Description de la sécurisation d'un réseau local dans le monde universitaire

Exemple du réseau *math.jussieu.fr*

Joël Marchand - CNRS - jma@math.jussieu.fr

Plan

- Contexte organisationnel, culturel et histoire
- Situation actuelle
  - Les 3 vlan des postes utilisateurs
  - Le vlan des postes de gestion-secrétariat
  - Le vlan des serveurs
  - Sauvegardes
  - Les virus
  - Les utilisateurs
  - Outils de monitoring et de diagnostics

Plan

- Evolutions envisagées
- Conclusion
- Remerciements

Contexte organisationnel

- Un ensemble de chercheurs, d'enseignants-chercheurs, de doctorants, de post-doctorants, de personnels administratifs, sous tutelle des Universités Paris VI, Paris 7 et du CNRS

- Environ 550 comptes informatiques, y compris les visiteurs

Contexte organisationnel

- D'abord sur le site de Jussieu, puis sur le site tampon de Chevaleret (Paris 13)

- Trois ingénieurs informaticiens (à temps partiel), et une dizaine de correspondants informatiques
(les *power-users* des équipes scientifiques)

Contexte organisationnel

- Budget commun uniquement pour les achats communs (réseau, serveurs) et les postes des thésards (terminaux X-Window). Autonomie financière et donc d'achat pour les postes dans les équipes scientifiques

- A notre connaissance, pas d'informations confidentielles à protéger

Contexte culturel

- Les mathématiciens ont très tôt pris le pas d'Internet, notamment pour la messagerie électronique, et ont vite appris le triplet

  telnet - *mail* - *ftp*

- Une très forte proportion de postes Macintosh (moitié du parc)

Contexte culturel

- Une connaissance d'Unix et des réseaux très variable selon les utilisateurs - une tendance libertaire forte - une acceptation de la hiérarchie faible

- Forte culture Unix chez les informaticiens successifs, et même avant leur arrivée (1996) chez les *power-users*

Contexte culturel

- Un bon soutien des directions
- Réunion semestrielle d'une commission informatique, regroupant les correspondants informatiques et les informaticiens

Histoire

- Rentrée 1998 : piratage du serveur central et unique Sun Solaris, par snif de mot de passe

- Après de fortes tensions, et par la volonté et la ténacité de mon prédécesseur, Eric Boix, acceptation du principe de politique de sécurité. Accord trouvé pour suppression du service telnet, par remplacement par S/Key ou SSH, mais *pas touche* à FTP et à POP

Histoire

- Avril 2000 : piratage par snif de mot de passe lors d'une connexion FTP et rejeu dans une connexion SSH (normal !)

- Institution de deux tables de mots de passe, avec demande aux utilisateurs d'avoir des mots de passe distincts

Histoire

  - 1 pour l'accès par SSH et FTP depuis l'extérieur, et à la messagerie par POP
  - 1 pour l'accès aux serveurs interactifs internes
  - acceptation du risque de tricherie de la part des utilisateurs

- Renforcement de la politique de sécurité, et décision de supprimer FTP fin 2000

Histoire

- Développement par Albert Shih d'un outil *webftp* : application écrite en PHP, tournant sur Apache + mod_ssl, permettant de faire
  - sur Internet, du HTTP sur SSL avec le navigateur du client
  - en interne, du FTP avec le serveur FTP interne

- Ceci de manière à compléter l'offre insuffisante d'outils FTP sur SSH

Histoire

- Fin 2000 : suppression du service FTP

- Remplacement sans douleur par
  - clients SSH sachant faire *scp* ou *sftp*
  - FTP en tunnel sur SSH
  - webftp

Histoire

- Mi-2001 : séparation du serveur d'accès distant par SSH et du serveur de messagerie

- Si bien que désormais les deux mots de passe distincts servent
  - 1 pour accès par SSH uniquement
  - 1 pour tout le reste, y compris POP

Histoire

- Actuellement : douce pression pour usage d'outils de messagerie sécurisés
  - POP sur SSL
  - POP sur SSH
  - webmail (IMP)
  - .forward

- Objectif : suppression au maximum de POP avec mot de passe en clair

Situation actuelle

- Réseau local
  - Ethernet 100BaseT tout commuté
  - qui fonctionne bien
  - exploité au niveau 2 par le CRI (CCR)
  - merci le désamiantage !

- Achat et gestion, en bonne intelligence avec le CRI, d'un commutateur-routeur Foundry FastIron 4802

Situation actuelle

- Définition de 5 vlan correspondants à 5 sous-réseaux IP :
  - 1 pour les serveurs
  - 1 pour les postes de gestion-secrétariat
  - 3 pour les postes utilisateurs

- Routage-filtrage entre ces 5 vlan, c'est-à-dire toute communication *Internet - interne* mais aussi *poste interne - serveur interne*

Situation actuelle

- Internet == tout ce qui n'est pas interne, c'est-à-dire y compris nos voisins

- Mode par défaut : tout est interdit, sauf ce qui est autorisé

Les 3 vlan des postes utilisateurs

- Aucune connexion ne peut être établie depuis Internet vers ces 3 vlan des postes utilisateurs. L'ACL est donc grosso modo
  - *permit tcp any any established*
  - réponses en UDP des DNS du site et du serveur NTP
  - tout est autorisé entre ces vlan et depuis le vlan des serveurs, sauf depuis la machine d'entrée
  - *deny ip any any log*

Les 3 vlan des postes utilisateurs

- On part du principe que ces postes sont hors contrôle (ce qui est le cas), que n'importe quoi peut être connecté au bout, à notre insu éventuellement

- Nous ne contrôlons pas les adresses MAC sur les commutateurs, et n'offrons pas de serveur DHCP

Les 3 vlan des postes utilisateurs

- Vu le contexte fortement mobile des gens, l'accès facile aux locaux, et la progression des portables, nous considérons donc que ces zones sont potentiellement à risque, mais qu'il n'y a pas de *méchant* dessus
- Nous n'avons pas d'idée claire sur comment améliorer la situation, avec un coût de gestion humain raisonnable, surtout si on lève l’hypothèse précédente

Les 3 vlan des postes utilisateurs

- Pistes :
  - logiciel *Survey*
    (Luc Veillon et Jean-Marc Vinet de l'IRD)
  - arriver à *isoler facilement* les machines inconnues (portables des visiteurs) dans un vlan spécifique avec encore plus de restrictions

Le vlan des postes de gestion-secrétariat

- Isolement *au cas où* de ces postes à caractère un peu plus sensibles

- Il permet de gérer aussi, au cas par cas, toutes les exceptions. Exemples :
  - le logiciel de comptabilité de l'université fait des impressions par envoi de connexions *lpd* vers les imprimantes des secrétaires

Le vlan des postes de gestion-secrétariat

  - Idem avec d'autres applications de gestion
  - Idem pour des exceptions et des personnes particulières, ayant des besoins particuliers (ex : AppleShare sur IP)
- On envisage de restreindre encore plus le filtrage sur ce vlan, pour ne plus router même de l'intérieur vers l'extérieur les PC de gestion, et au passage forcer l'usage du proxy-cache Web (Squid)

Le vlan des postes de gestion-secrétariat

- Mais est-ce que cela va améliorer la sécurité, sans introduire des pertes de fonctionnalité ?

- On teste actuellement la migration de gestionnaires d'un PC Windows 9x vers un client léger relié à notre serveur W2K/MetaFrame

Le vlan des postes de gestion-secrétariat

- Idée de passer les salles libre-service sur un VLAN de ce type (mais un autre bien sûr !)

- Idem peut-être pour les portables

Le vlan des serveurs

- Une dizaine de serveurs sous
  - FreeBSD 4.x (machines de service et en visibilité sur Internet)
  - Linux Redhat 6.2 et 7.1 (machines internes de session interactive, pour notamment les 120 terminaux X-Window et clients légers)
- Un serveur Windows 2000 Server avec l'extension Metaframe (accès par ICA et X11, en plus de RDP)

Le vlan des serveurs

- Un serveur Macintosh sous AppleShare IP, pour espace de duplication des documents pour les PC/Windows (SMB) et les Mac (AppleShare)

- Le tout dans une salle, à accès limité à l'équipe informatique, avec une grosse climatisation, et des petits onduleurs pour alimenter chacun quelques serveurs

Le vlan des serveurs

- La sécurité physique de cela nous semble néanmoins fragile

- Parmi les serveurs Unix, deux machines fichiers avec NFS v2 et v3 . Choix de ne pas exporter les $HOME vers d'autres machines que les serveurs que nous gérons. Par peur du syndrome suivant :

Le vlan des serveurs

- *linux single mode*
- *adduser -u uid_boss boss*
- *su - boss*
- *more ~boss/rapport.tex*
- *mutt -f ~boss/Mail/machin*

- On essaie de suivre les avis de sécurité sur FreeBSD et Linux, et de faire les mises à jour *assez rapidement*. Découverte récente de l'outil *up2date* de RedHat

Le vlan des serveurs

- Répartition des services sur plusieurs serveurs
- Ceux qui sont vus depuis l'extérieur
  - DNS + proxy-cache + TFTP des tX + syslog central
  - SMTP + POP + IMAP + webmail
  - LDAP + webftp
  - telnet+S/key + SSH + FTP sur SSH + HTTP

Le vlan des serveurs

- Ceux qui sont purement internes
  - 2 pour NFS
  - 4 de sessions interactives, via XDM et SSH

- Le filtrage est donc grosso modo strictement limité
  - aux accès depuis les 4 autres vlan
  - aux ports TCP correspondants des services externes
  - aux réponses du serveur NTP et des serveurs DNS du site en UDP

Le vlan des serveurs

- Filtrage du service DNS :

  - Utilisation dans *named.conf* de l'option

    - query-source address * port 53

  – Ce qui permet de pouvoir limiter l'ACL à

- access-list 111 permit udp any host 134.157.13.103 eq dns
- access-list 111 permit tcp any host 134.157.13.103 eq dns

Le vlan des serveurs

- Filtrage du service FTP :
  - en tunnel sur SSH, on ne fait passer en fait que le protocole FTP, pas le protocole FTP-DATA.
  - avec *wu-ftpd*, en forçant le client à être en mode passif, on doit laisser ouvert un intervalle de ports > 1024 qui sont donnés par *wu-ftpd* au client pour se connecter en FTP-DATA (merci à Luc Veillon de l'IRD)

Le vlan des serveurs

- En règle générale, en plus du filtrage IP,
  - usage systématique des TCP-wrappers
  - un service = un uid distinct des autres et de 0

Sauvegardes

- Méthode du *bison sur la prairie* pour être tranquilles
- Volume à sauver très faible en rapport au nombre de personnes (< 100 Go)
- Objectifs : coût minimal - indépendance maximale

Sauvegardes

- Quatre lecteurs DLT 4000 sur
  - machine de messagerie
  - deux serveurs NFS
  - serveur Macintosh (logiciel Retrospect)

- Sur les trois premiers, usage de *tar*, pour sa simplicité et sa portabilité dans le temps et l'espace

Sauvegardes

- On sauve tout
  - toutes les nuits
  - + bande hebdo dans la nuit de lundi à mardi (rotation sur 3 bandes)
  - + bande mensuelle dans la nuit du 1er au 2 (rotation sur 3 bandes)

Sauvegardes

- On stocke les bandes *pas tout près* de la salle machines, et on en archive *de temps en temps* à notre domicile

- Recopie des données des autres serveurs par *rsync, scp et smbtar*, sur l'un des serveurs NFS, pour miroir et pour sauvegarde sur bande

Sauvegardes

- Depuis récemment, miroir, sur des disques IDE pas chers , des disques SCSI d'un des serveurs NFS, par *tar*, une fois par nuit

- Cela permet de récupérer rapidement le *rm* malheureux

Sauvegardes

- Comme on sait qu'on sera à nouveau piraté, et que nos serveurs, PC d'intégrateurs sans maintenance, sont susceptibles de tomber en panne à tout instant, dispositions prises pour
  - possibilité a priori de migrer un service d'une machine à une autre (faible charge de chacune, systèmes homogènes)

Sauvegardes

– script de post-installation et post-configuration, qui permet d'automatiser la partie *simple* de la configuration système, après la descente du CD-ROM.
  Exemples :
  - mise en place des bons fichiers dans /etc
  - les liens symboliques qu'il faut
  - la mise en place des clefs SSH
  - la suppression des bits s

Sauvegardes

- on pense donc pouvoir en moins d'une demi-journée pallier la défaillance ou la nécessité de devoir mettre *off* un serveur, au moins pour les services de base (DNS, SSH, SMTP/POP, HTTP, FTP, LPD)
- mais nous n'avons pas testé en grandeur nature encore..

- Point critique connu : quid si le gros serveur de fichiers lâche ?

Les virus

- Mise à disposition (depuis une année), via les correspondants informatiques, et par un tour du parc par un stagiaire, des anti-virus pour Windows et MacOS

- Appels réguliers à sauvegarde volontaire des disques personnels et encouragement à vérification du bon fonctionnement de ces anti-virus

Les virus

- Page Web d'explications
  http://www.math.jussieu.fr/informatique/virus.html

- Comme le parc PC/Windows est faible, peu de problèmes, même si cela monte

- Consensus pour ne pas mettre d'anti-virus sur le serveur de messagerie

Les virus

- Début de sensibilisation aux risques liés au surf sur le Web, avec comme *exemple* la perte totale d'un disque dur

Les utilisateurs

- Depuis l'automne 1998, la sécurité informatique est un sujet récurrent au sein du laboratoire. Il était passionné, mais devient normal et mieux accepté

- Néanmoins on n’a pas pu contraindre tous les utilisateurs à signer explicitement une charte informatique

Les utilisateurs

- Décision a été prise de considérer que tout le monde est tenu de respecter les chartes du CNRS, du CCR et de RENATER

- Depuis deux ans, l'ouverture d'un compte se fait après signature de la prise de connaissance de ces chartes. On envisage de faire une telle campagne de signatures pour les anciens comptes

Les utilisateurs

- Dans la pratique, très peu de débordements constatés du bon usage souhaité

- Nombreuses pages Web rédigées et enrichies au fil du temps sur comment se connecter depuis l'extérieur, pour les trois services telnet / FTP / POP

Les utilisateurs

- Tout est accessible depuis

  http://www.math.jussieu.fr/informatique/acces.html

- Avec notamment
  - documentations sur SSH, SSL et S/Key
  - usage de SSH pour remplacer telnet et FTP
  - comment faire des tunnels sur SSH
  - comment utiliser POP sur SSL
  - usage du webmail

Les utilisateurs

- Plusieurs séances de formation sur
  - le b-a-ba sur les réseaux (couches, vocabulaire)
  - SSH et les outils associés

- Les comptes pour les personnels non-permanents ont une date de blocage, qui est automatiquement prise en compte. Leur suppression effective reste manuelle, au début de chaque mois

Outils de monitoring et de diagnostics

- Syslog centralisé + *swatch* + *logcheck*
- Usage intensif de *Big Brother*
- Bricole locale sur les signatures MD5 des binaires des serveurs
- Usage de *detescan.pl* sur les logs du routeur

Outils de monitoring et de diagnostics

- Passages épisodiques de *Nessus*, et de *John the Ripper* sur les tables de mot de passe
- Monitoring de l'espace disques et de la bande passante réseau par *MRTG*
- Début de l'usage de *Survey*

Evolutions

- A court terme
  - séparation en deux du premier serveur :
    - 1 machine DNS/proxy-cache Web
    - 1 machine syslog
    - passage du service TFTP sur un serveur NFS
  - séparation en deux de la machine d'entrée :
    - 1 qui soit une impasse - sans rebond possible
    - 1 qui permette d'accéder vers les serveurs internes, mais sans montage NFS du $HOME, comme actuellement
    - exercice : où est la faille actuelle ?

Evolutions

- A moyen terme
  - restriction des tunnels SSH possibles depuis la machine d'entrée uniquement vers les services voulus (POP, IMAP, FTP, proxy-cache)
  - restriction au maximum de ce qui est autorisé à passer entre les postes clients et les serveurs
  - mise en oeuvre de *Snort*
  - achat d'un nouveau filer *solide et redondant*
  - passage de SSHv1 à SSHv2

Evolutions

- A plus long terme
  - extension de cette politique de sécurité à d'autres labos de maths du site
  - mise en place d'un outil comme *Tripwire*
  - usage des niveaux de sécurité sur FreeBSD
  - dédoublement du serveur DNS en un DNS public et un DNS privé
  - idem avec le serveur de messagerie
  - suppression de POP avec mot de passe en clair

Conclusion

- Bonne acceptation par les utilisateurs de cette politique (concertation, explications, documentations, formations et délais)

- Estimation d'avoir actuellement un environnement raisonnable par rapport à ce qu'on sait faire (techniquement), ce qu'on peut faire (humainement), et ce qu'on doit faire (pas de confidentialité forte exigée)

Conclusions

- Possibilité de compléter par des évolutions à peu près transparentes pour 95% des utilisateurs, et acceptables par les *power-users*

- Au-delà ? L'usage de bi-clefs RSA et plus tard de certificats électroniques se heurtera à une difficile compréhension de la part des utilisateurs, et à leur forte mobilité

Remerciements

- Tous mes remerciements
  - A Eric Boix, qui a enclenché courageusement ce long processus, et a réalisé les fondements de ce qui existe aujourd'hui
  - A Albert Shih, mon collègue de tous les jours, qui a développé l'application WebFTP, et s'est plongé avec brio dans SSL, HTTP sur SSL, POP sur SSL, IMAP sur SSL, les solutions webmail, …
  - A Thierry Besançon et Pierre David, mes maîtres de longue date
  - Au groupe Sécurité de l'UREC, unité réseaux du CNRS, pour son support, ses informations, ses formations, la constitution d'un groupe d'échange
  - A l'OSSIR, pour ses activités, et la richesse de ses réunions et de ses listes de diffusion
  - A de nombreuses personnes lues ou rencontrées sur le Net, dont je ne fais que reprendre bon nombre d'idées ou de solutions