryptage):
    - ☞ env 100.000 mots/s pour unix,
    - ☞ 1.200.000 mots/s pour NT

Erreurs d'administration

- Attaque par dictionnaire
  - ⇨ les mots les plus classiques
    - prénoms
    - noms communs
    - toto, titi, etc.
    - astu6eux, 2vinekoi, etc.
  - ⇨ combinaison standards
    - claude3, zoe6
    - zoezoe
- Par expérience :
  - ⇨ il suffit de trouver 1 seul mot de passe pour entrer dans le système !!

Erreurs d'administration

- Important
  - ⇨ changer régulièrement les mots de passe
  - ⇨ prendre des mots de passe d'au moins 8 lettres
  - ⇨ alphabet contenant au moins un symbole
  - ⇨ révéler le moins d'informations nominatives possibles (finger)

Erreurs d'administration

◆Mots de passe mal cachés

- ⇨ Windows 95, 98, Word, Excel, etc.
  - en mémoire
  - un clic et c'est tout
- ⇨ Windows NT et Unix
  - Unix : mots cryptés stockés dans un fichier en accès libre
  - NT et 2000 : des vieilles versions du fichier sont accessibles

◆Parade :

- ⇨ Windows 95/98 : aucune
- ⇨ Unix: cacher les fichiers de mots de passe
- ⇨ Windows NT et 2000 : supprimer les vieux fichiers

Outils de recherche de vulnérabilités (1/6)

- ◆ Audit local de machine
  - COPS (obsolete), Tiger, Check (perl) : Unix,
  - ISS (payant) : Tous OS
- ◆ Vérifient ou détectent :
  - permissions sur fichiers et répertoires
  - les permissions de certains fichiers, répertoires, devices
  - les mots de passe "pauvres"
  - l'installation correcte de FTP anonyme
  - certains trous de sécurité ("+" dans hosts.equiv, montages NFS, "." dans PATH de root)

Outils de recherche de vulnérabilités (2/6)

- Scanner réseau
  - Strobe, nmap : Unix
  - ISS (payant) : Tous OS
- Détectent à distance :
  - les ports ouverts
  - les services en route
  - l'efficacité du firewall

Outils de recherche de vulnérabilités (4/6)

- Scanner réseau : caractéristiques
  - utilisent parallèlement des ping, TCP SYN, TCP ACK, etc.
  - permettent parfois de passer les firewalls et de tester leur efficacité
  - détection du type de génération de séquence TCP
  - détection taille fenêtre TCP
  - réaction à la fragmentation des paquets
  - etc.
- en fonction des résultats, déduit l'OS de la machine !!

Outils de recherche de vulnérabilités (5/6)

- Testeur d'intrusion
  - Nessus, Cheops, SARA : Unix
  - Retina : Windows
  - en général reposent sur un scanner (Nessus ⇒ nmap)
- Vérifient ou détectent à distance
  - les comptes sync, guest, lp, ... (mot de passe ?)
  - les services en route et leur version
  - les vulnérabilités de ces services
  - les utilisateurs connectés
  - etc.
- Outil très dangereux entre certaines mains

Une fois le système compromis...

- En général, l'intrus

  ⇨ installe un sniffer
  ⇨ capture le fichier des mots de passe
  ⇨ modifie les logs

Rootkits

- Outil de pilotage de machine à distance
  - ⇨ accès **sans restriction**
  - ⇨ diffusé comme « aide aux administrateurs »
- Rootkits principaux :
  - ⇨ BackOrifice, pcAnywhere, CarbonCopy, CoSession (Windows)
  - ⇨ lrk (Linux Root Kit)
- Détection :
  - ⇨ certains anti-virus le font
  - ⇨ ~~checksum des programmes principaux~~

Java et Applets Java

- Langage de programmation complet
- Sécurité assurée par le « Security Manager »
  - ⇨ interdit à une applet de communiquer avec un autre site que celui d'origine
  - ⇨ interdit à l'applet de manipuler des fichiers locaux
  - ⇨ etc.
- Pourtant
  - ⇨ des problèmes d'implémentation
    - ☞ nuisances plutôt que dommages (applets « hostiles »)
      - ✓ saturation du disque dur, crash du navigateur, etc.
      - ✓ capture les chemins d'accès des plugins, etc.

ActiveX

- Uniquement pour Windows et Internet Explorer
- Sécurité ActiveX
  - ⇨ repose sur la cryptographie (signature électronique)
  - ⇨ vérifie seulement l'origine et laisse à l'utilisateur le choix de la confiance (!), selon le niveau de sécurité du navigateur
- Aucune limite de potentiel
  - ⇨ peut reformater le disque dur
  - ⇨ peut apporter des virus, etc.
  - ⇨ des pirates ont pu conduire une transaction bancaire frauduleuse sur un site de banque en-ligne

2 Firewall

Définition

- Firewall
  - ⇨ un firewall est un système protégeant les frontières d'un réseau vis à vis de l'internet
  - ⇨ un firewall peut être composé de plusieurs machines et intégrer plusieurs techniques ou logiciels

Firewall

Que peut faire un firewall ?

- Analyse du traffic
  - ⇨ analyse du traffic entrant et sortant
  - ⇨ s'il est autorisé, il est routé
  - ⇨ sinon, il est bloqué
- Relai de connexion
  - ⇨ depuis l'extérieur ou l'intérieur
  - ⇨ filtrage par informations du paquet
  - ⇨ bases de données locales
  - ⇨ applications "maison"

Firewall

Que peut faire un firewall ?

- Relai applicatif
  - ⇨ application gateway / proxy / serveur mandataire
  - ⇨ contrôles au niveau de la couche application (http get, post, ftp put, telnet rm, etc.)
- Dissimulation du réseau local
  - ⇨ topologie, adresses, OS, services, etc.
- Enregistrement des activités

Firewall

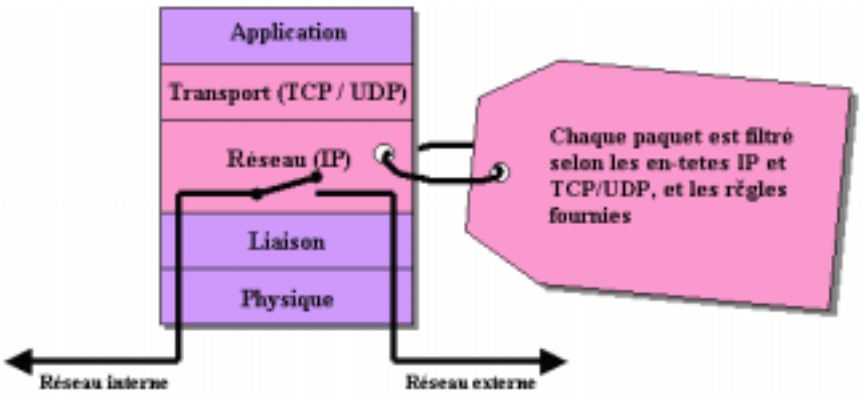
Que ne peut un firewall ?

- Un firewall est inutile si
  - ⇨ les politiques de sécurités ne sont pas claires
  - ⇨ les personnes ne suivent pas les règles de sécurité
    - attaques ou incidents depuis l'intérieur
    - accès internet par modem non sécurisé
    - insertion de virus par disquette
    - "social engineering"
- Détecter
  - ⇨ les chevaux de troie, les virus
  - ⇨ l'exploitation de vulnérabilités dans les applications

Firewall

Les relais de connexion (1/4)

- Le plus simple type



Firewall

Les relais de connexion (2/4)

- Règles de filtrage

IP source	IP dest	Port source	Port dest	Action
any	192.54.113.10	any	25	allow
93.54.84.35	any	any	23	allow
any	any	any	23	deny

⇨ actions possibles : deny / accept / reject

Firewall

Les relais de connexion (3/4)

- Problèmes

⇨ si l'accès est autorisé, il n'y a plus d'autre contrôle

☞ exploitation de vulnérabilités possible

⇨ sujet à l'IP spoofing

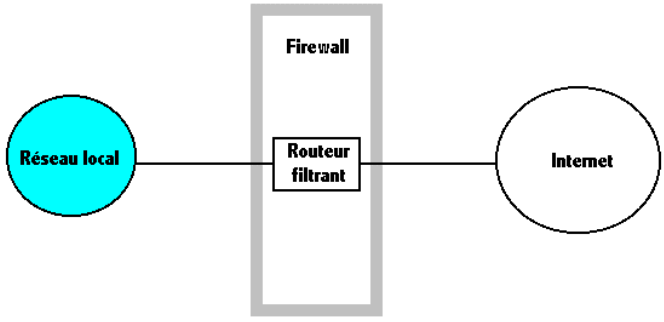
Firewall

Les relais de connexion (4/4)

- Pour résumer
  - ⇨ avantages
    - la performance n'est pas (trop) altérée
    - coût très bas / bien adapté aux problèmes de traffic
    - transparent aux utilisateurs
  - ⇨ inconvénients
    - pas adapté aux attaques
    - nécessite la présence de trous de sécurité
    - pas d'inspection du contenu
    - les règles peuvent devenir très compliquées à concevoir

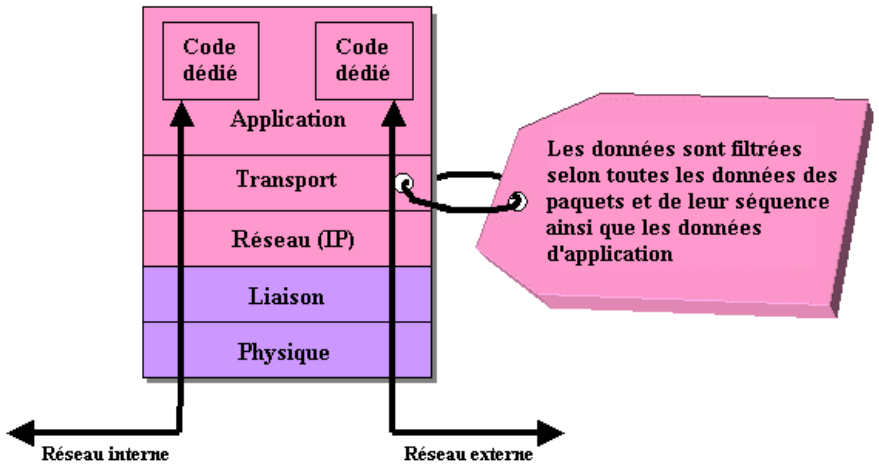
Routeur filtrant

•Est un relais de connection implanté dans un routeur



Firewall

Les relais applicatifs (1/4)



Firewall

Les relais applicatifs (2/4)

- Pas de connexion directe entre l'intérieur et l'extérieur
- Deux possibilités
  - ⇨ le relais applicatif est seulement un filtre au niveau des applications
  - ⇨ le relais applicatif est un délégué (proxy)
- le proxy est considéré comme
  - ⇨ un serveur pour le client
  - ⇨ un client pour le serveur

Firewall

Les relais applicatifs (3/4)

- Permet de cacher la topologie du réseau interne
- Utilisation de “l’IP masquerading” (PAT / NAT)
  - ⇨ les adresses du réseau interne ne sont pas routables sur l’Internet
  - ⇨ le proxy est
    - le seul possédant une adresse routable
    - le seul visible sur l’internet
  - ⇨ toutes les communications sont déléguées au proxy
  - ⇨ table de correspondance port/adresse IP réseau interne

Firewall

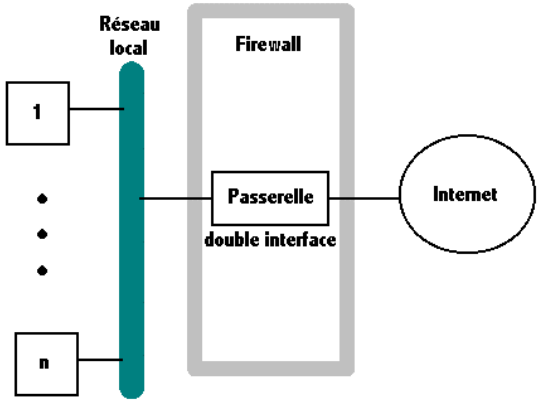
Les relais applicatifs (4/4)

- Pour résumer
  - ⇨ avantages
    - aucune connection directe intérieur / extérieur
    - analyse les données des paquets
    - cache la topologie du réseau interne
    - permet l’archivage (log) des activités et cache des accès
    - considéré comme le plus sûr type générique de firewall
  - ⇨ inconvénients
    - performance du réseau altérée
    - nécessite la configuration spécifique du réseau interne
    - nécessite de la maintenance (cas des applications nouvelles ou non prévues)

Firewall

Passerelle à double interface

- Est un relais applicatif implanté dans une machine



Passerelle à double interface (2/3)

- La machine
  - ⇨ possède deux adresses IP : interne et externe
  - ⇨ bloque le traffic par défaut, seuls les services “délégués” passent
  - ⇨ pour les utilisateurs :
    - ☞ soit les communications sont déléguées
    - ☞ soit un compte spécial est créé sur le firewall
  - ⇨ permet de cacher la topologie du réseau interne

Passerelle à double interface (3/3)

- La machine

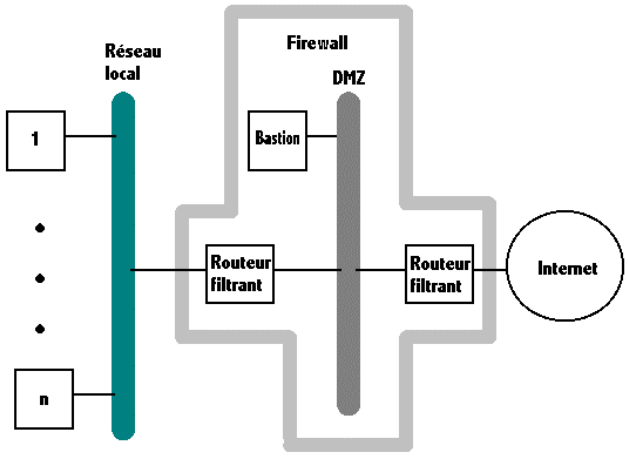
  ⇨ doit être **extrèmement sécurisée**

  - si le firewall est compromis, toutes les machines du réseau sont à portée de main

  ⇨ doit supporter la charge du réseau interne

  - difficulté de rajout d'une deuxième machine
  - d'autres architectures existent …

Sous-réseau filtrant (1/5)



Sous-réseau filtrant (2/5)

- DMZ = Zone Démilitarisée
  - ⇨ héberge le relais applicatif, les serveurs web, les accès modem, etc.
  - ⇨ isolée par deux routeurs
  - ⇨ performance adaptée au haut-débit

Sous-réseau filtrant (3/5)

- Les routeurs
  - ⇨ autorisent ou interdisent
    - ☞ le traffic DMZ / Internet
    - ☞ le traffic DMZ / réseau local
  - ⇨ les attaques doivent passer deux points
  - ⇨ communication directe possible entre l'extérieur et l'intérieur pour des protocoles particuliers, ou (mieux)
  - ⇨ placement des serveurs en question dans la DMZ

Sous-réseau filtrant (4/5)

- Avantages
  - ⇨ communication directe possible entre l'extérieur et l'intérieur pour des protocoles particuliers
  - ⇨ performances adaptées au haut-débit
  - ⇨ plus pratique que la passerelle à deux interfaces
  - ⇨ plus sécurisé que le bastion (2 points de sécurité)
- Inconvénients
  - ⇨ communication directe possible entre l'extérieur et l'intérieur pour des protocoles particuliers
  - ⇨ architecture de sécurité non centralisée (i.e. difficulté de configuration en particulier des routeurs) et chère

Sous-réseau filtrant (5/5)

- Solution populaire pour les réseaux à fort traffic
- Architecture en cascade
  - ⇨ plusieurs DMZ
  - ⇨ droits d'accès croissants
    - ☞ DMZ 1 : public
    - ☞ DMZ 2 : clients
    - ☞ DMZ 3 : fournisseurs
    - ☞ DMZ 4 : collaborateurs
    - ☞ réseau interne : utilisateurs

Variation sur les architectures

- Une architecture de firewall
  - ⇨ s'inspire de ces solutions génériques
  - ⇨ est adaptable
    - selon les découpages fonctionnels du réseau
    - selon les découpages de sécurité interne du réseau
  - ⇨ peut être complétée avec des outils divers (anti-virus, anti-spam, IDS, etc.)

Faiblesses des firewalls

- L'efficacité d'un firewall diminue si :
  - ⇨ celui-ci est mal configuré
    - architecture mal pensée
    - ACL trop laxistes
    - connections non authentifiées
  - ⇨ pas de surveillance
    - pas d'analyse des logs
    - pas de détection d'intrusion

Firewall

Faiblesses des firewalls

- L'efficacité d'un firewall diminue si :

⇨ celui-ci est mal configuré

- architecture mal pensée
- ACL trop laxistes
- connexions non authentifiées

⇨ pas de surveillance

- pas d'analyse des logs
- pas de détection d'intrusion

Systèmes de détection d'intrusions (IDS)

Généralités

- Pourquoi un IDS ?
  - ⇨ Dernière étape de la sécurisation d'un système
  - ⇨ Un système d'alarme
    - permet de prévenir en cas d'attaque en cours
    - permet de gauger la quantité d'attaques
- Qu'est-ce qu'une intrusion ?
  - ⇨ Qqu'un essaie de se loguer *root* 1 fois ? 50 fois ?
  - ⇨ Un scan de ports ?
  - ⇨ Exploitation d'un trou de sécurité connu ? Inconnu ?

Généralités

- Difficulté de définition d'une intrusion
  - ⇨ Problème des fausses alarmes
  - ⇨ Problème de la durée des intrusions
    - A partir de quand une action est-elle une intrusion ?
    - Quelle quantité de mémoire (au sens du temps) faut-il ?
    - Ex : un scan durant plusieurs heures, de manière irrégulière
- Que faire en cas d'intrusion ?
  - ⇨ E-mail, pager, message clignotant, menace ?
  - ⇨ Et si l'intrus s'attaque d'abord aux e-mails ?

Signatures d'intrusion

- Une intrusion
  - ⇨ est identifiée par un ensemble de symptômes (sa signature)
  - ⇨ la signature prend en compte :
    - la présence de fichiers (chevaux de Troie, etc.)
    - la violation de permissions
    - les processus illegaux
    - le traffic suspect (difficile si encrypté)
      - ✓ sniffers
      - ✓ scanners
    - etc.

Fonctionnement des IDS

- Deux types :
  - ⇨basé sur des règles
    - ex : tel port est accédé, telles données sont envoyées
    - ex : tel fichier est présent
    - nécessité d'une mise à jour constante des signatures
  - ⇨basé sur des statistiques
    - évaluation d'une activité "normale"
    - détection de tout changement "notable" dans les habitudes
    - basé sur
      - ✓ des modèles mathématiques
      - ✓ des réseaux neuronaux

Types d'IDS

- Network IDS
  - ⇨ s'intéresse au traffic réseau
  - ⇨ permet une réaction automatique = attention !
    - ex : shunning - reconfiguration des ACLs du routeur
  - ⇨ détection de code pour les attaques de type applicatif
- Faiblesse des Network IDS
  - ⇨ "Stick" déborde les capacités du shunning
  - ⇨ adresse du proxy d'un important ISP spoofée
    - blocage des clients légitimes du site

Types d'IDS

- Faiblesse des Network IDS
  - ⇨ traffic important
    - plusieurs IDS
    - réduction des analyses
  - ⇨ traffic crypté
  - ⇨ possibilité de polymorphisme du code des attaques applicatives

Types d'IDS

- Host IDS
  - ⇨ installé sur les serveurs critiques
  - ⇨ analyse des logs
  - ⇨ protège :
    - le système de fichiers
    - la table des processus
    - les E/S, les ressources systèmes
    - l'allocation de la mémoire

Types d'IDS

- Faiblesse des Host IDS
  - ⇨ nécessite des mises à jour constantes
  - ⇨ difficile à administrer sur toutes les machines
  - ⇨ doivent être très bien réglés
    - en fonction de l'utilisation de la machine
    - en fonction des utilisateurs
    - pour éviter les alertes à répétition