Sécurité : par où commencer ?

- Version 1.3 (juillet 1996)
  - A consulter en format paysage
  - Cliquer sur la flèche en haut à gauche pour accéder à la suite
  - Une ancienne version (1) a été présentée à JRES'95
  - Une version PostScript est disponible : ici
- Jean−Luc Archimbaud
  - CNRS/UREC
  - jla@urec.fr
- Cours d'une journée pour :
  - **Décrire les premières mesures à prendre pour protéger un site contre les attaques venant de l'Internet.**
  - **Ces mesures sont classées par ordre de priorité.**

Sécurité, par où commencer ? : plan

- Avertissement et orientations
  - Sites visés, ...
- Organisation
  - Responsable, CERT, chartes, ...
- Filtres dans les routeurs
  - Principes, exemples, ...
- Outils de diagnostique (audit)
  - ISS, Satan, COPS, CRACK
- Stations de travail
  - tcpd, inetd.conf, Sendmail, X11, ...
- Architecture du réseau
  - Machine services réseau, garde−barrière applicatif ...
- Annexes
  - Vérités, vocabulaire, besoins, mécanismes, où agir ?

Avertissement et orientations

- Les recommandations peuvent être suivies page à page
  - Elles sont fléchées "☞ "
  - Elles sont partiales (reflettent l'avis de l'auteur)
  - Elles se rapprochent d'un schèma directeur technique
- Site visé :
  - Environnement : Internet − IP − UNIX
  - Ouvert −−−> moins ouvert
  - Peu de moyens −−−> faire les bons choix
  - Laboratoire de recherche ou université ou campus
- Ce document n'est pas :
  - Un cours de sensibilisation
  - Une revue d'incidents
  - Une présentation de la sécurité sur l'Internet
  - Un guide d'administration Unix ou de réseau

Organisation

- Mener une réflexion globale −−−> Politique globale
- Responsable sécurité nommé par le Directeur du laboratoire
- Etre en contact avec un CERT
  Via le correspondant CNRS ou des Universités
- Pour les grands sites, mettre en place une organisation interne :
  correspondants, groupes de travail
- Vérifier le respect de la loi
  Logiciels utilisés, déclarations CNIL

Mener une réflexion globale −−−> Politique globale

Le risque (pour un ingénieur) en ne menant pas une réflexion globale est de miser sur des produits très intéressants conceptuellement et techniquement mais qui ne protégent pas contre les principales menaces.
Exemple : le chiffrement ne protége pas des attaques de crackers, le mot de passe en clair sur le réseau n'est pas le seul risque lié aux mots de passe, ...
Une bonne politique globale doit inclure la sensibilisation des utilisateurs, la protection physique du matériel, la bonne administration des ordinateurs, les sauvegardes régulières, les contrôles d'accès dans le réseau, ...

Organisation : charte de bon usage

- Statistiques CLUSIF : 3/4 des sinistres sont dus à la criminalité interne
- Responsabilité / Internet
- Pour sensibiliser et responsabiliser
- Signée par tous les utilisateurs des systèmes d'information
- Peut être intégrée dans un dossier de bienvenu
- Exemples
- ☞ Rédiger une charte, la faire signer et respecter

Organisation : charte de bon usage : contenu

- Respect des recommandations des administrateurs
- Bon usage des outils : ni rendre vulnérable, ni attaquer
- Usage uniquement professionnel
- Compte personnel non cessible
- Pas de consultation des informations des autres utilisateurs
- Respect des lois sur les logiciels (pas de copie illégale)
- Respect des lois sur sur la presse (droit d'auteurs, publications à caractère injurieux, pornographique, diffamatoire, d'incitation au racisme ...)
- Pas de page personnelle WWW sans autorisation du Directeur
- Sanctions applicables sur le site et rappel des lois

Organisation

- Lancer une première sensibilisation
  - Direction : responsabiliser
  - Utilisateurs : rappels réguliers, informations, exemples
  - Administrateurs : recommandations, diffusion avis des CERTs, ...
- Campagne pour des mots de passe solides, personnels et non écrits (articles de jla en ASCII, en Postscript, de jplg en ASCII)
- Campagne pour la protection des serveurs X (article de cg ici)
- Pour les stations définir de bonnes procédures pour :
  - L'ouverture et la fermeture des comptes
  - Les sauvegardes
  - (chaque station doit avoir un administrateur)
- Choisir de bons anti−virus pour les micros

Organisation : carnet d'adresses

- Serveur UREC et serveur CRU
- BCRCI (1) 40 97 87 72 (Bureau Central de la Répression de la Criminalité Informatique)
- DST (1) 40 57 55 34 (Direction de la Sureté Nationale)
- 3615 CNIL (Comission Nationale Informatique et Liberté)
- SCSSI (1) 41 46 37 20 (Service Central Sécurité des Sys d'Info)
- LITIEL (association pour acheter des logiciels shareware)

Filtres : plan

Filtres : principes des applications IP

- Mode Client − Serveur
  - La partie cliente envoie des requêtes à la partie serveur en attente
  - Derrière le client se trouve généralement un utilisateur (sauf X11)
  - Le serveur est un process en attente (daemon sous Unix)
- Serveurs Unix : inetd + sendmail + nfsd + ...
- TCP : mode connecté (ouverture et fermeture de session)
- UDP : mode non connecté (pas de session)
- Datagramme TCP ou UDP : numéros port source et port destination
- Ports clients : 1024, 1025, 1026, ... pour les applications
  - FTP, telnet, SMTP, NNTP, DNS, syslog, http, gopher, wais, archie
- Ports clients : 1023, 1022, 1021... pour les applications
  - rexec, rlogin, rsh, rcp, rdist, lpr

Filtres : ports serveurs : wellknown ports

RFC "ASSIGN NUMBERS" (RFC1700 ou plus récent) et /etc/services

ftp−data 20 (TCP)	ftp−commandes 21 (TCP)
telnet 23 (TCP)	smtp 25 (TCP)
whois 43 (TCP)	DNS 53 (UDP et TCP)
bootp 67 (UDP)	tftp 69 (UDP)
gopher 70 (TCP)	finger 79 (TCP)
http 80 (TCP)	pop2 109 (TCP)
poppass (Eudora) 106 (TCP)	pop3 (Eudora) 110 (TCP)
rpc portmap 111 (UDP et TCP)	nntp (News) 119 (TCP)
ntp (Time) 123 (UDP)	snmp 161 (UDP)
snmp trap 162 (UDP)	z3950 (wais) 210 (TCP)
rexec 512 (TCP)	rlogin 513 (TCP)
rsh (rcp, rdist) 514 (TCP)	printer (lpr) 515 (TCP)
syslog 514 (UDP)	rip 520 (UDP)
uucp 540 (TCP)	archie 1525 (UDP)
openwin 2000−20xx (TCP)	harvest 2138 (TCP)
nfs 2049 (UDP ou TCP)	X11 6000−6063 (TCP)

Filtres : Ack bit (established)

- Dans le datagramme TCP un "Ack bit" indique que le datagramme est aussi un accusé de réception d’un datagramme précédent
- Dans le premier datagramme d’ouverture de session TCP, ce bit n’est pas positionné
- En bloquant le premier datagramme toute session TCP est impossible
- Donc, en filtrant les datagrammes TCP entrants sans "Ack bit", on bloque les connexions TCP entrantes (tout en autorisant les connexions sortantes)
- N’existe pas dans UDP
- Langage routeur : "Ack bit" = "established"

Filtres : ports FTP et NTP

FTP : TCP

- Ports serveur : commandes 21 − données 20
- Port client > 1023
- Le canal données est ouvert par le serveur
  - Port serveur 20 et port client > 1023
  - Attention au TCP "Ack bit" (cf avant)
  - Avec la commande FTP "PASV", ce particularisme disparaît

NTP (Time) : UDP

- Serveur 123 <−−−−> Client > 1023
- Serveur 123 <−−−−> Serveur 123

Filtres : ports DNS

Interrogations et transferts de zone (primaire −−−> secondaires)

Interrogations :

- UDP généralement,
  - TCP pour IBM−AIX et quand beaucoup de données à transmettre
- Client > 1023 −−−−−> Serveur 53
- Serveur 53 −−−−−> Serveur 53

Transferts de zone :

- TCP : Primaire 53 <−−−− Secondaires > 1023
- Les secondaires font aussi des interrogations
  - (pour connaître le numéro de version des fichiers zones)

Filtres : ports RPC

- NIS, NFS, ...
- UDP courant mais aussi TCP
- Serveur portmap port 111
- Serveur RPC : choisit un port TCP/UDP quelconque et s'enregistre auprès du server portmap
- Client : interroge serveur portmap −−−> serveur RPC
- NFS serveur : port 2049
- Si utilisation interne des RPC, recommandation :
  - ☞ filtrer portmap (UDP et TCP 111)
  - ☞ filtrer UDP inconnu (pas DNS, syslog, Archie) car les RPC fonctionnent principalement au dessus de UDP

Filtres : ports SNMP, X11, OpenWindows

SNMP : UDP

- Agent attend sur le port 161
- Station reçoit des alarmes (traps) sur le port 162
- Client port > 1023

X11 et **OpenWindows** : TCP

- Serveur X11 : port 6000 pour 1er display, 6001 pour 2nd, ...
- Serveur OpenWindows : ports 2000, 2001, ...
- Remarque : les systèmes peuvent attribuer les ports 2000 ou 6000 aux clients d'autres applications (car port client > 1023)
- Recommandation compromis :
  - ☞ Filtrer TCP 6000−6003 et 2000−2003 (dans certains cas rares les utilisateurs auront à recommencer leurs essais de connexion)

Filtres : champs d’une trame Ethernet

Un routeur (connecté sur Ethernet) reçoit des trames qui contiennent :

En−tête Ethernet

- Adresses Ethernet d’origine et de destination
- Champ "type" : 0800 IP, 0806 ARP, ...

En−tête IP

- Protocole : 1 ICMP, 6 TCP, 17 UDP
- Adresses IP d’origine et de destination

En−tête TCP ou UDP

- Numéro de port source et numéro de port destination

Un routeur peut donc filtrer sur ces informations (mais il lui est impossible de retrouver des données : nom des utilisateurs ...)

Filtres : 2 politiques

- 2 politiques
  1. On filtre ce que l’on ne veut pas, on laisse passer le reste (tout ce qui n’est pas interdit est autorisé)
  2. On laisse passer certains trafics, on interdit tout le reste (tout ce qui n’est pas permis est interdit)
- 1 : Facile à mettre en place après une ouverture totale
  Connaissance de toutes les applications et de tous les trous
  Vulnérable aux "nouveaux" trous
- 2 : Ouverture progressive aux applications que l’on maîtrise
  Très délicat après une ouverture compléte : installation en une seule fois de tous les filtres (après étude des applis utilisées et tests)
  −−−> Mécontentements d’utilisateurs (erreurs, limitations)
- 2 bien plus efficace que 1 comme protection

Filtres : CISCO : access−list ACL

- ACL par interface (commande access−group)
- Dans le sens sortant (défaut) ou entrant (mot clé "in")
- Numéros : 1 à 99 simple (uniquement sur les @ source)
- Numéros : 100 à 199 ou plus "extented"
- Filtre : autorise ("permit") ou interdit ("deny")
- Exécutés en séquence. S'arrête quand une des conditions (permit ou deny) est remplie. En fin de ACL : le reste est interdit
- Filtre sur le protocole (ip, udp, tcp, icmp)
- Filtre sur le numéro de port destinataire (EQ GT LT NEQ)
- Filtre sur les adresses avec la notation :

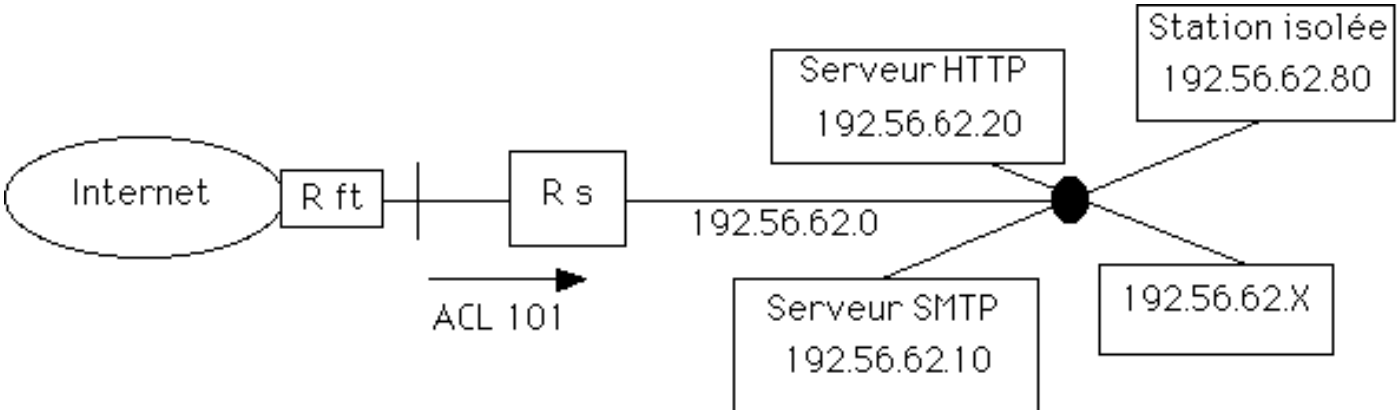
    @ source − masque @ source − @ destination − masque @ destination
    129.90.0.0 0.0.255.255 −−−−> 129.90.X.X
    129.90.5.3 0.0.0.0 −−−−> 129.90.5.3
    0.0.0.0 255.255.255.255 −−−−> X.X.X.X

Filtres politique 1: exemple recommandé

Exemples de filtres sur www.univ−rennes1.fr
Exemple politique 1 :

- Réseau interne 192.56.62.0 / 24 (classe C)
- On place des filtres sur le routeur d'entrée du site Rs
- Tout est autorisé sauf : tftp, NFS, SNMP, r−commandes, lpr, X11, OpenWindows
- 192.56.62.80 ne doit pas communiquer avec l'extérieur
- Le réseau 190.190.0.0 est interdit d'entrée
- Restreint SMTP serveur à 192.56.62.10
- Restreint HTTP serveur à 192.56.62.20
- Schéma : ici
- Filtre CISCO (Access List) : ici

Filtres politique 1: schéma



Filtres politique 1 : exemple recommandé

```
! Exemple de politique 1 : on filtre ce que l'on ne veut pas
! on laisse passer le reste
!
! Reseau interne 192.56.62.0 / 24 (classe C)
! Tout est autorise sauf :
! tftp, NFS, SNMP, r-commandes, lpr, X11, OpenWindows
! 192.56.62.80 ne doit pas communiquer avec l'exterieur
! Le reseau 190.190.0.0 est interdit d'entree
! Restreint SMTP serveur a 192.56.62.10
! Restreint HTTP serveur a 192.56.62.20
!
!  ATTENTION CECI PEUT CONTENIR DES ERREURS
!  NE PAS APPLIQUER SANS COMPRENDRE CHAQUE LIGNE
!
! Description de l'interface du routeur d'entree cote Internet
interface Ethernet0
ip address 193.5.5.1 255.255.255.0
ip access-group 101 in
!
! Interdit le source routing
no ip source-route
! Vide l'access list
no access-list 101
!
! N'accepte pas les datagrammes entrant avec le numero IP source
! etant un numero local ou 127.x.x.x (IP spoofing - mascarade)
access-list 101 deny ip 192.56.62.0 0.0.0.255 0.0.0.0 255.255.255.255
```

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 0.0.0.0 255.255.255.255
! N'accepte pas tout ce qui vient de 190.190.0.0
access-list 101 deny ip 190.190.0.0 0.0.255.255  192.56.62.0 0.0.0.255
! Interdit toute connexion IP avec la machine a isoler
access-list 101 deny ip 0.0.0.0 255.255.255.255 192.56.62.80 0.0.0.0
! Restreint SMTP (TCP 25) a 192.56.62.10
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.10 0.0.0.0 eq 25
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 25
! Restreint HTTP (TCP 80) a 192.56.62.20
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.20 0.0.0.0 eq 80
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 80
! Interdit tftp (UDP 69)
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 69
! Interdit portmap (UDP ou TCP 111)
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 111
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 111
! Interdit NFS (UDP 2049)
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2049
! interdit acces agents SNMP (UDP 161)
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 161
! Interdit les "r command" et lpr
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 512
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 513
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 514
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 515
! Interdit X11
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6000
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6001
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6002
access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6003
! Interdit Openwin
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2000
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2001
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2002
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2003
!
! Autorise tout le reste
access-list 101 permit ip 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255
```

Filtres politique 1 : AUSCERT

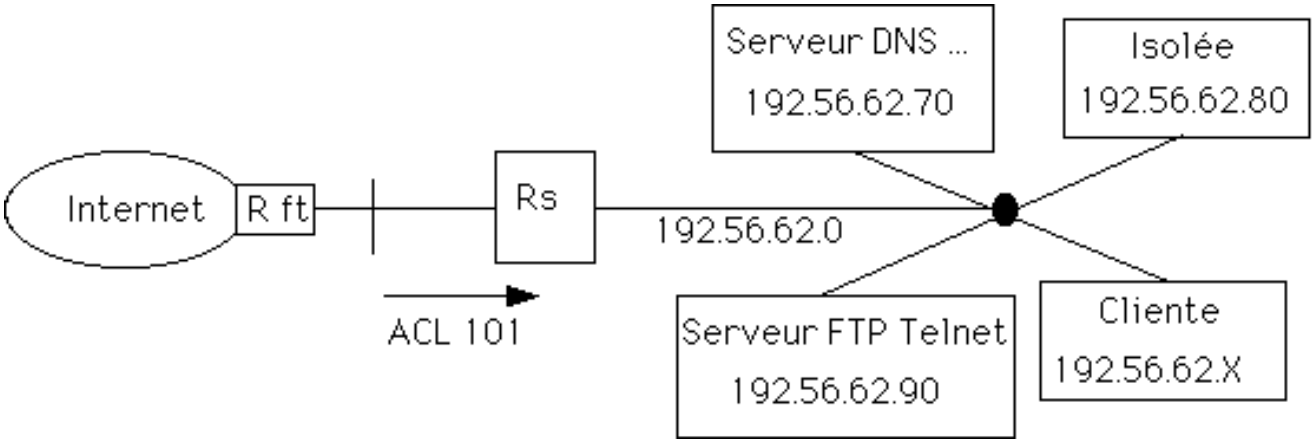
Le CERT australien AUSCERT recommande de filtrer :
(cf son avis)

```
systat 11 (TCP)       netstat 15 (TCP)   bootp 67 (UDP)
tftp 69 (UDP)         link 87 (TCP)      supdup 95 (TCP)
sunrpc 111 (TCP/UDP)  NeWs 144 (TCP)
snmp 161 (UDP)        xdmcp 177 (UDP)    exec 512 (TCP)
login 513 (TCP)       shell 514 (TCP)    printer 515 (TCP)
biff 512 (UDP)        who 513 (UDP)      syslog 514 (UDP)
uucp 540 (TCP         route 520 (UDP)    openwin 2000 (TCP)
NFS 2049 (UDP/TCP)    X11 6000−6020 (TCP)
```

Filtres politique 2 : exemple recommandé

- Réseau interne 192.56.62.0/24 (classe C)
- On place des filtres sur le routeur d'entrée du site Rs
- Tout est interdit sauf :
  - . 192.56.62.70 est serveur DNS, SMTP, WWW, NTP, FTP, telnet
  - . 192.56.62.80 ne doit pas communiquer avec l'extérieur
  - . 192.56.62.90 est serveur telnet et ftp uniquement
  - . Les autres stations peuvent être clientes uniquement
- Schéma : ici
- Filtre : ici

Filtres politique 2 : schéma



Filtres politique 2 : exemple recommandé

```
! Exemple de politique 2 : on laisse passer certains trafics
! on interdit tout le reste
!
! Reseau interne 192.56.62.0/24 (classe C)
! On place des filtres sur le routeur d'entree du site Rs
! Tout est interdit sauf :
! . 192.56.62.70 est serveur DNS, SMTP, WWW, NTP, FTP, telnet
! . 192.56.62.90 est serveur telnet et ftp uniquement
! . 192.56.62.80 ne doit pas communiquer avec l'exterieur
! . Les autres stations peuvent etre clientes uniquement
!
!  ATTENTION CECI PEUT CONTENIR DES ERREURS
!  NE PAS APPLIQUER SANS COMPRENDRE CHAQUE LIGNE
!
! Description de l'interface du routeur d'entree cote Internet
interface Ethernet0
ip address 193.5.5.1 255.255.255.0
ip access-group 101 in
!
! Interdit le source routing
no ip source-route
! Vide l'access list
no access-list 101
!
! N'accepte pas les datagrammes entrant avec l'adresse IP source
! avec un numero local ou 127.x.x.x (IP spoofing – mascarade)
```

```
access-list 101 deny ip 192.56.62.0 0.0.0.255 0.0.0.0 255.255.255.255
access-list 101 deny ip 127.0.0.0 0.255.255.255 0.0.0.0 255.255.255.255
! Interdit toute connexion IP  avec la machine a isoler
access-list 101 deny ip 0.0.0.0 255.255.255.255 192.56.62.80 0.0.0.0
! Autorise les communications avec la machine serveur 192.56.62.70 :
! DNS (UDP/TCP 53)
access-list 101 permit udp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 53
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 53
! SMTP (TCP 25)
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 25
! WWW (TCP 80)
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 80
! NTP (UDP 123)
access-list 101 permit udp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 123
! Telnet (TCP 23)
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 23
! FTP commande (TCP 21)
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 21
! FTP donnees (TCP 20)
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.70 0.0.0.0 eq 20
! Autorise les commucations telnet et ftp vers la station 192.56.62.90
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.90 0.0.0.0 eq 23
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.90 0.0.0.0 eq 21
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.90 0.0.0.0 eq 20
!
! Autorise toutes les machines a acceder a l'Internet en mode client
! TCP > 1023  pour telnet, ... et legerement < 1023 pour les r-commandes :  > 960
! Il faut UDP > 1023 mais interdit 2000-2003 (OpenWin), 2049 (NFS), 6000-6003 (X11)
access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 gt 960
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2000
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2001
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2002
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2003
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 2049
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6000
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6001
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6002
access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 6003
access-list 101 permit udp  0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 gt 1023
!
! TOUT LE RESTE EST INTERDIT
```

Filtres dans les routeurs

- Une forme de garde−barrière
- Mesure simple à mettre en place, économique mais qui techniquement demande une bonne connaisance des protocoles et de ses trafics
- Moins on laisse passer −−−> moins de trous possibles
- Installer éventuellement des filtres sur le backbone interne et des bâtiments
- Problèmes :
  - Incidence sur les performances : 2 Mbit/s à peu près nulle
  - Effets de bord possibles à chaque modification
  - Listes deviennent illisibles
  - Pas d'authentification des utilisateurs, pas de traces
  - Risques : client port 25 et serveur port 1025, rebonds, ...

Filtres : autres fonctionnalités

- Production automatique de filtres
- Produits type Firewall−1
- Différentes fonctionnalités selon routeurs :
  - Filtres dans le sens entrant et sortant
  - Filtres sur le port source
  - Facilité de configuration
  - Architecture interne prévue pour le filtrage
  - Alarmes et redirections quand déclanchement de filtres
  - Messages ICMP envoyés à l'émetteur
- ☞ Installer des filtres très similaires aux précédents exemples sur vos routeurs

Outils de diagnostique (audit) : plan

Les outils suivants sont disponibles ici

☞ Utiliser ces 4 outils :

- ISS
- SATAN
- COPS
- CRACK

Outils d'audit : ISS

- Internet Security Scanner
- Audit de sécurité d'un réseau de machines : à distance, essai des trous de sécurité connus des applications réseau
- ISS teste :
  - Les comptes sync, guest, lp, ... (mot de passe ?)
  - Le port 25 (quelle version de Sendmail ?)
  - Certains alias dangereux (uudecode, ...)
  - FTP anonymous (peut on créer un répertoire ?)
  - rexd (nombreux trous)
  - NIS (cherche le nom de domaine) ; NFS (répertoires exportés ?)
  - Les utilisateurs connectés
- Outil très dangereux dans certaines mains
- Fichier résultat : exemple

Outil d'audit : exemple ISS

```
Commande " iss 157.211.150.1 157.211.150.154" ---- Extrait du fichier resultat :
Scanning from 157.211.150.1 to 157.211.150.154
157.211.150.4 chose.truc.edu
SMTPchose.truc.edu Sendmail AIX 3.2/UCB 5.64/5.17 ready at Tue, 5 Oct 1995
250 <guest>
550 decode... User unknown: A system call received a parameter that is not valid
550 bbs... User unknown: A system call received a parameter that is not valid.
550 lp... User unknown: A system call received a parameter that is not valid.
550 uudecode User unknown:A system call received a parameter that is not valid.
FTP:220 chose FTP server (Version 4.1 Sat Nov 23 12:52:09 CST 1991) ready.
530 User anonymous unknown.
export list for 157.211.150.4:
/usr/local/tex   (everyone)
/usr/lib/X11/ncd (everyone)
/usr/local/X11R5 (everyone)
/tempo           meltemi,busar
/local_home      (everyone)
/home            (everyone)
toto  chose.truc:pts/1    Oct  5 07:13       2
titi   chose.truc:pts/2    Oct  4 15:03  9550:21
tata  chose.truc:pts/2    Oct  4 15:03  9550:21
157.211.150.9 machine.truc.edu
```

Outils d'audit : SATAN

- Mêmes objectifs et mêmes méthodes que ISS
- Interface client WWW
- Beaucoup de bruit mediatique : pas de catastrophe
- Aurait plus être beaucoup plus dangereux
- Cf articles, logiciel, ... : ici
- Passer régulièrement SATAN et ISS sur son réseau

Outil d’audit : COPS

- Computer Oracle and Password System
- Audit de sécurité d’une machine Unix
- Ensemble de programmes qui vérifient ou détectent :
  - Les permissions de certains fichiers, répertoires, devices
  - Les mots de passe "pauvres"
  - Le contenu des fichiers passwd et group
  - Les programmes lancés dans /etc/rc et par cron
  - Les fichiers SUID root
  - L’accès à certains fichiers utilisateurs (homedir, .profile, .cshrc, ...)
  - L’installation correcte de FTP anonyme
  - Certains trous de sécurité ("+" dans hosts.equiv, montages NFS, "." dans PATH de root)
  - . . .

Outil d’audit : COPS

- Peut sceller certains fichiers
- Création d’un fichier résultat ou envoi d’un message
- Peut être éxécuté sans être root
- Configurable : fichiers à sceller, objets dont l’accès est à vérifier, dictionnaires
- On peut : ajouter ses propres vérifications, le mettre dans le CRON
- Problèmes : messages succincts, pas de MAJ récente
- ☞ Faire passer COPS sur toute nouvelle machine installée et régulièrement sur les autres
- Fichier résultat : exemple

Outil d’audit : COPS : extrait d’un fichier résultat

```
Security Report for Thu Mar 10 17:13:18 WET 1995 from host xxxx
**** root.chk ****
Warning!  "." (or current directory) is in roots path!
**** is_able.chk ****
Warning!  /usr/spool/mail is _World_ writable!
Warning!  /etc/aliases.dir is _World_ writable!
Warning!  /etc/aliases.pag is _World_ writable!
Warning!  /etc/motd is _World_ writable!
**** rc.chk ****
**** cron.chk ****
**** home.chk ****
Warning!  User uucp’s home directory /var/spool/uucppublic is mode 03777!
**** passwd.chk ****
Warning!  Password file, line 10, no password:
        sync::1:1::/:/bin/sync
Warning!  Password file, line 11, user sysdiag has uid = 0 and is not root
        sysdiag:*:0:1:Old System
**** user.chk ****
**** misc.chk ****
Warning! /bin/uudecode creates setuid files!
**** ftp.chk ****
Warning!  /etc/ftpusers should exist!
```

Outil d’audit : crack

- Enorme erreur d’Unix :
  - /etc/passwd lisible par tous
  - Même algorithme de chiffrement sur toutes les machines
- Dans /etc/passwd : chiffrement non inversible
- Par combinaison (sans dictionnaire), la puissance actuelle des machines permet de découvrir des mots de passe jusqu’à 5 caractères
- Crack à partir de mots de dictionnaires :
  - Ajoute des mots venant d’informations dans /etc/passwd (nom, ...)
  - Crée de nouveaux mots (cle+, Cle, elc, ...)
  - Chiffre chaque mot et compare le résultat avec la chaîne dans /etc/passwd
  - Mémorise les mots de passe testés (pour les exécutions ultérieures)

Outil d'audit : crack

- Configurable :
  - Nouvelles règles pour générer les nouveaux mots
  - Ajout de dictionnaires
  - Peut travailler sur plusieurs fichiers passwd
  - Peut envoyer un message aux utilisateurs
- La première exécution est très longue
- Crack a beaucoup de succès sur les serveurs FTP anonymes
- Ajouter des dictionnaires francais, ...
  - Cf les dictionnaires
- ➪ Utiliser shadow password
- ➪ Passer régulièrement crack sur les machines le week−end et envoyer un message aux utilisateurs fautifs
- Fichier résultat : exemple

Outil d'audit : crack : extrait de résultat

```
Feb 21 13:32:47 Crack v4.1f: The Password Cracker,
(c) Alec D.E. Muffett, 1992
Feb 21 13:32:48 Loaded 17 password entries with 17 different salts: 100%
Feb 21 13:32:48 Loaded 240 rules from 'Scripts/dicts.rules'.
Feb 21 13:32:48 Starting pass 1 − password information

Feb 21 13:33:38 Guessed dupont (/bin/ksh in ./passwd) [dupont9] f5em4JkrApYAQ

Feb 21 13:34:36 Starting pass 2 − dictionary words
Feb 21 13:34:36 Applying rule '!?Al' to file 'Dicts/bigdict.Z'

Feb 21 21:18:39 Applying rule '28!?Al$9' to file 'Dicts/bigdict.Z'
Feb 21 21:24:37 Guessed durant (/bin/ksh in ./passwd) [tomate.] DQywOoXMwQFiI
```

Stations de travail : plan

Unix est vulnérable à cause de son succès et de l'attitude des vendeurs

- Chaque station doit avoir un administrateur
- Définir de bonnes procédures pour :
  - L'ouverture et la fermeture des comptes
  - Les sauvegardes
- Installer tcp−wrapper ou xinetd ou NETACL
- Ménage dans inetd.conf
- Ménage des autres daemons
- Sendmail
- X11
- Vérifications système
- Micros

Stations : tcp_wrapper (tcpd)

- Disponible : ici
- Fonction d'audit et de contrôle d'accès sur les serveurs
- S'intercale entre inetd et l'appel du serveur. Exemple dans inetd.conf :
  - tftp dgram udp wait root /usr/etc/tcpd in.tftpd −s /tftpboot
- Transparent : utilisateur, temps de réponse, ...
- Trace −−−> syslog (mail)
- Filtres : sites − services (écriture de script possible). Exemple
  - /etc/hosts.allow : "ALL: .urec.fr" et /etc/hosts.deny : "ALL:ALL"
- Limitations : uniquement inetd, pas efficace à 100 % pour les services UDP
- ☞ A installer sur toutes les stations avec la journalisation dans un fichier log non standard

Stations : ménage dans inetd.conf

- Une station peut être cliente sans être serveur
- Moins de serveurs −−−> moins de trous potentiels
  pour ne pas lancer un daemon dans inetd.conf : # en début de ligne
- Enlever tftpd si inutile
  ou vérifier qu'il est lancé avec un argument qui limite l'accès à un répertoire (−s)
- Enlever rexd (trop de trous)
- Oter les r−commandes si elles ne sont pas utilisées
- Oter fingerd s'il n'est pas utile
- ☞ Faire ces opérations à chaque installation de machine

Stations : ménage d'autres daemons

☞ Faire ces opérations à chaque installation de machine

- Oter /etc/hosts.equiv (sauf ... et attention "+")
- Supprimer rwhod dans un rc*
- Vérifier que "su" est obligatoire pour passer "root" (/etc/ttytab)
- Supprimer tout ce qui a un rapport avec UUCP
- Supprimer routed (sauf si vous utilisez RIP) dans un rc*
- Installer le routage minimum
- NFS serveur
  Si pas utilisé, oter nfsd dans rc.local, rpc.mountd dans inetd.conf
  Si en service, ☞ vérifier régulièrement /etc/exports

Stations : Sendmail

- Sendmail :
  - 30 000 lignes de code SUID root
  - Source public
- Nombreux outils d'attaque publics pour utiliser les trous de sécurité connus
- ☞ Utiliser une version sans trou de sécurité (connu) : 8.6.10 ou +
  - Disponible : ici
- ☞ Limiter sendmail à une ou deux stations identifiées et bien gérées

---

Stations − Terminaux : X11

- Si aucune protection tout le monde peut lire ce qu'un utilisateur tape sur le clavier de son serveur X ou ce qui est écrit sur son écran
- xhost nom de machine : contrôle d'accès par machine
  - Pas de "xhost +"
- .Xauthority : contrôle d'accès par utilisateur
- Article détaillé : ici
- ☞ Sensibiliser vos utilisateurs et vérifier qu'ils utilisent au moins xhost comme contrôle d'accès

Stations : vérifications système

- Faire ces vérifications à chaque installation de machine
- /etc/passwd : enlever les comptes guests ..., mettre des mots de passe
- Accès fichier aliases
- Enlever les alias uudecode et decode dans aliases
- PATH (pas de ".") et fichiers .* de root
- Ce qui touche au cron
- Choisir un bon umask pour les utilisateurs
- Ajouter quelques vérifications dans .login ou .profile de l'administrateur
  who, last du log de tcp_wrapper, ...
- Articles : ici

Stations : micros

- Pas le sujet du cours
- Installer de bons anti−virus
  dans une version récente (abonnement à une mise à jour)
  surtout pour DOS−Windows
- PC (McAfee, ...) : ici
- Mac (Disinfectant) : ici
- FAQ sur Virus : ici

Architecture : plan

- Une machine dédiée aux services réseau
- Plusieurs réseaux internes
- Garde−barrière applicatif
- Authentification des utilisateurs

Architecture : 1 machine services réseau

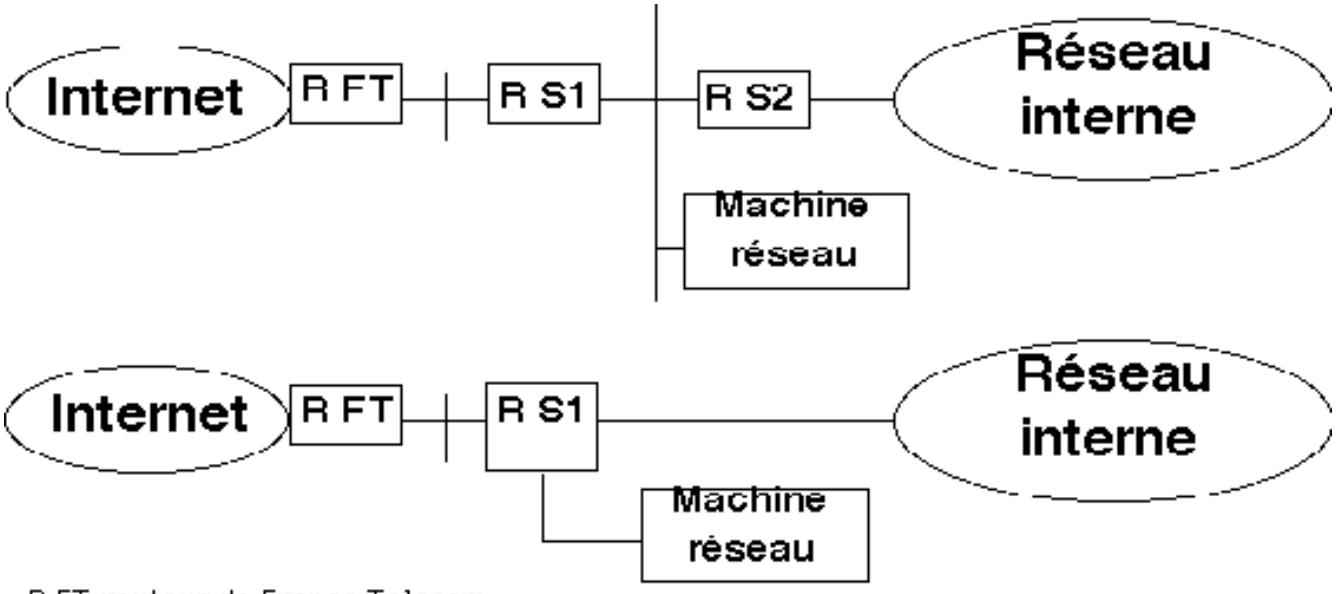
- Services réseau −−−> machine dédiée
  DNS, Sendmail, serveur FTP, HTTP, NTP, NNTP, POP
- Pas d'utilisateur enregistré sur cette machine
  Sauf les administrateurs
- Machine très visible et avec beaucoup de trous potentiels :
  Risques supérieurs
- Pas d'utilisateur :
  Mais dégâts minimes
  Facile de contrôler les accès interactifs
- Interdire les r−commandes et (avec tcp_wrapper) filtrer par machine appelante les accès telnet et FTP, ...

Architecture : 1 machine services réseau

- Ajouter une fonction proxy serveur (WWW ...) sur cette machine
  (Harvest ou ...)
- Mettre cette machine sur un réseau frontière : 2 solutions
- Ajuster les filtres dans les routeurs R S1 (et R S2) en conséquence
  Ils doivent devenir plus précis et plus restrictifs :
  SMTP, DNS, ... uniquement avec la machine de service
- Il devrait y avoir beaucoup moins de trafic entre le réseau local et l'Internet
- Des stations clientes ne devraient plus avoir besoin d'une route par defaut :
  restreindre le routage

Ensuite commencent les mesures plus coûteuses . . .

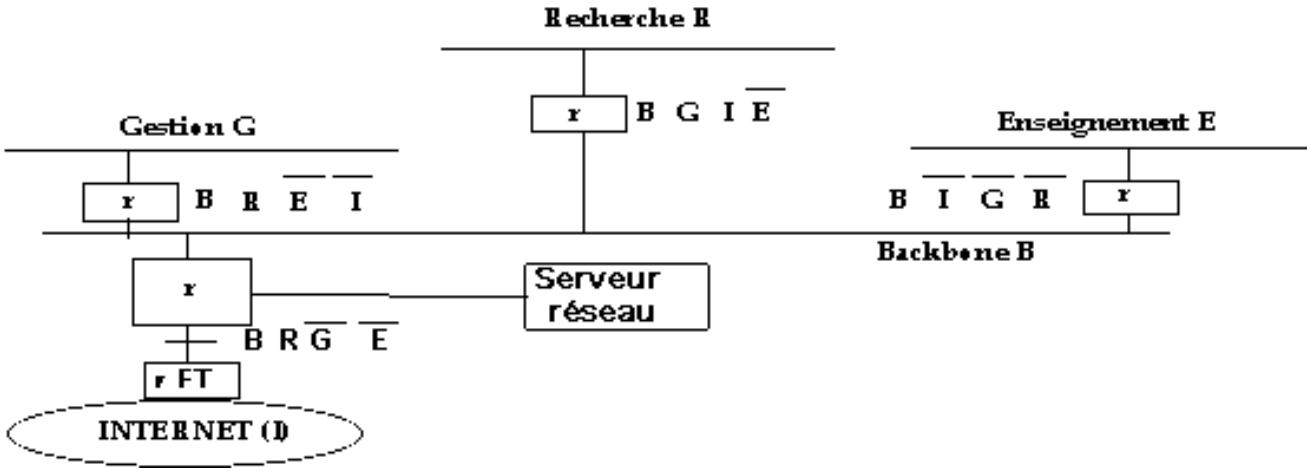
Architecture : schéma avec une machine services réseau



R FT routeur de France Telecom,
R S1 et R S2 routeurs de site

Architecture : schéma de plusieurs réseaux internes

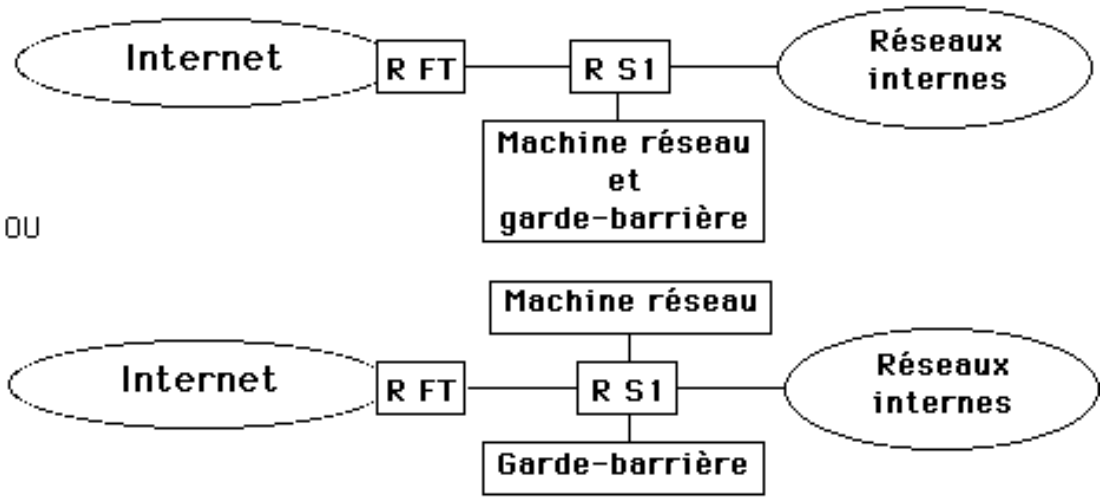
G, R, E, B sont 4 réseaux de classe C
Routage :
B et R seuls réseaux annoncés à Renater-Internet
G peut communiquer avec B, avec R mais pas avec E et I



Architecture : garde−barrière applicatif

- Passerelle applicative
  Double login : authentification des utilisateurs
- Applications en mode connecté. Relayées :
  telnet, rlogin, FTP, rcp, SMTP, HTTP, X11
- TIS très connu
  Documentation et logiciels : au CRU ou à l' UREC
- Avantages :
  Centralisation de la sécurité (blindage, traces, ...)
  Très bonne protection : jusqu'à l'authentification des utilisateurs
- Désavantages : lourd, coûteux, portes dérobées très dangereuses
- Schéma

Architecture : schéma avec un garde−barrière applicatif



Architecture : authentification forte

- Ajouter une authentification forte dans le garde−barrière applicatif :
  Calculette ou S/Key

Annexes : plan

- Vérités à prendre en compte
- Vocabulaire, besoins, mécanimes en sécurité réseau
- Où agir ? −−−> schéma récapitulatif

Annexes : vérités à prendre en compte

- On ne peut pas ignorer la sécurité
  - Si un ordinateur est utile il faut le protéger
  - Laisse−t−on sa voiture ouverte avec la clé de contact à l'intérieur ?
  - Il ne faut pas oublier l'image du laboratoire
- C'est toujours un compromis
  - Technique : il n'y a pas de zéro défaut
  - Financier : un campus n'est pas une centrale nucléaire
- La Direction doit jouer le rôle clef
- Ne rapporte rien mais coûte
- Demande du bon sens, des compétences en réseaux et du temps
- Un réseau ouvert peut convenir à une application sécurisée
- Les crackers sont rarement des experts : ils appliquent des recettes
- Ce n'est pas un but en soi − Recherche et Enseignement : réseau vital

Annexes : vocabulaire sécurité réseaux

- Confidentialité <−−− chiffrement
  - Message envoyé doit être compris uniquement par le destinataire
  - Besoin partiel sur certaines informations : mots de passe, courrier
- Intégrité <−−− scellement − signature
  - Le message reçu doit être identique au message envoyé
  - Les erreurs de transmission sont exclues du domaine de la sécurité
  - Ex de mécanisme : en fin de message, l'expéditeur ajoute un "CRC" : suite de bits fonction du message et d'une clé secréte
- Contrôle d'accès <−−− listes d'accès
  - Seuls les émetteurs autorisés doivent pouvoir envoyer des messages à l'objet (réseau, machine, application, ...)
  - ACL (Access Control List) : tableau 2 dimensions (Acteurs−Objets) : un élément du tableau indique le type d'accès autorisé

Annexes : vocabulaire sécurité réseaux

- Disponibilité <−−− contrôle d'accès
  - Matériels et logiciels doivent correctement fonctionner
  - −−−> ils doivent être protégés contre des attaques malveillantes
  - La disponibilité au sens classique d'un réseau n'entre pas dans le champs de la sécurité
- Traces <−−− journalisation (log)
  - Avoir des informations sur un problème en cours
  - Comprendre un incident passé pour évider la réédition
  - Problèmes : volume, dépouillement
- Alarmes quand événements anormaux <−− administrateur vigilant
  - Problème : qu'est ce qui est anormal ?
  - Ex : essais d'accès interdits, charge du réseau, modification d'un exécutable, présence anormale d'un utilisateur sur un système

Annexes : vocabulaire sécurité réseaux

- Audit <−−− outils d'audit
  Quel est le niveau de sécurité ? −−−> mesures à prendre
- Garde−barrière
  Antéserveur, écluse, gate−keeper, par−feu, coupe−feu, fire−wall, ...
  Poste frontière entre l'intérieur sans danger et l'extérieur dangereux
  Point de passage à rendu obligatoire
  Fonctions : contrôle d'accès, authentification, journalisation, ...
  Avantages : permet de ne pas sécuriser toutes les machines internes, administration centralisée de la sécurité
  Deux types : filtres dans un routeur et garde−barrière applicatif
  Principaux problèmes : demande du temps, difficile (techniquement et psychologiquement) à mettre en place après l'ouverture
  Documentation : ici

Annexes : vocabulaire authentification

Certificat d'identité : équivalent de la présentation de sa carte d'identité ou de son passeport

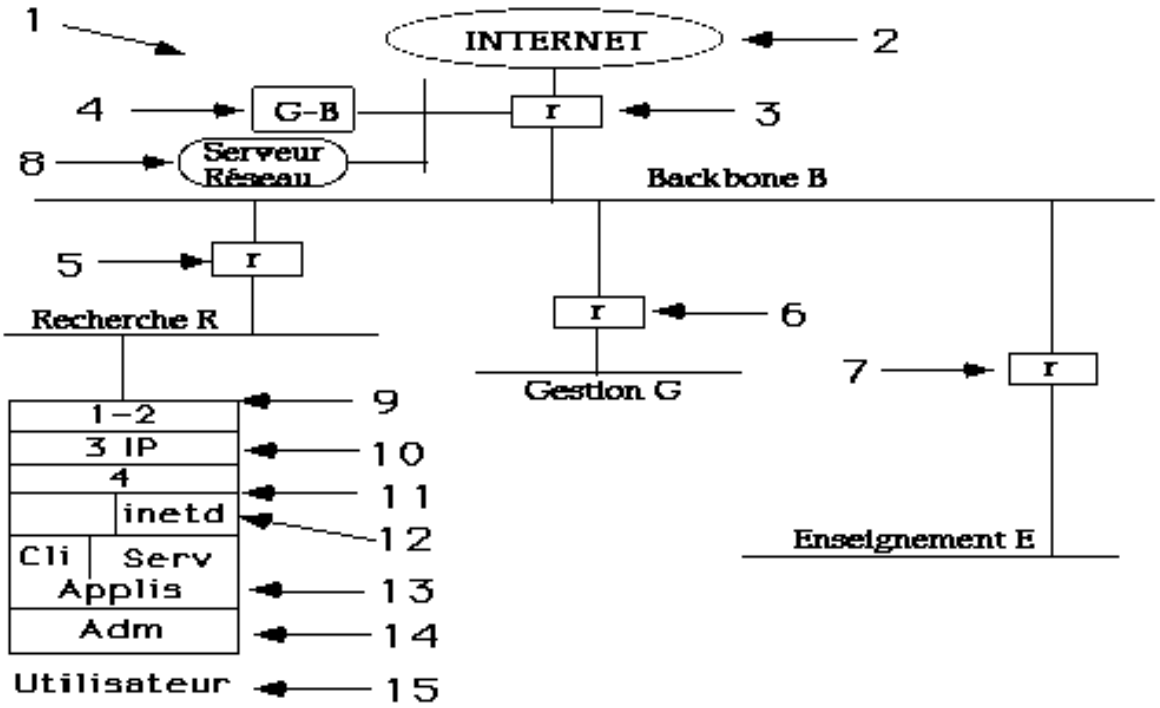
- Dans les 2 sens : appelant <−> appelé
  Si un utilisateur (appelant) doit s'authentifier, la machine (ou l'application ou ...) appelée doit aussi prouver son identité (il faut payer le magasin où on a effectué ses achats)
- Problèmes sur Internet : unicité de l'identité,
  choix de l'autorité qui délivrera les certificats d'identité
- Mécanismes d'authentification d'un utilisateur :
  . Mot de passe (pb confidentialité dans le transport)
  . Fonction : S/Key
  . Objet : authentifieur (calculette) ; carte à puce

Annexes : vocabulaire chiffrement

Transforme des données en clair en des données non intelligibles pour ceux qui n'ont pas à les connaître

- Fonction mathématique avec un paramètre : clé
- Inverse : déchiffrage ou déchiffrement
- Services assurés : confidentialité, intégrité, authentification
- Algorithmes symétriques (à clé secréte) comme DES
  Même clé pour le chiffrement et le déchiffrement
- Algorithmes asymétriques (à clé publique) comme RSA
  La clé de chiffrement (publique) est différente de la clé de déchiffrement (secréte)
- Problèmes : gestion des clés, législation, coût, à quelle couche OSI ?
- Documentation : ici

Où agir ? ----> 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15



Annexes : où peut on agir ? −−−> 1

Arriver à une architecture qui prend en compte la sécurité :

- En construisant plusieurs réseaux physiques (différents câbles) et logiques (différents numéros IP)
- En installant des routeurs avec des filtres, un serveur dédié réseau et éventuellement un garde−barrière applicatif

Cf le chapitre architecture de ce cours

Annexes : où peut on agir ? −−−> 2

Rendre inaccessibles depuis l'Internet (routage IP) certains réseaux internes :

Annoncer sur l'Internet (à Renater) uniquement les réseaux qui doivent communiquer avec l'extérieur

Et pas systématiquement l'ensemble des réseaux internes

Annexes : où peut on agir ? −−−> 3

Installer des filtres sur le routeur d’entrée de site
Cf le chapitre filtres de ce cours

Annexes : où peut on agir ? −−−> 4

Installer un garde−barrière applicatif à l’entrée du site
Cf le chapitre garde−barrière applicatif de ce cours

Annexes : où peut on agir ? −−−> 5 − 6 − 7

Interdire certains trafics venant des différents réseaux (gestion, ...), entre eux et avec l'Internet

- En ne mettant pas systèmatiquement une route par défaut
- En installant des filtres dans les routeurs

Cf le chapitre filtres et le chapitre plusieurs réseaux de ce cours

---

Annexes : où peut on agir ? −−−> 8

Installer une machine dédiée pour les services réseaux avec un bon Sendmail, DNS, FTPd, httpd, proxy WWW, . . .
Cf le chapitre 1 machine services réseau de ce cours

Annexes : où peut on agir ? −−−> 9

Si la machine est vraiment sensible, éventuellement :

La déconnecter du réseau physiquement ou
Logiquement en ne configurant pas le coupleur
(pas de commande "ifconfig")

Annexes : où peut on agir ? −−−> 10

Limiter le routage sur la station :

Pas de commande "route add default" lorsque ce n’est pas nécessaire

Annexes : où peut on agir ? −−−> 11

Installer un logiciel de trace et de filtrage tel que tcp_wrapper sur toutes les stations du réseau
Cf le chapitre tcp_wrapper de ce cours

Annexes : où peut on agir ? −−−> 12

Faire du ménage dans inetd.conf et dans le lancement des daemons réseau sur toutes les stations
Cf les chapitres inetd et daemons de ce cours

Annexes : où peut on agir ? −−−> 13

Utiliser des applications sécurisées telles que PGP (Pretty Good Privacy) pour le courrier électronique

---

Annexes : où peut on agir ? −−−> 14

Surveiller et contrôler la bonne configuration et la bonne utilisation des stations avec des outils tels que COPS, CRACK, ISS . . .
Cf le chapitre outils d'audit de ce cours

Annexes : où peut on agir ? −−−> 15

Sensibiliser, éduquer et contrôler les utilisateurs
Cf les chapitres charte et organisation de ce cours
