SECURITE

Ce cours est très inspiré des textes diffusés par l'unité réseau du CNRS (www.urec.fr). La sécurité est une chose essentielle sur le réseau Internet. Elle est associée très étroitement aux lois de protection des données. On trouvera en fin de chapitre un extrait de la loi française sanctionnant les intrusions dans un système informatique.

Il n'y a pas de sécurité sans une réflexion globale au niveau de l'organisme et sans la nomination explicite d'une personne en charge de ce problème. En effet, d'après des statistiques 3/4 des sinistres sont dus à une « criminalité » interne (source CRU). La figure 1 montre la croissance des incidents sur le réseau.

1 - ORGANISATION

Le Computer Emergency Response Team (CERT, www.cert.org) est une partie d'un programme de Carnegie Mellon University. Il regroupe toutes les informations concernant les attaques du réseau, diffuse des recommandations et des corrections des trous de sécurité. Il maintient en relation tous les correspondants sécurité. Cette organisation ne remplace pas la police mais permet par la diffusion de courrier de manière hiérarchique de prévenir ou de contrer des attaques.

Elle recommande notamment l'adoption de charte de sécurité au niveau des organisations. Cette charte doit contenir :

- le respect des recommandations des administrateurs,
- le bon usage des outils,

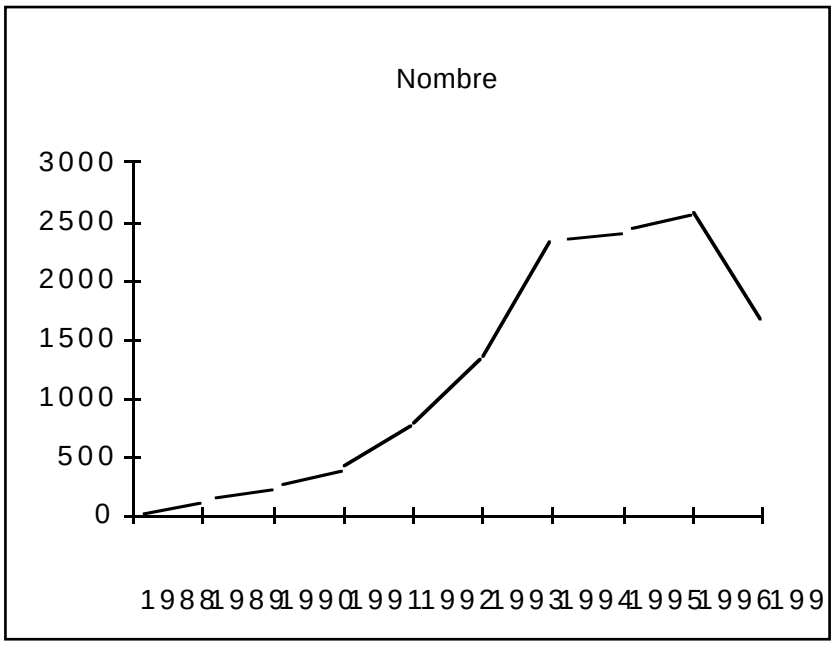

Figure 1. Incident réseau, source CERT

- la notification qu'un compte est personnel et non cessible,
- le respect des lois sur les logiciels,
- le respect des lois sur le multimédia,
- le rappel des lois.

L'organisation doit s'accompagner d'une campagne de sensibilisation à la robustesse des mots de passe, et de l'installation d'anti-virus sur les micros. Enfin, l'administrateur système doit mettre en place des filtres permettant la protection.

2 - FILTRES ET POLITIQUE DE FILTRAGES

Filtrer consiste à examiner le contenu d'une trame à un niveau de couche donné et en fonction de son contenu à acheminer ou non la trame.

L'ensemble des ports serveurs habituels est défini dans le RFC 1700. Il est possible de filtrer ces ports afin de minimiser les attaques possibles.

Par exemple, les datagrammes TCP comportent un bit indiquant si ce datagramme est une réponse à un datagramme précédent. Dans un datagramme d'ouverture de session, ce bit n'est pas positionné. Bloquer tout datagramme entrant ne positionnant pas ce bit interdit une ouverture de connexion de l'extérieur du réseau.

L'un des ports le plus fragile est le port 111 (portmap pour RPC) qui permet d'obtenir les numéros de port de service. La plupart des applications utilisant ce port sont en UDP, on peut donc par exemple filtrer les datagrammes UDPs inconnus (pas DNS, syslog, archie,...). Les datagrammes TCP sur le port 111 sont systématiquement filtrés par le bit d'ouverture de session.

Les serveurs X11 attribuent des ports 2000 à 2003 et 6000 à 6003 aux clients d'applications TCP. Ces ports de même doivent être filtrés.

Il est possible de filtrer également la trame Ethernet elle-même au niveau d'un routeur par exemple par :

- l'en-tête de la trame : adresses origine et destination, type,
- l'en-tête IP : protocole transporté, adresses IP origine et destination,
- l'en-tête TCP ou UDP : port.

Il est par contre impossible de filtrer les informations (retrouver le nom de l'utilisateur par exemple).

Deux politiques peuvent être mises en place :

- filtrer ce que l'on ne veut pas, vulnérable
- n'autoriser que ce qui est connu et interdire tout le reste, peu vulnérable mais mécontente les utilisateurs.

L'ensemble de ces mesures sont simples à mettre en place, économiques mais techniquement demandent une bonne connaissance des protocoles et de leurs trafics. Elles constituent une première solution en matière de pare-feux. Dans le cas de backbone interne, il convient d'installer les filtres sur le backbone. L'incidence sur les performances est à peu près nulle pour un backbone à 2Mb/s.

3 - EXEMPLE DE FILTRE SUR ROUTEUR

Les routeurs permettent de fabriquer des listes d'autorisations (access-list ou ACL sur CISCO). La commande permet de définir des interdictions ou des autorisations dans le sens sortant ou entrant. Elle est définie pour des protocoles (ip, udp, tcp, icmp) et des ports de provenance et de destination. Le filtre d'adresse est constitué par une adresse source suivi d'un masque puis une adresse destination suivie d'un masque.

Exemple de masque par exemple sur CISCO

129.90.0.0 0.0.255.255 définit la classe 129.90.x.x

129.90.0.0 0.0.255.129 définit la classe

{129.90.x.128, 129.90.x.1, 129.90.x.129}

Exemple de construction de liste

Un exemple pour CISCO (extrait de http://www.urec.fr/securite/commencer/) est donné ci-dessous. Le réseau interne est 192.56.62.x (classe C). On place des filtres sur le routeur d'entrée du site. Tout est autorisé sauf : tftp, NFS, SNMP. De plus,

- 192.56.62.80 ne doit pas communiquer avec l'extérieur
- le réseau 190.190.0.0 est interdit d'entrée
- on restreint SMTP serveur à 192.56.62.10
- on restreint HTTP serveur à 192.56.62.20

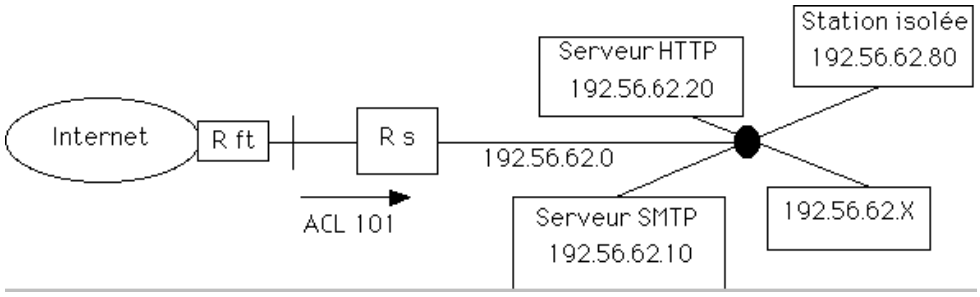

Figure 2. Schéma du site.

```
! Extrait de la description de l'interface du routeur d'entrée côté Internet
interface Ethernet0
ip address 193.5.5.1 255.255.255.0
ip access-group 101 in
!
! 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
! 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
```

4 - OUTILS DE DIAGNOSTICS

Les principaux logiciels permettant l'audit de sécurité d'un réseau de machine sont ISS(Internet Security Scanner) et SATAN. Ils effectuent des tests de comptes, recherchent les alias dangereux et analysent les trous de sécurité.

Exemple de résultat de commande 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)

COPS (Computer Oracle and Password System) permet d'effectuer l'audit d'une machine Unix. Il vérifie les permissions de certains fichiers, les mots de passe, le contenu des fichiers passwd et group, les programmes lancés par rc et cron, les fichiers SUID root, l'installation du FTP et recherche les trous de sécurité.

Exemple de résultat de commande COPS.

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!

Le logiciel crack est un logiciel permettant de tester la fiabilité des mots de passe. En effet, par combinaison sans dictionnaire, la puissance des machines permet de découvrir des mots de passe jusqu'à 6 caractères. Crack enrichit ces combinaisons par des dictionnaires, les encode puis les compare à /etc/passwd. Il mémorise les résultats pour des exécutions ultérieures.

Exemple de résultat de commande crack.

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

La protection d'une machine UNIX est essentielle puisqu'elle est vulnérable. En règle générale , on restreint le nombre de serveurs, on enlève rexd et tftpd, on ote les r-commandes, finger. Si NFS n'est pas utilisé supprimer nfsd sinon il faut également vérifier régulièrement le /etc/exports de NFS. Le premier logiciel à installer est tcp_wrapper. Ce logiciel permet l'audit et le contrôle d'accès à la machine. Il s'intercale entre inetd et tout serveur et est transparent à l'utilisateur. Les traces d'intrusions se trouvent dans syslog.