



HAL
open science

Cours sécurité réseaux (orienté Unix et TCP/IP)

Jean-Luc Archimbaud

► **To cite this version:**

Jean-Luc Archimbaud. Cours sécurité réseaux (orienté Unix et TCP/IP). Engineering school. Divers lieux en France, 1995, pp.68. cel-00560176

HAL Id: cel-00560176

<https://cel.hal.science/cel-00560176>

Submitted on 27 Jan 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SECURITE RESEAUX

Jean-Luc Archimbaud

CNRS/UREC

jla@urec.fr
<http://www.urec.fr/jla>

Octobre 95

Cours orienté Unix et IP

PLAN (1)

Exemples d'incidents

La sécurité dans notre monde
Généralités

Support "logistique"
Structures en France
Actions CNRS
CERTs
Chartes

Sécurité des réseaux
Concepts
Chiffrement
L'écoute sur Ethernet et le câblage

Caractéristiques de l'Internet, Renater, IP

Sécurité des applications réseaux Unix

PLAN (2)

Contrôle d'accès

- Avec les tables de routage dans les stations
- Avec les tables de routage dans les routeurs
- Avec des filtres sur un routeur
- Exemple de structuration de réseau

Outils

- crack
- cops
- iss et satan
- tcp_wrapper
- kerberos
- boite de chiffrement IP
- calculettes et S/Key
- gardes-barrières

Résumé : où peut on agir ?

Conseils pour la mise en place d'une politique de sécurité

Conseils pour les administrateurs de réseaux

Conseils pour les administrateurs de stations Unix en réseaux

Documentation on-line

EXEMPLES D'INCIDENTS

GET /ETC/PASSWD

CHOOSE GIRL

/BIN/LOGIN

MOT DE PASSE NVRAM (EEPROM)

TREMPIN POUR HACKERS

UNE ECOLE DE HACKERS

LA SECURITE DANS NOTRE MONDE : GENERALITES SUR LA SECURITE

Les communications sont vitales pour l'Enseignement
et la Recherche

---> la sécurité ne doit pas être un frein
systématique

---> ouvrir quand c'est nécessaire

On ne peut pas ignorer la sécurité

Image de marque de l'université ou du labo !

Ca ne rapporte rien mais ça coûte

C'est toujours un compromis

C'est d'abord une affaire de Direction

Elle doit être vue globalement

LA SECURITE DANS NOTRE MONDE : GENERALITES SUR LA SECURITE

La sensibilisation est indispensable

Direction (---> responsabiliser)

Utilisateurs

Administrateurs de machines et de réseau

---> La sécurité est l'affaire de tous

La sécurité c'est 80 % bon sens et 20 % technique

70 % des délits viennent de l'intérieur

Unix est surtout vulnérable à cause de
sa popularité

l'attitude des vendeurs qui livrent un système
ouvert

LA SECURITE DANS NOTRE MONDE : GENERALITES SUR LA SECURITE

En réseau : demande de la compétence et de la disponibilité

Les mécanismes de sécurité doivent être fiables
Ils doivent faire ce qu'ils sont sensés faire
--> validation des matériels et des logiciels

Le service doit répondre aux besoins
Ex : le chiffrement est inutile si on a besoin de contrôle d'accès

Il faut regarder le coût / efficacité
---> la confidentialité ou l'intégrité sélective

Facilité d'utilisation et d'apprentissage
Rejet ou contournement si trop contraignant
Ex : mots de passe, accès aux fichiers

Souplesse d'adaptation & portabilité
Evolution, matériel hétérogène
---> normes, standards

STRUCTURES

Haut fonctionnaire de défense ENSRIP : M. Pioche

Universités

Un correspondant / Université ou Ecole

Nombre d'établissements : 130

Coordination CRU

CNRS

Fonctionnaire de défense : M. Schreiber

RSSI : Michel Dreyfus

CM "Sécurité informatique (réseaux)" 1/2 temps

Correspondant / DR

Correspondant technique / "gros labo"

Accord tacite de réciprocité" CNRS et Ens Sup

STRUCTURES

RENATER

Charte RENATER

CERT-RENATER

Un correspondant sécurité par organisme
Isabelle Morel

FRANCE

BCRCI

CNIL

DST

SCSSI

ACTIONS CNRS

Aide en cas d'incident de sécurité

Diffusion électronique -> correspondants techniques
---> CERT-CNRS

Diffusion fax -> correspondants DR

Cours - sensibilisation

Bulletin d'information ---> Dir Labo

Cours sécurité Unix en réseaux

Journées de sensibilisation avec le SCSSI

Rubrique "Sécurité" dans le Microbulletin

<ftp.urec.fr>, <gopher.urec.fr>, www.urec.fr

Recommandations papiers

Tests de certains produits

Groupe sécurité SOSI

LES CERTS

Computer Emergency Response Teams

SERT UNE COMMUNAUTE

FIRST : regroupe les CERTs

Organise les moyens de défense et de réaction

Diffusion d'information

Recommandations

Corrections de trous de sécurité (informatique e
réseau)

Mise en relation des responsables sécurité

Petite cellule

Experts

Pression sur les constructeurs . . .

Ne remplacent pas la police

CHARTES

"de bon usage" ou "de sécurité"

Sensibilisation-responsabilisation des personnels

Par université ou laboratoire

Exemples : <ftp.urec.fr:pub/securite/Chartes>

Contenu

Utilisation des Systèmes d'Information

Qui est responsable de quoi

Ce qu'il ne faut pas faire

Recommandations (choix du mot de passe, ...)

Rappel des lois et des peines encourues

Signée par tous (même les utilisateurs de passage)

Peut-être courte

Pas de valeur juridique

CONFIDENTIALITE

Message compris uniquement par le destinataire
Mécanisme : chiffrement

INTEGRITE

Message reçu identique à celui émis
Mécanisme : scellement - signature

CONTROLE D'ACCES

Uniquement les émetteurs autorisés peuvent
envoyer des messages
Toutes les couches et étapes
Filtrage - ACL

NON RÉPUDIATION

Sur l'émetteur
Sur le destinataire
Mécanisme : notariation

AUTHENTIFICATION

Certificat d'identité

Couplée avec identification

Dans les 2 sens

Appelant (individu) ---> Appelé (application)

Appelé (application) ---> Appelant (individu)

Problème de l'unicité de l'identification

Problème de l'Autorité

Authentification d'un utilisateur : mécanismes

Ce qu'il sait - Ce qu'il est - Ce qu'il possède

Mot de passe

Pour accéder à quoi ?

Problème réseau : où est il stocké ?

Avec un matériel spécifique

Caractéristique physique de l'utilisateur

Objet que détient l'utilisateur

Carte à puce

Authentifieur - Calculette

Problèmes

Coût - Normalisation - Accès universel

Exemple sur un réseau : KERBEROS

DISPONIBILITE

Matériels et logiciels doivent fonctionner
Maillage des liaisons, duplication des équipements

TRACES

Journalisation

Etre au courant d'un problème, comprendre et éviter la réédition

Problème du dépouillement

Problème du volume de données

ALARMES

AUDIT

Quel est le niveau de sécurité de ma machine, de mon réseau, de mon site ?

**CONCEPTS SECURITE RESEAUX :
 SERVICES ET MECANISMES**

	M	E	C	A	N	I	S	M	E	S
	C	h	i	f	r	e	m	t	e	n
	S	i	f	i	g	n	a	a	r	t
	I	n	t	é	g	o	u	o	s	a
	S	o	l	n	n	B	o	r	i	s
	C	h	r	ô	l	a	r	u	a	t
	E	c	h	a	n	B	o	r	i	s
	C	h	r	ô	l	a	r	u	a	t
	O	n	t	é	h	e	e	e	n	n
SERVICES										
Auth d'homologues	s	s	•	•	O	•	•	•	s	s
Auth de l'origine	s	s	•	s	•	•	•	•	s	s
Contrôle d'accès	•	•	s	s	s	•	•	•	•	•
Confidentialité	O	•	•	•	•	•	•	s	•	•
Confi champs sélectif	O	•	•	•	•	•	•	•	•	•
Confi flux de données	O	•	•	•	•	s	s	•	•	•
Intégrité de connexion	s	•	•	O	•	•	•	•	•	•
Intégrité sans conn	s	s	•	O	•	•	•	•	•	•
Non-répudiation	•	s	•	s	•	•	•	•	•	s

O : Le service est fourni
 • : Le service n'est pas fourni
 s : Selon la config ou les autres mécanismes utilisés

Auth : Authentification
 Confi : Confidentialité

<p style="text-align: center;">CONCEPTS SECURITE RESEAUX : SERVICES ET COUCHES</p>
--

SERVICES

COUCHES

	1	2	3	4	5	6	7
Authentification	•	•	0	0	•	•	0
Contrôle d'accès	•	•	0	0	•	•	0
Confi mode connecté	0	0	0	0	•	0	0
Confi mode non-connecté	•	0	0	0	•	0	0
Confi champs sélectif	•	•	•	•	•	0	0
Confi du flux de données	0	•	0	•	•	•	0
Intég connecté avec reprise	••	•	•	0	•	•	0
Intég connecté sans reprise	••	•	0	0	•	•	0
Intég connecté champs sélec	•	•	•	•	•	•	0
Intég sans connexion	•	•	•	•	•	•	0
Non-répudiation	•	•	•	•	•	•	0

0 : Le service peut être fourni

• : Le service ne peut pas être fourni

Confi : Confidentialité

Intég : Intégrité

sélec : sélectif

Tous les services peuvent être fournis en couche 7

De nombreux services peuvent être rendus par les couches 3 et 4

SECURITE DES RESEAUX : CHIFFREMENT

Le chiffrement est le mécanisme le plus important

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

Algorithme mathématique avec un paramètre (clé)

Inverse : le déchiffrage (ou déchiffrement)

Peut être non-inversible

Services: authentification - intégrité - confidentialit

Algorithmes symétriques (à clé secrète)

le + connu : DES : Data Encryption Standard
clé de chiffrement = clé de déchiffrement

Algorithmes asymétriques (à clé publique)

le + connu : RSA : Rivest Shamir Adleman
clé de chiffrement \neq clé de déchiffrement

Problèmes

Gestion des clés

Législation

Coûteux : en temps CPU, ...

A quelle couche OSI ?

SECURITE DES RESEAUX : CHIFFREMENT

code secret (= clé) ---> chiffrement

1986 : décrets et arrêtés

Matériel de chiffrement classé

Obligation d'autorisation

Fabrication et de commerce (importateur)

Utilisation

Déc 90 : article 28 de la loi télécommunication

Autorisations : Services Premier Ministre

Authentification et intégrité

pas besoin d'autorisation d'utilisation

Procédures simplifiées pour certains

Législation américaine

Très stricte sur l'exportation

---> impossible d'exporter l'algorithme DES

---> L'utilisation des produits est réglementé

SECURITE DES RESEAUX : L'ECOUTE SUR ETHERNET ET LE CABLAGE

ETHERNET

Non buts du DIX (1980) : sécurité

Problème de la diffusion : confidentialité

Limiter la diffusion : ponts, routeurs

Charte

Attaque interne -> sensibilisation et
responsabilisation

Vérifier les accès (/dev, tcpdump, . . .)

r-commandes : le mot de passe ne circule pas

Avec "su" : difficile de récupérer le mot de passe

S/Key

SUPPORTS

Paire torsadée ou fibre optique

On ne peut pas s'y brancher en pirate

Des étoiles "sécurisées" existent (3COM,
SynOptics)

Internet

Beaucoup (trop ?) d'informations sont publiques
---> Toutes les @ IP et les noms sont publics

RFC1281 Guidelines for the Secure Operation of the Internet

Utilisateurs responsables de leurs actes

Utilisateurs doivent protéger leurs données

Prestataires de services responsables de la sécurité de leurs équipements

Vendeurs et développeurs doivent fournir des mécanismes de sécurité et corriger les bugs

Besoin de coopération

Besoin d'ajouts dans protocoles actuels et futurs

Les réseaux de l'Internet affichent des règles de bon usage

RENATER

Liste des réseaux autorisés à entrer à chaque point d'accès

CARACTERISTIQUES DE IP

Protocole réseau (niveau 3)

N'est pas un mode connecté

Pas de début de session où insérer des contrôles

Accès "bijectif"

---> Impossible d'interdire un sens et d'autoriser l'autre (au niveau IP)

Les numéros IP des machines sont fixés par logiciel

---> Mascarade possible

La résolution des noms est distribuée (DNS)

---> Aucune garantie : mascarade

Les réseaux IP supportent de très nombreuses applications

---> nombreuses portes possibles

@ IP = @ réseau + @ locale (machine)

Circulation des datagrammes IP : contrôlée par le routage

---> agir sur ce routage pour limiter les accès

CARACTERISTIQUES DE IP

Routage IP

= trouver l'itinéraire = laisser passer ou pas

basé sur le numéro de réseau

---> utilisation de différents numéros

Uniquement l'adresse destination est utilisée

Application : réciprocity de "non accès"

Principal outil de protection actuellement :
contrôles d'accès à différents niveaux

Où agir pour avoir des contrôles d'accès ?

Daemons sur la station Unix

Table de routage (accès IP) sur la station

Table de routage dans les routeurs

Filtres dans les routeurs

Principe des applications (services) réseaux

Client : souvent utilisateur

Serveur

Daemon en attente

Activation : /etc/inetd.conf ou /etc/rc*

Dialogue IP entre serveur et client

inetd

Daemon qui regroupe la partie serveur de très nombreuses applications réseaux

Configuration : /etc/inetd.conf

telnet

Serveur : telnetd (conf : /etc/inetd.conf)

Login ---> droits de l'utilisateur local

Coup d'œil : who (sans argument ou -R ou ?)

tftp

Transfert de fichiers sans contrôle d'accès

Serveur : inetd

Par défaut accès à tous les fichiers • • 4

Limiter l'accès à un directory (man tftpd)

Vérifier que l'on a une bonne version

ftp

Serveur ftpd configuré dans /etc/inetd.conf

Login ---> droits de l'utilisateur local

ftp anonymous

Cf man ftpd ou documentation papier

chroot sur ~ftp

Fichiers déposés : accès • • 4

~/.netrc

Permet un login automatique lors d'un ftp sur une machine distante

A n'utiliser que pour les ftp anonymous

Trace : ftpd -l ---> syslogd

Contrôle d'accès : /etc/ftpusers

Utiliser une version de ftpd récente (> Déc 88)

r-commandes

Permettent de s'affranchir de la phase d'identification et d'authentification manuelle

Les serveurs de r-commandes : daemon inetd

~/.rhosts

Equivalence : users distants - user local

Liste : nom_machine nom_d'utilisateur

/etc/hosts.equiv

Equivalence : tous les utilisateurs machine distante et tous les utilisateurs locaux

Format : Liste de noms de machines

L'équivalence est basée sur les noms

Utilisation des r-commands

Avantages (quand on en a besoin)

Evite aux utilisateurs la phase de login

N'impose pas aux utilisateurs la mémorisation de plusieurs mots de passe

Le mot de passe ne circule pas en clair sur le réseau

Désavantages

On fait confiance à une autre machine

Entrées possibles (via ~/.rhosts) que l'administrateur ne maîtrise pas

Conseils

S'ils ne sont pas utilisés ôter les "r-serveurs" dans inetd.conf

Vérifier régulièrement le contenu des fichiers .rhosts de vos utilisateurs et leurs accès

Attention à host.equiv

Ne pas lancer rexecd ou rexd (sauf besoin)

Sendmail - SMTP

Un administrateur de machine peut lire tous les courriers électroniques qui :

- Partent de sa machine

- Arrivent sur sa machine

- Transitent par sa machine

Ceci pour tous les types de messageries (Internet-SMTP, EARN, X400 . . .)

Daemon serveur : sendmail lancé dans rc*

Fichier de "configuration" sendmail.cf

L'origine du message n'est pas fiable

Trous de sécurité très connus

Remarques

- Les bugs de sécurité sont régulièrement corrigés

- Très pratique : on ne peut plus s'en passer
- Jusqu'à présent, son manque de confidentialité et d'authentification ne justifie pas son rejet

NFS (Network File System)

Permet un système de gestion de fichiers distribué sur plusieurs machines

Origine SUN

Basé sur les RPC (Remote Procedure Call)

Serveur :

 nfsd en n exemplaires lancé dans rc.local
 rpc.mountd dans inetd

Client :

 biod (n exemplaires) lancé dans rc.local

/etc/exports

 Liste des directories qui peuvent être exportées

 Options :

NFS (suite)

Exemple de fichier /etc/exports

Après modif de /etc/exports : exports -a

Accès root

Root sur A monte une arborescence sur B

Si -root dans exports alors UID sur B = 0

Sinon UID sur B= -2 ou 32767 ou 65534

Remarques - Conseils

Les droits d'accès sont basés sur les UID

Il faut une gestion centralisée des UID et GID

Ne lancer NFS serveur qu'après avoir correctement configuré /etc/exports avec les accès minimum

Vérifier régulièrement /etc/exports

Attention à root=

finger

Peut donner des informations sur les utilisateurs d'une station à tout l'Internet

Les informations proviennent de /etc/passwd, de /etc/wtmp, ~/.plan, ~/.project, . . .

Serveur : fingerd dans inetd

Ce peut être très utile mais aussi dangereux

Version de fingerd postérieure à dec 88 ?

rwho

Permet de connaître les utilisateurs connectés sur toutes les machines du réseau local

Serveur et client : rwhod lancé dans rc*

Broadcast de l'information

L'information ne traverse pas les routeurs

Conseil : ne pas le lancer

Similaires :

 rusers avec serveur rusersd (inetd)

 rup avec serveur rstatd (inetd)

 ruptime avec daemon rwhod

Quel est le risque de rwho ou finger ?

Un pirate peut faire :

 finger @nom_de_la_machine

Il obtient une liste d'utilisateurs

Il essaie chaque nom avec des mots de passe triviaux

/etc/ttytab - secure terminal
Avec SunOS

"secure" = login root direct possible
pas "secure" = login user suivi de su

Ne mettre "secure" que sur la console

Sur HP-UX : /etc/securetty

/usr/adm/inetd.sec pour HP/UX

Services locaux avec la liste des machines ou des réseaux qui peuvent y accéder

Exemple :

```
login allow 192.34.56.* 132.40.5.1
shell deny urec.imag.fr
tftp allow termserv1
```

Une station peut être client sans être serveur

Daemons "réseaux" sur la station Unix

- Ne lancer que ceux utilisés

 - Faire du ménage dans inetd.conf et rc*

- Limiter et contrôler la bonne d'utilisation

 - Config correcte de : hosts.equiv, .rhosts, exports ...

- Surveiller

 - sulog, syslog, inetd.log, .rhosts des utilisateurs, ...

Sendmail : installer version de Erci Allman

R-Commandes

- Interdire ou limiter au réseau local

NFS

- Limiter au réseau local si possible

X11

Installer tcp_wrapper

CONTROLE D'ACCES AVEC LES TABLES DE ROUTAGE DANS LES STATIONS

Station inaccessible au niveau IP : accès aux applications impossibles

Une table de routage dynamique stocke les informations d'accessibilité

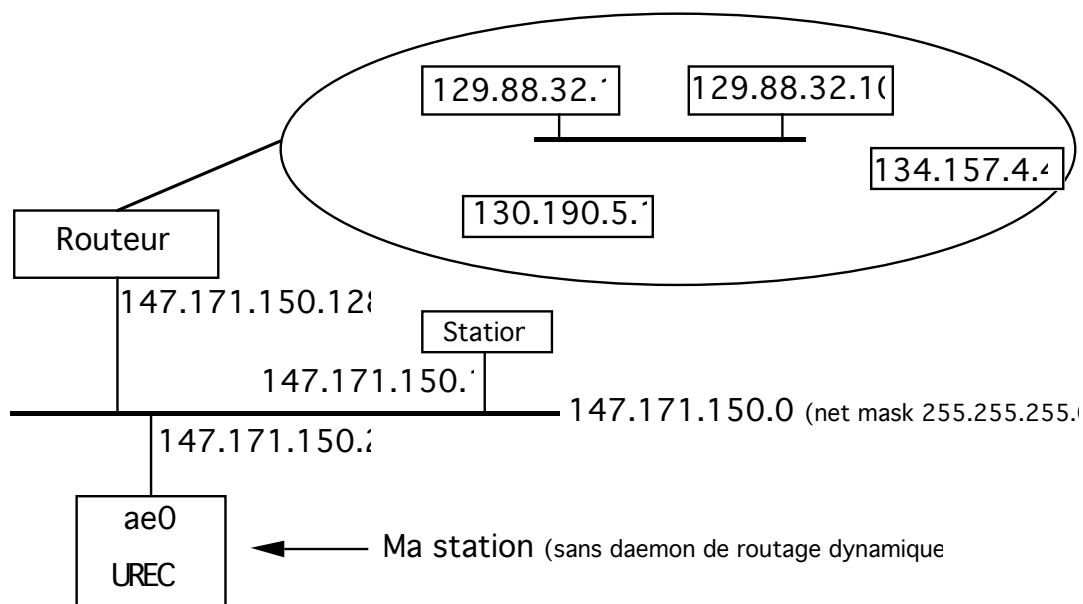
Cette table est mise à jour par

- La commande ifconfig (dans rc*)

- Les commandes route (dans rc*)

- Les daemons de routage dynamique (routed, gated ...)

Exemple de réseau



CONTROLE D'ACCES AVEC LES TABLES DE ROUTAGE DANS LES STATIONS

CONTROLE D'ACCES AVEC LES TABLES DE ROUTAGE DANS LES STATIONS

```
urec.jla # route add net 129.88.0.0 147.171.150.128 1
add net 129.88.0.0: gateway 147.171.150.128
urec.jla # netstat -rn
Routing tables
Destination      Gateway          Flags    Refs    Use  Interface
129.88           147.171.150.128 UG       0       28  ae0
127.0.0.1       127.0.0.1       UH       0       63  lo0
147.171.150     147.171.150.2   U        6      191  ae0
urec.jla # ping 129.88.32.10
PING 129.88.32.10: 56 data bytes
64 bytes from 129.88.32.10: icmp_seq=1. time=66. ms
64 bytes from 129.88.32.10: icmp_seq=2. time=33. ms
64 bytes from 129.88.32.10: icmp_seq=3. time=33. ms
----129.88.32.10 PING Statistics----
5 packets transmitted, 3 packets received, 40% packet loss
round-trip (ms)  min/avg/max = 33/44/66
urec.jla # ping 130.190.5.1
Network is unreachable
urec.jla # ping 134.157.4.4
Network is unreachable
```

< Uniquement les machines 147.171.150.X et les machines 129.88.X.Y peuvent m'atteindre >

```
urec.jla # route add default 147.171.150.128 1
add net default: gateway 147.171.150.128
urec.jla # netstat -rn
Routing tables
Destination      Gateway          Flags    Refs    Use  Interface
129.88           147.171.150.128 UG       0       78  ae0
127.0.0.1       127.0.0.1       UH       0       63  lo0
default         147.171.150.128 UG       0        0  ae0
147.171.150     147.171.150.2   U        4      353  ae0
urec.jla # ping 134.157.4.4
PING 134.157.4.4: 56 data bytes
64 bytes from 134.157.4.4: icmp_seq=0. time=533. ms
64 bytes from 134.157.4.4: icmp_seq=1. time=733. ms
----134.157.4.4 PING Statistics----
3 packets transmitted, 2 packets received, 33% packet loss
round-trip (ms)  min/avg/max = 533/633/733
urec.jla # ping 130.190.5.1
PING 130.190.5.1: 56 data bytes
64 bytes from 130.190.5.1: icmp_seq=0. time=16. ms
64 bytes from 130.190.5.1: icmp_seq=1. time=16. ms
----130.190.5.1 PING Statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 16/16/16
urec.jla #
```

< Toutes les machines du monde peuvent m'atteindre >

SECURITE IP : CONTROLE D'ACCES AVEC LES TABLES DE ROUTAGE DANS LES ROUTEURS

Idem station

Le routeur se base sur les numéros de réseaux

Bien répartir ses numéros de réseau

Bien maîtriser les algorithmes de routage dynamique

CONTROLE D'ACCES AVEC LES FILTRES DANS LES ROUTEURS

Concrètement : Access Lists

Forme de garde-barrière

Structure d'une trame Ethernet - telnet

1. Entête Ethernet

1.1 Adresse Ethernet du destinataire

1.2 Adresse Ethernet de l'origine

1.3 Type = 0800

2. Entête IP

• • •

2.1 Protocol = 6

2.2 Adresse IP de l'origine

2.3 Adresse IP du destinataire

• • •

3. Entête TCP

3.1 Source port

3.2 Destination port

• • •

4. Les données

CONTROLE D'ACCES AVEC LES FILTRES DANS LES ROUTEURS

Le routeur peut filtrer sur

- Les adresses Ethernet (champs 1.1 et 1.2)

- Le protocole de la couche 3 (1.3)

- Le protocole de la couche 4 (2.1)

- Les algorithmes de routage dynamique (1.3, 2.1)

- L'adresse IP d'origine (2.2)

- L'adresse IP destinataire (2.2)

- Un numéro de port (3.1 et 3.2)

Degrés de liberté

- Offset, masques avec des valeurs hexa

- Autoriser - interdire

- Plusieurs listes d'accès

- Listes d'accès par interface

Problèmes

- Connaissance des protocoles : obligatoire

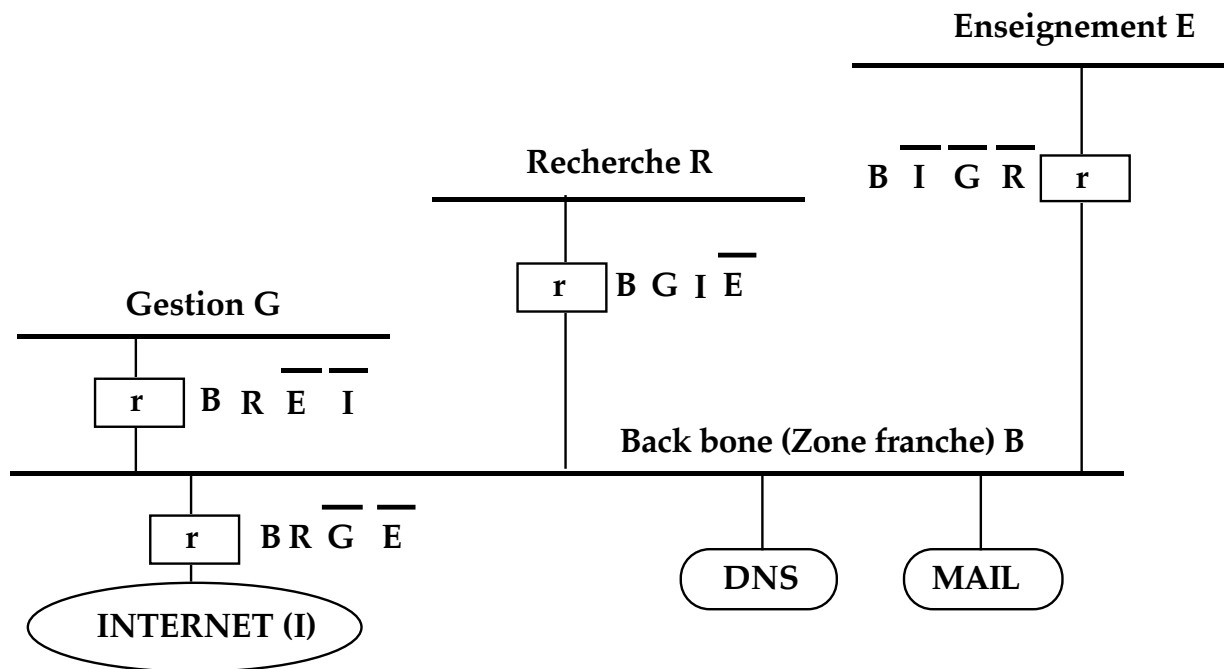
- Chaque modification : conséquences inattendues ?

- Les listes deviennent rapidement illisibles

- Les performances du routeur sont affectées

- L'accès au routeur doit être protégée

EXEMPLE DE STRUCTURATION DE RESEAU DE CAMPUS



Chaque réseau B, G, R, E a un numéro IP propre

Le réseau backbone (B) contient les services "ouverts" tels que le DNS, la messagerie, FTP anonyme, ...

Le réseau gestion G n'est accessible que par le réseau backbone (B) et le réseau recherche (R). Le réseau enseignement (E) et l'extérieur (Internet I) ne peuvent pas y accéder.

L'extérieur (Internet I) ne peut accéder qu'au réseau backbone et au réseau recherche (et réciproquement)

Etapes suivantes :

Filtrage par applications dans les routeurs
Garde-barrière applicatif à différents noeuds

OUTIL DU DOMAINE PUBLIC : CRACK

Remarques sur ces 5 outils du domaine public
D'autres existent peut-être meilleurs
Ils peuvent contenir des chevaux de Troie

Enorme erreur d'Unix : /etc/passwd lisible par tous

Beaucoup de fichier passwd circulent sur l'Internet

Par combinaison (sans dictionnaire), on peut
découvrir des mots de passe jusqu'à 5 caractères

Solutions

- Avoir un bon mot de passe

- Changer de mot de passe régulièrement

- Machine sensible = utilisateurs fiables uniquement

- Shadow password

- Commande passwd qui n'accepte que de bons mots de passe

- Faire passer crack régulièrement

Crack : A Sensible Password Checker for Unix

Version 4.1

Découvrir les mots de passe par essais successifs

Un mot en clair est chiffré puis comparé avec la chaîne que l'on trouve dans /etc/passwd

Utilise

- Les informations dans /etc/passwd

- Des dictionnaires (listes de mots)

OUTIL DU DOMAINE PUBLIC : CRACK

Crée de nouveaux mots avec les dictionnaires

Langage pour générer ces mots : règles

Configurable

- Ajout de dictionnaires

- Ajout ou modification de règles

Fonctionnalités

- Travaille sur un ou plusieurs fichiers passwd

- Exécution partagée entre plusieurs serveurs

- Envoi automatique d'un message aux utilisateurs

- Plusieurs passes

- Mémorise les mots de passe traités

La première exécution est longue

Arme défensive ou offensive ?

Faut il le mettre sur ftp anonymous ?

OUTIL DU DOMAINE PUBLIC : CRACK

OUTIL DU DOMAINE PUBLIC : COPS

Computer Oracle and Password System

Audit sécurité d'un système Unix

Actuellement version 1.04

Un ensemble de programmes qui vérifient/défectent

- Les permissions de certains fichiers, répertoires et "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

- Les modifications de certains fichiers

- L'accès de certains fichiers utilisateurs

- L'installation correcte du ftp anonymous

- Certains trous de sécurité très connus

- Diverses choses

- Les dates de certains fichiers avec les avis CERT

- □ • □ •

Création d'un fichier résultat ou envoi de message

OUTIL DU DOMAINE PUBLIC : COPS

N'a pas besoin d'être exécuté sous root

Configurable

crc_list : fichiers à sceller

is_able.lst : objets dont l'accès est à vérifier

pass.words : dictionnaire

CARP (COPS Analysis and Report Program)

Ce que ne fait pas COPS

Corriger les erreurs

En tirer partie

Se substituer à la vigilance des administrateurs

On peut (il faudrait) :

Ajouter ses propres vérifications

Le mettre dans CRON

Le faire passer sur chaque nouveau système installé

Les hackers connaissent COPS

OUTIL DU DOMAINE PUBLIC : COPS

OUTIL DU DOMAINE PUBLIC : ISS ET SATAN

ISS : INTERNET SECURITY SCANNER

Audit de sécurité d'un réseau de machines

Essaie les trous de sécurité connus

Trous exploitables via le réseau

Outil très dangereux dans les mains de hackers

Essaie

Les comptes sync, guest, lp , ...

Le port sendmail (version ?)

Certains alias (uudecode ...)

FTP anonymous (et essaie de créer un répertoire)

NIS (cherche le domaine)

rexid

NFS (regarde les répertoires exportés)

Les utilisateurs connectés

SATAN

Mêmes objectifs et même méthode que ISS

Interface client http

---> passer régulièrement SATAN sur son réseau

OUTIL DU DOMAINE PUBLIC : ISS

OUTIL DU DOMAINE PUBLIC : TCP_WRAPPER

Trace et filtre les accès TCP/IP entrant

Services lancés par inetd

tcpd s'intercale entre inetd et l'appel du serveur
Ne modifie pas le système où il est installé
Ne détériore pas les temps de réponse
Aucun dialogue avec les clients

Trace (avec le daemon syslogd)
Enregistre nom site appelant - service appelé

Filtres : sites-Services
Programme (try) pour tester les filtres
Exécution de script possible

Vérification des noms

Limitations
Uniquement inetd
Pas NIS, NFS et X

Actuellement version 6.1

OUTIL DU DOMAINE PUBLIC : KERBEROS

Le Cerbère

Système d'authentification centralisé sur un réseau non sécurisé

Origine MIT - Projet Athena (1ère version 86)

Utilisé au MIT et dans certaines universités US

Permet

- à des systèmes de prouver leur identité (ticket)
- d'éviter les attaches par rejeu
- de garantir l'intégrité
- de préserver la confidentialité

Tous les mots de passe sont
stocker sur un serveur
ne circulent pas en clair sur le réseau

Utilise un système de chiffrement DES

Sur le réseau

- Des stations d'utilisateur
- Des serveurs (calcul, impression, ..)
- Un serveur Kerberos qui
 - contient le fichier des mots de passe
 - partage un secret avec chaque serveur

Avec son mot de passe un utilisateur obtient un certificat d'identité

Quand il veut accéder à un service, il demande un autre ticket en présentant son certificat d'identité

OUTIL DU DOMAINE PUBLIC : KERBEROS

Principales applications kerberisées :

telnet, rlogin, ftp, nfs, dns

2 versions : 4 et 5 incompatibles

DES ne peut pas être exporté en Europe --->

Version Bones

Exportation sous certaines conditions

Versions peut-être utilisables

DEC - Athena (V4)

OSF-DCE (V5)

Avantages de Kerberos

Ca existe

C'est utilisé aux USA

Ca fait ce que ça dit

Désavantages

Problèmes d'exportation

Versions différentes mal supportées

Centralisation des mots de passe

Une (plutôt deux) stations immobilisées

Kerbérisation des applications

Utilisation d'algorithme symétrique

Toujours basé sur les mots de passe

Version US : athena-dist.mit.edu:pub/kerberos

Version Europe (Bones) :

ftp.funet.fi:pub/unix/security/kerberos

OUTIL COMMERCIAL : BOITE DE CHIFFREMENT IP

DCC : Origine EDF/DER

Dispositif de Chiffrement de Communication sur un réseau IP

Répéteur Ethernet-Ethernet intelligent

Ne chiffre pas ICMP et ARP

Ne modifie pas la longueur des trames

Utilise un chiffrement DES en mode chaîné

Clé de chiffrement / adresse ou / groupe d'adresses

Peut chiffrer ou pas

Performances : 5 Mbps

Prix : 30-50 KF

AUTHENTIFIEUR : CALCULETTES OU S/KEY

Pour l'authentification des utilisateurs

Pas de mot de passe en clair sur le réseau

Indépendant du réseau

Envoi d'un aléa par le système

Calcullette

De la taille d'une carte de crédit

De 300 à 500 F par utilisateur

Pas de norme

S/Key

Fonction sur Unix, PC et Mac

RFC1760

---> utilisation pour les "gros" centres de calcul
ou lorsque l'authentification est centralisée (garde-
barrière applicatif)

OUTIL : GARDE-BARRIERE

Antéserveur, écluse, gate-keeper, par-feu, coupe-feu, fire-wall

Point de passage obligé - Etablit une frontière

Fonctions possibles en sécurité

- Filtrage

- Authentification (fichier des mots de passe)

- Contrôle d'accès (fichier des droits)

- Journalisation

Fonctions annexes

- La facturation

- Le chiffrement

- Convivialité : menu d'accueil

- ...

Avantages

- Permet de ne pas modifier les systèmes internes

- Administration centralisée

Problèmes

- Les utilisateurs ne peuvent pas utiliser toutes les applications : difficile à faire accepter après l'ouverture

- Performances

- Station - équipements dédiées

- Service doit être fiable

- Si le pirate est introduit . . .

GARDE-BARRIERE FILTRES

Cf filtres dans routeurs

Transparent pour l'utilisateur

Intéressant d'avoir d'autres fonctions que le filtrage

- Langage de configuration simple

- Lui-même protégé et sécurisé,

- De journaliser les rejets

- D'envoyer des alarmes

- De détourner les datagrammes

- De convertir les adresses IP (NAT)

Recommandation (pour site important) : utiliser un routeur dédié à cette fonction

Produits :

- Routeurs classiques

- Routeur Network Systems (complet pour filtrage
FireWall-1

- . . .

Architecture : sur le routeur d'entrée ou sur le routeur d'accès au réseau gestion, ...

GARDE-BARRIERE APPLICATIF

Station : passerelle applicative

Double login : authentification des utilisateurs

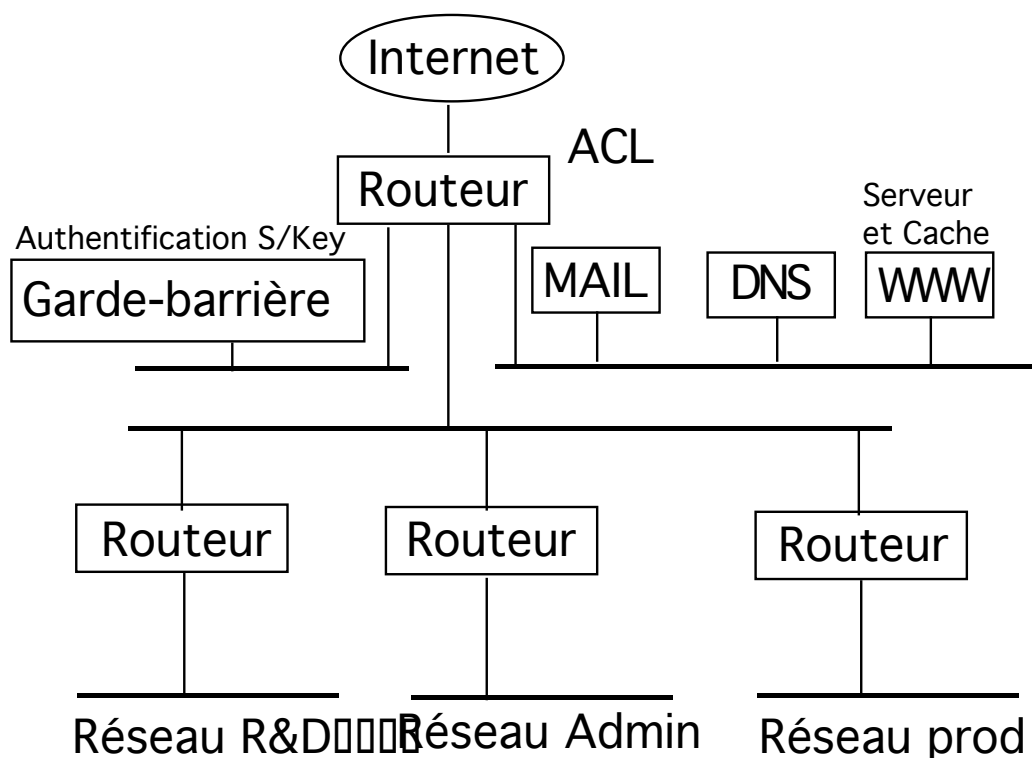
Applications en mode connecté

TIS

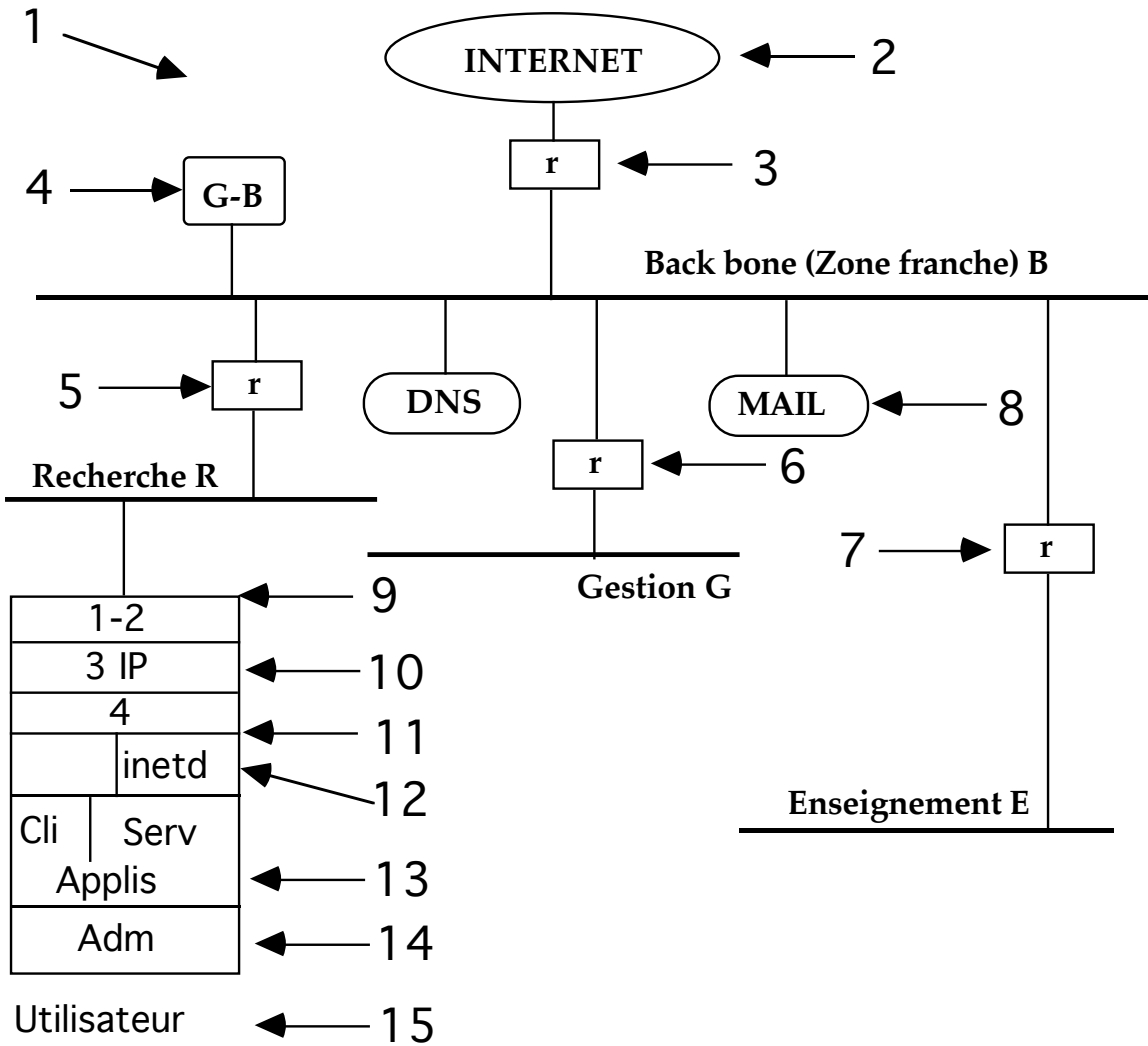
Version domaine public

Applications : telnet, rlogin, X11, SMTP, HTTP

Exemple d'architecture



RESUME : OU PEUT ON AGIR ?



RESUME : OU PEUT ON AGIR ?

- 1 : architecture physique et logique du réseau
- 2 : réseau Gestion "inconnu"
- 3 : annoncer uniquement R et B
- 4 : Garde-barrière
- 5 : filtrer le réseau E
- 6 : ne router que R et B, filtrer / appli et station
- 7 : ne router que R et B
- 8 : installer un "bon" sendmail
- 9 : pas de ifconfig
- 10 : pas de "route default"
- 11 : filtres et trace ---> tcpd, xinetd
- 12 : inetd.conf
- 13 : applis sécurisées : PGP
- 14 : surveiller - contrôler : COPS, CRACK
- 15 : sensibiliser, charte

CONSEILS POUR LA MISE EN PLACE D'UNE POLITIQUE DE SECURITE

Impliquer la Direction

La sécurité doit être vue globalement

Informatique et réseaux

Matériel

Personnel

Logiciels

Données

La sensibilisation est indispensable

Direction (---> responsabiliser)

Utilisateurs

Administrateurs de machines et de réseaux

---> La sécurité est l'affaire de tous

Le responsable sécurité informatique et réseaux

Un engagement moral : charte

Prise en compte à la conception

CONSEILS POUR LA MISE EN PLACE D'UNE POLITIQUE DE SECURITE

Etablir ses besoins et les risques

Prendre des mesures adéquates

Faire respecter les réglementations :
copie de logiciel
déclaration à la CNIL

Charte

Etre en contact avec le CERT-Renater

Pas de station sans administrateur

Campagnes régulières sur les mots de passe

Choisir entre garde-barrière applicatif ou non

Choisir quelques outils (crack, cops, ...)

CONSEILS POUR LES ADMINISTRATEURS DE RÉSEAUX

Protéger les éléments de communication

physiquement

accès logique

attention à SNMP

Segmenter le réseau / sécurité

Tri par activité (et degré de confiance)

Différencier les serveurs : sensibles ou non

Créer plusieurs réseaux physiquement et/ou
logiquement

CONSEILS POUR LES ADMINISTRATEURS DE RÉSEAUX

Architecture avec garde-barrière

Périmètre de sécurité : connaître tous les points d'entrée

Serveurs d'info dans une zone "ouverte"

Filtres dans le routeur d'entrée : obligatoire

Garde-barrière applicatif ?

Ne pas donner l'accès "international" à tous

Passer régulièrement SATAN

Chiffrement : difficile à mettre en place et à utiliser dans notre domaine

La messagerie n'est pas sécurisée

Evolution : PGP

CONSEILS POUR LES ADMINISTRATEURS DE STATIONS UNIX EN RESEAU

En cas de problème de piratage, avertissez immédiatement votre responsable hiérarchique

Répartir les utilisateurs / stations avec un critère sécurité

Utiliser avec circonspection les logiciels "publics"

A LA MISE EN SERVICE D'UNE STATION

Vérifier principalement
/etc/passwd et /etc/group
Accès sur /dev/*
Accès au fichier aliases
PATH et les fichiers .* de root
/etc/exports ou l'équivalent
ce qui touche à cron
les script rc*
le contenu de inetd
que tftpd n'est pas ouvert

CONSEILS POUR LES ADMINISTRATEURS DE STATIONS UNIX EN RESEAU

Supprimer

- /etc/hosts.equiv
- alias decode et uudecode dans aliases
- ce qui est utilisé par uucp

Choisir un bon umask pour les utilisateurs

- Forcer l'utilisation de su pour passer "root"
- .Xauthority pour les terminaux X

Installer

- Sendmail version 8
- le routage minimum
- crack dans le cron
- tcp_wrapper
- des vérifs de sécurité dans .login de l'admin

Passer cops et crack

Faire une sauvegarde complète

- Connecter la station sur le réseau et l'ouvrir aux utilisateurs

CONSEILS POUR LES ADMINISTRATEURS DE STATIONS UNIX EN RESEAU

OPERATIONS A EFFECTUER REGULIEREMENT

Sauvegardes

"ps -e" ou l'équivalent

Passer cops et crack

Installer les nouvelles versions de système/applicati

Sensibiliser les utilisateurs

Coup d'oeil sur les .rhosts et .netrc des utilisateurs

HABITUDES DE TRAVAIL

Attention au mot de passe de root

Logout chaque fois que l'on quitte son poste de trava

Travailler au minimum sous root

Ne pas laisser une autre personne travailler sous
root

Faire /bin/su au lieu de su

Utiliser un compte spécial pour les démos

Bien utiliser les groupes

Chaque compte doit correspondre à une seule
personne

Attention a SUID root

<http://www.urec.fr/securite.html>

DOCUMENTS, LOGICIELS ... STOCKÉS À L'UREC

Documents généraux

Lois en France

(textes de loi, chiffrement, CNIL, DISSI, SCSSI)

Chartes en français

Documents divers (mot de passe, orange book dictionnaires, RFC "Site Security Handbook", ...)

Articles en ligne (en HTML) :

Les outils de sécurité sur X11

RFCs et groupes de travail de l'IETF

Les CERTs

Documentations diverses sur les CERTs

CERT-Renater

CERT-CC

Notes d'informations d'autres CERTs (CIAC, ...)

Sécurité (documents, logiciels, patches, ...)

Réseaux (cours, RFCs, satan, tamu, ...)

Unix (conseils, cops, tcp_wrapper, ...)

Macintosh (disinfectant, gatekeeper, ...)

PC

SUR D'AUTRES SERVEURS

Français

- CRU (très complet)

- INRIA (logiciels Unix et réseaux)

- Groupe sécurité AFUU

- CNRS (sécurité des systèmes d'information)

Etrangers

- CIAC (logiciels de sécurité, documents, ...)

- NIST

- DFN-CERT

- CERT-CC

- FIRST

- TIS (garde-barrière)

Bonnes pages

- Antivirus PC (serveur ftp.loria.fr)

- Utilisation du chiffrement en France

- Filtres dans un routeur

- Patches SUN

- Kerberos

- PGP