SÉCURITÉ INFORMATIQUE

SECURITE DES SYSTEMES D'INFORMATION

Numéro 27 Décembre 1999

éditorial

Dis, raconte-moi une histoire…

L'intrusion malveillante dans les réseaux informatiques n'est pas un phénomène nouveau, mais avec l'explosion du nombre des bons et méchants internautes le volume des attaques subies par nos systèmes poursuit une croissance spectaculaire. Vous pourrez vous convaincre de la réalité de cette menace en lisant plus loin les témoignages que des administrateurs et des responsables de sécurité ont bien voulu nous faire remonter.

En nous montrant comment ils ont détecté les intrusions, comment elles ont révélé les faiblesses de leur installation et comment ils y ont remédié, ils nous donnent une grande leçon de franchise et d'honnêteté intellectuelle. Nous devons les en remercier.

Dans l'éternel affrontement de l'épée et du bouclier, l'ingéniosité perverse des pirates ne faiblit pas, et il n'y a donc pas de honte à s'être fait pirater comme cela est arrivé et arrivera encore aux systèmes même les mieux protégés.

N'enviez pas celui qui se vante de n'avoir jamais laissé passer une attaque. Le plus souvent, c'est son manque de vigilance qui ne lui a pas permis de repérer celles qui se sont produites et parfois répétées pendant de longs mois. Lorsqu'il y trouve son intérêt, le pirate sait se montrer discret afin de garder ouverte la porte dérobée qu'il a installée ou de cacher les bombes à retardement qu'il est venu placer.

Alors, ouvrez l'œil, épluchez les logs, offrez-vous un outil de surveillance du trafic entrant et, lorsque vous aurez détecté une belle tentative d'intrusion, venez nous la raconter pour que nos collègues puissent profiter de votre expérience. Merci d'avance.

Philippe Schreiber
Fonctionnaire de défense

C'est arrivé aussi chez nous …

Voici une histoire fort édifiante qui montre à quel point, en tant que laboratoire de recherches, nous sommes vulnérables et désarmés face à certains actes de malveillance. Les noms propres et les noms des machines en cause ont été modifiés de façon à préserver l'anonymat des personnes et des sites.

Les faits…

Deux semaines de vacances, suivies d'une mission pour participer à un congrès, je retourne au laboratoire après donc quasiment trois semaines d'absence. Mon premier réflexe est d'ouvrir ma boîte aux lettres, dans laquelle se sont accumulés plus de 200 messages. Fort heureusement, ces messages ne sont pas tous aussi importants les uns que les autres. En particulier de nombreux messages émanaient d'une liste de diffusion dont je me suis désabonné depuis. En revanche, en tant qu'administrateur du réseau local, je reçois aussi régulièrement des messages provenant des différents serveurs du laboratoire.
Il me semble utile de préciser ma position : je suis enseignant à l'École Supérieure des Techniques Avancées dans le Domaine du Piratage Informatique Subi (ESTADPIS) à Paris et chercheur dans un laboratoire associé au CNRS ; accessoirement administrateur du réseau du laboratoire. Mon serveur principal, celui sur lequel se sont passés les événements décrits dans cet article, est un PC fonctionnant sous Linux RedHat 4.2.

En dépouillant ma boîte aux lettres, je vois passer (rapidement) un premier message d'erreur, provenant du processus cron de mon serveur principal ; je le jette sans m'y attarder. Deux minutes plus tard, à nouveau le même message ; je le jette également. Puis à nouveau le même message… je commence à me poser quelques questions. Mon serveur est opérationnel depuis plus d'un an et je n'avais encore jamais reçu ce type de messages.
J'y regarde donc de plus près ; en fait, il s'écoule précisément une semaine entre chaque message ; ces derniers résultent tous de ma commande cron hebdomadaire. Or le seul fichier présent dans /etc/cron.weekly est makewhatis.cron ; ce script reconstruit la base de données des mots-clés à partir des fichiers d'aide en ligne. Le texte du message d'erreur est le suivant : zcat: ./y2.3.gz: not in gzip format.
Les connaisseurs identifient tout de suite le fichier d'aide en ligne pour la fonction y2 (fonction de Bessel de la librairie mathématique) dans la section 3 du manuel. Or il n'existe en fait aucune fonction y2… les fonctions de Bessel disponibles en standard sont y0, y1 et yn. Une recherche rapide avec la commande locate y2.3.gz confirme le diagnostic et fournit l'arborescence complète du fichier : /usr/man/man3/y2.3.gz.

Je vais donc voir ce fichier d'un peu plus près… Je constate qu'en effet ce n'est pas un fichier compressé, mais un fichier texte parfaitement lisible avec tout bon éditeur. Par contre, le fichier fait un peu plus de 20 Mo, et donc l'éditeur « vi » est un peu long à le charger en mémoire ! Les premières lignes que j'ai alors devant mes yeux sont malheureusement édifiantes et identifiables tout de suite : date et heure, machines d'origine et de destination, numéro de port tcp/ip, nom de login, mot de passe, puis le détail de toutes les commandes passées lors de la session interactive. Cela est caractéristique de l'activité pirate d'un logiciel sniffer qui tourne sur mon serveur.
Les traces ont démarré le 2 avril 1999 de bonne heure le matin (donc aussi le lendemain du 1er avril, date célèbre pour les plaisanteries de toutes sortes… est-ce là du pur hasard ?) par une connexion que j'avais effectuée sur mon serveur. Nous sommes le 6 mai 1999, soit un peu plus d'un mois après le démarrage du sniffer. Les 770 000 (environ) lignes traçaient toutes les communications, les ports privilégiés par le sniffer étant 21 (ftp), 23 (telnet) et 110 (pop), comme par hasard 3 protocoles utilisant une identification avec mot de passe. Environ 70 000 mots de passe sont ainsi identifiables (on retrouve plusieurs fois les mêmes mots de passe), en France et dans le monde, sans compter les traces de commandes su ou passwd…

Première étape : on déconnecte la machine du réseau.
Deuxième étape : on essaie de calmer les chercheurs et enseignants du laboratoire, qui ne peuvent plus accéder au mail, à Internet… En effet, ce serveur était configuré avec la mascarade IP et était le point de passage obligé pour accéder aux ressources extérieures.
Troisième étape : on essaie d'inventorier les dégâts, et là, cela commence à faire mal…

Les dégâts…

Après de nombreuses recherches, voici ce nous avons découvert sur notre serveur, relativement au sniffer :

- l'interface réseau tournée vers l'extérieur est configurée en mode PROMISC ;
- l'exécutable du sniffer est identifié : /usr/sbin/inetd, dont la version de base (15932 octets) a été remplacée par un programme de 38924 octets ;
- le fichier dans lequel était tracé le trafic : /usr/man/man3/y2.3.gz.

Nous avons ensuite découvert un processus parasite qui apparaissait dans la liste des processus sous la forme ./lpd. On est facilement tenté de confondre ce processus avec le démon gestionnaire d'impression, mais la syntaxe ./ pour un processus lancé par root est tout de même suspecte. Après recherche sur tous les fichiers du disque, nous avons identifié toute une arborescence parasite /usr/sbin/rinetd.d dans laquelle nous avons retrouvé, entre autres, l'exécutable lpd. Un examen approfondi des fichiers dans cette arborescence nous a

permis d'identifier un egg-drop avec les caractéristiques suivantes :

- un script /usr/sbin/test a été installé, à ne pas confondre avec l'exécutable standard /usr/bin/test ; ce script permet de relancer l'egg-drop automatiquement ;
- le fichier /etc/crontab a été modifié par ajout d'une ligne permettant de déclencher l'exécution du script précédent toutes les 10 minutes ; selon l'auteur du logiciel parasite en question, cette étape serait requise par la présence d'un bug non identifié ayant pour conséquence l'interruption aléatoire du démon sur certains systèmes ;
- l'egg-drop maintenait une connexion IRC permanente avec un autre serveur français, mimosa.univ.fr, appartenant à une institution d'enseignement, en utilisant le port non standard 41609 ;
- l'egg-drop maintenait également une connexion IRC permanente avec un serveur, probablement aux États-Unis, cage.arpa.com (dans le courant du mois de juin, un autre serveur du même site a rejeté plusieurs tentatives de connexion telnet en provenance d'une machine rage.arpa.com ; étonnant non ?).

Parmi les fichiers générés par l'egg-drop, nous avons également identifié trois serveurs français potentiellement concernés par une affaire similaire : mimosa.univ.fr que je viens de mentionner ci-dessus, ancolie.univ.fr (autre institution française d'enseignement) et bleuet.com.fr (institution à vocation commerciale cette fois) ; ainsi qu'un serveur en Finlande, un aux États-Unis et deux au Japon.

Contact a alors été pris avec les administrateurs des serveurs mimosa.univ.fr et ancolie.univ.fr ; nous avons rapidement pu établir que ces deux serveurs avaient été attaqués de la même façon que nous, avec les mêmes programmes pirates générant les mêmes fichiers dans les mêmes répertoires. Dans tous les cas, les traces générées par le sniffer commencent le 2 avril 1999.

Concernant le serveur bleuet.com.fr, il semble que les fichiers du disque aient été détruits pour une raison qui n'a pas été identifiée par les administrateurs locaux.

Les identifications des machines à l'étranger ont alors été transmises au CERT-Renater.

Les coûts…

Il semble intéressant d'analyser les conséquences d'une telle attaque informatique. Tout d'abord, notre serveur Linux filtrait systématiquement tous les accès depuis le réseau par l'intermédiaire de tcp-wrapper. J'ai donc sérieusement envisagé l'éventualité d'une intrusion provenant de l'intérieur du laboratoire (80 % des intrusions informatiques sont, paraît-il, amorcées depuis l'intérieur même du site visé). Cette éventualité n'a certes pas survécu très longtemps ; néanmoins cela conduit à un climat assez malsain de suspicion mutuelle.

De même, un des premiers effets de l'egg-drop identifié sur notre serveur était la connexion IRC permanente avec mimosa.univ.fr ; à nouveau cela entretient un climat de méfiance vis-à-vis du site en cause. Rapidement, nous avons finalement conclu que cette machine était victime au même titre que nous.

Nous devons également envisager le problème du point de vue du crédit du laboratoire vis-à-vis de ses partenaires industriels. De nombreux laboratoires mènent des recherches en collaboration avec ce type de partenaires, dans le cadre de contrats prévoyant souvent des clauses de confidentialités. Or il est extrêmement difficile de savoir quelles informations ont été récupérées par les pirates à partir de notre système.

Comme de nombreux autres laboratoires de recherche, nous entretenons également des relations privilégiées avec d'autres chercheurs, en France et à l'étranger. Ce type de collaboration implique généralement des transferts d'informations entre notre serveur au laboratoire et d'autres serveurs à l'étranger. Or toutes ces connexions ont été sniffées ; il convient donc d'analyser en détail le fichier des traces du sniffer pour identifier clairement ce qui a été sniffé ou pas, et intervenir auprès des administrateurs des sites étrangers éventuellement concernés. D'une part cela demande beaucoup de temps, d'autre part cela nous met dans une position délicate vis-à-vis des administrateurs en question.

Je dois reconnaître que tous les contacts que j'ai pu avoir dans cette affaire ont été très positifs, ma responsabilité individuelle n'ayant jamais été mise en cause. J'ai personnellement veillé à maintenir cette situation de confiance en assurant une totale transparence dans l'exploitation des données issues du sniffer. Je tiens du reste à remercier toutes les personnes concernées par leur compréhension, leur assistance et le temps qu'elles ont pu me consacrer.

On peut également essayer de quantifier les conséquences d'une telle affaire de façon plus concrète. La première conséquence est l'immobilisation d'un serveur : l'ordinateur ne peut plus être connecté au réseau ni assumer son rôle, mais il faut également maintenir la machine en l'état le plus longtemps possible, afin de garder les traces susceptibles d'expliquer clairement ce qui a pu se passer. Deuxièmement, il faut réinstaller et reconfigurer totalement un ordinateur secondaire pouvant se substituer à la machine agressée. Là encore, il faut pouvoir disposer d'un ordinateur, installer les systèmes et configurer tous les outils utilisés par le laboratoire. Enfin, il faut aussi compter le temps que nous consacrons à identifier les sources du piratage, à contacter les autres administrateurs concernés, à analyser en détail toutes les connexions sniffées,… autant de temps que je ne peux pas consacrer à des activités de recherche ou d'enseignement correspondant à ma fonction principale. On pourrait également prendre en compte le temps consacré à cette affaire par l'administrateur du réseau sur notre site, par les services du CERT-Renater ou de l'UREC,… en fait les conséquences humaines et financières sont difficilement chiffrables.

Il me semble également important de souligner que les conséquences ne sont pas localisées dans le temps, mais qu'elles vont probablement s'installer dans la durée. En effet, je vais être conduit à surveiller de façon accrue tout ce qui se passera sur mon nouveau serveur, et ce sûrement pendant plusieurs mois.

Pourra-t-on revenir à une situation antérieure ? Probablement non. Les considérations de sécurité m'ont déjà conduit à limiter plus encore les accès au laboratoire depuis le réseau ; il n'est pas dans mes intentions de rétablir certains services dans un avenir proche. Dans ce cas, ce sont les enseignants et chercheurs du laboratoire qui en subissent les conséquences dans leur méthode de travail quotidien.

L'intention des pirates…

Une dernière question que l'on est en droit de se poser dans ce genre de circonstances est d'essayer d'imaginer ce que recherchent les pirates qui attaquent ainsi des sites informatiques partout dans le monde. Il est certainement difficile de savoir précisément ce que ces gens ont en tête, néanmoins on peut tout de même avancer certaines hypothèses.

Il y a certainement de nombreux pirates pour lesquels l'aspect ludique domine, indépendamment des dégâts (humains, matériels, logiciels) qu'ils peuvent causer ou non sur les sites qu'ils attaquent. J'imagine que ce genre de pirate ne représente pas un trop grand danger, dans la mesure où il se satisfera d'avoir réussi à pénétrer le système qu'il visait, le fera peut-être savoir par orgueil personnel, et continuera ensuite à rechercher d'autres sites vulnérables… Un premier site piraté peut alors servir de rebond pour attaquer ailleurs.

Beaucoup plus problématique est l'intention de compromission qui porte atteinte à l'image de marque d'un laboratoire ou d'une institution. Dans certains cas, la divulgation de ce type d'attaque peut porter un coup sévère à la crédibilité et au sérieux de la gestion informatique d'un laboratoire, ce qui peut expliquer que certains sites piratés ne diffusent pas l'information, ou que certains articles paraissent de façon anonyme… N'oublions pas non plus que nos ordinateurs sont susceptibles de contenir des informations confidentielles (personnelles, résultats de recherche, rapports…) dont la divulgation peut porter un sévère préjudice à l'institution visée.

Il y a aussi le pirate qui casse pour le plaisir de casser ; il est difficile de se protéger de ce genre de pirate, son intention étant dès le départ de causer un maximum de dégâts en un minimum de temps, juste pour rire…

Il faut également penser que les pirates, une fois qu'ils ont réussi à prendre le contrôle sur un système distant, peuvent utiliser comme ils le souhaitent les ressources de ce système, en particulier les espaces disques. Ces zones de stockages gratuites permettent de stocker temporairement, dans des répertoires difficilement détectables, des données que nous ne contrôlons pas (logiciels piratés par exemple ; imaginez que votre ordinateur serve involontairement de serveur de téléchargement d'une suite bureautique bien connue tournant sur PC…), voire compromettantes du point de vue de la justice française ! Je trouve tout de même inquiétant que mon serveur soit resté hors contrôle pendant plus d'un mois !

Je souhaiterais terminer cette réflexion en citant une phrase entendue lors d'une journée de sensibilisation aux problèmes de sécurité informatique organisée par le CNRS : « Le pirate est seul, mais adore chasser en meute… » ; ce qui signifie que les pirates informatiques partout dans le monde ont un potentiel de communication énorme qui leur permet de diffuser très rapidement toute information susceptible d'intéresser leur communauté, comme la vulnérabilité d'un site par exemple.

Peut-être les laboratoires des universités et du CNRS, victimes d'agressions informatiques, devraient-ils mettre en œuvre des moyens de lutte communs, et en particulier privilégier le partage et la communication d'informations. On trouvera là une des raisons pour lesquelles j'ai pris le temps de rédiger ce document…

Moralité…

Indépendamment de ce piratage, je terminerais en décrivant brièvement un autre incident qui s'est produit sur le même serveur il y a un peu plus d'un an. L'incident en question est moins grave que ce que je viens de décrire, d'autant que je l'ai détecté très vite et que l'agression a été neutralisée tout de suite.

Un matin, j'ai trouvé dans ma boîte aux lettres toute une série de messages d'erreur provenant du démon sendmail, m'indiquant que les adresses électroniques des destinataires étaient incorrectes. En y regardant de plus près, de nombreuses adresses contenaient en effet deux caractères @ par exemple, rendant ainsi les adresses non conformes et les messages impossibles à délivrer. J'ai ainsi pu détecter une grande quantité de messages en attente d'émission. Or ces messages étaient envoyés depuis un site aux États-Unis à destination principalement de personnes ayant un compte chez AOL. Quant au message proprement dit, il donnait simplement l'adresse d'un site Web, très probablement à caractère pornographique. Ceci signifie que pendant une bonne partie de la nuit, ces messages pornographiques ont été envoyés à une grande quantité de destinataires, estampillés du nom de notre serveur qui identifie clairement notre site institutionnel… Cela fait désordre.

En fait, j'avais par erreur désactivé l'interdiction pour sendmail de relayer les messages provenant de sites extérieurs à notre laboratoire, et des petits malins s'en sont servis pour diffuser leur message par notre intermédiaire. Le principal danger est que, suite à une opération de ce type, le site peut se retrouver inscrit sur liste noire comme diffuseur abusif de courriers électroniques (genre SPAM). Et c'est comme pour les interdits bancaires : on est très vite inscrit sur ce genre de liste, les différentes listes se mettent à jour très rapidement sur Internet, mais il est ensuite beaucoup plus difficile d'en sortir… À titre d'exemple, certains sites (américains) rejettent systématiquement tous les courriers électroniques provenant de club-internet.fr !

Uvictpirinf

(**U**ne **vict**ime du **pir**atage **inf**ormatique)

Le sniffer est un programme parasite qui écoute tout ce qui passe sur un câble réseau ; dans le cadre des protocoles standards IP, il est important de noter que toute trame circulant sur le câble peut être détectée par tout ordinateur connecté au même câble, même si l'ordinateur n'est ni émetteur ni destinataire des trames. Il suffit pour cela de configurer la carte réseau en mode PROMISC, ce qui semble relativement aisé (aïe ! je ne sais pas faire) avec quelques fonctions standards du langage C disponibles sur tout bon système Unix. Une fois l'interface basculée dans ce mode, le programme parasite voit passer tout ce qui circule sur le réseau (et en clair, en particulier pour les noms de login et mots de passe). Le sniffer « évolué » va alors faire le tri parmi la masse d'informations et ne conserver des traces que ce qui peut être exploitable par la suite. Ainsi, le sniffer installé sur notre système ne s'intéressait qu'aux trames telnet, ftp et pop pour lesquelles on s'attend naturellement à trouver une bonne quantité de mots de passe ! Inutile dès lors de faire tourner un cracker de mots de passe, qui peut en outre échouer dans le décodage de mots de passe un peu trop tordus… et pourquoi se fatiguer à cracker un mot de passe que l'on peut voir passer en clair avec un bon petit sniffer, dont on pourra trouver les sources ou un binaire (toutes architectures supportées) sur nombre de sites Internet dans le monde…

Le programme tcpdump agit suivant le même principe que le sniffer, sauf que ses intentions sont honnêtes. Mais dans un monde où les sources des programmes sont libres (linux en est un bon exemple…), qui peut empêcher monsieur X de transformer tcpdump en un sniffer à intentions malhonnêtes ?

Le sniffer est malheureusement un classique des pirates informatiques.

L'egg-drop semble être un mécanisme moins classique et moins connu dans le domaine de la lutte contre le piratage ; par contre, cela semble être un moyen redoutable et particulièrement efficace pour prendre le contrôle à distance d'un ordinateur sans laisser de traces. Ce processus parasite tourne en permanence sur le système ; le pirate a généralement le mauvais goût de donner un nom ambigu à son exécutable. Dans notre cas, c'était lpd (« mais c'est tout à fait normal », m'a-t-on assuré à mimosa.univ.fr, « notre serveur gère une imprimante et ce processus n'est autre que le démon correspondant… » ; cette réaction est exactement celle que le pirate attend de nous) ; dans d'autres cas, on pourra l'appeler httpd ; l'imagination du pirate est sans limites.

Le principe consiste alors à utiliser des canaux IRC non standards pour maintenir des connexions ouvertes en permanence avec d'autres ordinateurs sur Internet, ces autres ordinateurs pouvant être piratés de la même façon. Le démon tournant de façon continue, les requêtes de communication transitent directement par l'intermédiaire de l'egg-drop, en contournant les autres démons du système qui permettent par exemple de gérer des restrictions d'accès. Les pirates créent ainsi une sorte de réseau « subliminal » auquel participe votre ordinateur sans que l'administrateur ne s'en rende compte.

Cet outil est, paraît-il, très pratique pour transformer votre ordinateur en serveur ftp sur lequel on dépose des fichiers récupérés ultérieurement par d'autres personnes. Outre le fait que ces actes malveillants génèrent du trafic et consomment une grande partie de votre bande passante, ils contribuent également à encombrer votre disque de fichiers dont vous n'avez aucune idée de l'existence ou du contenu ; qui plus est, le pirate se chargera de « faire de la place » s'il se sent trop à l'étroit avec votre disque, et il ne détruira pas prioritairement ses propres fichiers…

On peut trouver un peu partout sur Internet des informations sur l'egg-drop, par exemple à l'adresse suivante : http://xcalibre.net/eggdrop.htm.

La sécurité sur un réseau : ça commence où, ça finit comment ?

Responsable Systèmes et Réseaux à l'IFR 550 du CNRS (Institut de Biologie Physico-Chimique), je maintiens un parc informatique constitué de 350 machines en environnement hétérogène (MacOS, MS Windows, IRIX, AIX, Digital Unix, Solaris, Linux et HPUX). Toutes les machines sont connectées sur un réseau Ethernet 10/100 Mo, et sont réparties sur 4 réseaux de classe C.

La première fois où nous nous sommes trouvés face à un problème de sécurité fut le 14 juillet 1998. À cette date, le réseau de l'Institut était complètement ouvert. Lors d'une opération de maintenance sur certaines machines, nous nous sommes aperçus qu'elles contenaient des programmes supplémentaires habilement dissimulés. Ces programmes, de type « sniffer », collectionnaient les « mots de passe » des utilisateurs, et les stockaient dans un répertoire « caché », installé par le pirate. En outre, des fichiers de configuration et des exécutables tels que rc, login, passwd, boot avaient été modifiés sur ces machines. Nous avons également

observé que le trafic dirigé vers l'extérieur avait considérablement augmenté à partir de ces ordinateurs. Ultérieurement nous avons découvert que le « hacker » s'était introduit par le service d'impression qui n'est pas protégé par défaut.
Les machines incriminées ont été déconnectées immédiatement du réseau et inspectées. Les traces d'intrusion ainsi que le contenu des disques (fichiers utilisateurs) ont été sauvegardés. Avant de les réinstaller, nous avons décidé, lors d'une réunion avec les directeurs d'unités, les utilisateurs, les agents de police du Groupe « Criminalité informatique » et les personnels de l'UREC (Unité Réseau du CNRS), de sécuriser au maximum l'ensemble de notre réseau. Cette tâche fut facilitée par la présence d'un serveur central qui gère tous les services réseau de notre domaine.
La stratégie adoptée fut, dans un premier temps, de fermer tout trafic entrant à l'exception de celui dirigé sur le serveur central. La configuration du routeur a été modifiée pour ne laisser passer que les services transitant par les ports TCP 20-21 (FTP), 23 (Telnet), 25 (Sendmail), 53 (DNS) et 80 (Web), ainsi que le port UDP 53. Par ailleurs, le trafic ICMP a été bloqué sur le routeur. Au niveau du serveur, toutes les transactions sont enregistrées par Tcp-Wapper et confrontées avec la liste noire de Thierry BESANÇON (cela répertorie les adresses IP ainsi que le nom du domaine des sites ayant déjà été impliqués dans des tentatives d'intrusion sur les réseaux. Cette liste est disponible sur http://www.lps.ens.fr/blacklistip/). Dans le cas où une machine est incluse dans cette liste, seuls les services de la messagerie et du Web lui sont ouverts. Enfin, dans certains cas particuliers, les directeurs de laboratoire peuvent demander l'ouverture d'un « canal » privilégié permettant l'accès d'une machine extérieure vers une machine intérieure autre que le serveur.

De plus, un ancien 486 a été recyclé pour surveiller le trafic entrant et sortant de notre domaine. Installé sous LINUX, il comporte deux cartes réseau. L'une, sans adresse IP, est reliée au réseau connectant l'IBPC à l'extérieur, l'autre étant reliée au réseau interne. Le logiciel IPtrafic note tous les échanges s'effectuant entre les machines intérieures et extérieures. Les traces sont relevées, analysées et finalement archivées pour une durée de deux mois. Celles qui révélent des anomalies (telles qu'un « scan » du réseau) sont transmises au CERT-Renater, à la liste mayday du CNRS et aux agents de police du Groupe « Criminalité informatique ». Il faut noter que, depuis quelques mois et à ma grande surprise, les tentatives d'intrusions se sont amplifiées.

Dans un deuxième temps, et au vu de cette augmentation, nous avons décidé de remplacer l'usage de Telnet (port 23) par SSF (port 22). Alors qu'avec Telnet le login et le mot de passe transitent en « clair » sur internet, SSF crypte la liaison entre les deux machines, rendant difficile pour un pirate d'intercepter la transaction.
Un des problèmes majeurs de la sécurité informatique provient de la course permanente existant entre les administrateurs, cherchant à protéger leur réseau et les pirates de tout genre, qui cherchent à déjouer la vigilance de ces mêmes administrateurs. Pour cette raison, on ne peut considérer que des mesures de sécurité, aussi bonnes soient-elles, permettront de garantir à jamais l'inviolabilité de nos systèmes. Une des meilleures façons, à mon avis, de se prémunir contre ces agressions consiste à toujours garder « une longueur d'avance » en suivant régulièrement les avis des organismes de sécurité (CERT par exemple) et des concepteurs de logiciels. Ceux-ci nous informent des progrès réalisés en matière de sécurité sur les logiciels susceptibles de présenter une faille pouvant être utilisée par des individus mal intentionnés. En appliquant les « mises à jour » conseillées, nous repoussons d'un pas la vulnérabilité de nos systèmes.

Il faut être conscient que les tentatives d'intrusion dans les réseaux informatiques vont aller en s'accroissant, non seulement du fait de la massification de l'Internet, mais aussi par l'ouverture de concours dont la finalité est de s'introduire dans le plus grand nombre possible de sites dans un temps donné (par exemple, le concours CRYPTERIA qui sera lancé le 1er janvier 2000 est doté d'une récompense de 10 000 dollars). Dans ce contexte, il est nécessaire non seulement de protéger son réseau, mais également d'être informé de la conduite à suivre en cas d'intrusion. Plusieurs sites sur Internet proposent des marches à suivre. Celle qui est recommandée par le CNRS est disponible sur les pages de l'UREC à l'adresse http://www.urec.fr/securite/chartes/quefaire.html.

Marc ROMERO
Responsable Systèmes et Réseaux
Marc.Romero@ibpc.fr
http://www.ibpc.fr

Le serveur thématique national du CIMM

Gérer les problèmes de sécurité

Le Centre d'Ingénierie et de Modélisation Moléculaires de Marseille, dirigé par le Dr A. Baldy, héberge le Serveur Thématique National des bases de données pour la chimie.

Ce serveur permet à 1400 utilisateurs du CNRS et des Universités de consulter à travers le réseau Internet des bases de données moléculaires, structurales et réactionnelles. Nous avons principalement trois grandes bases (Beilstein, MDL, CSD), et chaque utilisateur peut accéder suivant son abonnement à 1, 2 ou 3 de ces bases.

Tout serveur de cette envergure attire fortement les convoitises des soi-disant génies de l'informatique qui mettent tout en œuvre pour les pirater. C'est pourquoi, de notre côté, nous avons établi des concepts de sécurité qui assurent l'intégrité des systèmes, la confidentialité des informations et la disponibilité des services – sachant que le risque zéro n'existe pas – et avons pour cela prévu une solution de sauvegarde. Ce serveur, bien que très vulnérable par sa portée, doit être protégé de la même façon que n'importe quel autre serveur, mais avec une mention particulière pour la disponibilité des services et la confidentialité des informations.

Toutes les bases sont en consultation, c'est-à-dire en lecture seule, et de ce fait nous avons très peu de risques de corruption des informations. De plus, les données n'évoluant pas en temps réel, nous pouvons toujours les restaurer à partir des bandes sources, mais cela peut prendre plusieurs jours dans certains cas. La taille des bases (74 Go) nous garantit contre une récupération de copies illicites par un utilisateur indélicat. Les bases sont accessibles soit par une procédure de client/serveur, soit directement par une session à distance sur le serveur. Dans le cas de procédure client/serveur, les utilisateurs téléchargent leur « client » à partir du serveur.

Notre réseau local est un réseau Ethernet à 10 Mb/s connecté à l'Internet. La connexion à l'Internet est assurée par le centre de Calcul de Saint-Jérôme de Marseille via Renater.

Méthodes et techniques utilisées pour la sécurité

Nos idées maîtresses ont été :

- que trop de sécurité tue la sécurité et oblitère fortement le service rendu. Nous nous sommes attachés à établir des règles de sécurité garantissant le meilleur équilibre possible entre la facilité de consultation et l'application de ces règles ;
- d'assurer la confidentialité des informations en contrôlant que nos utilisateurs aient accès à toutes les bases auxquelles ils ont souscrit à l'exclusion des autres, encouragés fortement dans ce sens par les fournisseurs des bases ;
- d'assurer la disponibilité des services en mettant localement tout en œuvre pour que l'information soit toujours disponible avec d'excellents temps de réponse, la maîtrise du réseau au-delà de notre Intranet nous échappant totalement.

Les règles générales de sécurité

Chaque nouvel utilisateur signe une charte dans laquelle il s'engage à respecter les règles de sécurité que nous avons établies.

Tous les serveurs ainsi que le Pare-feu sont sur courant secouru et installés dans des pièces climatisées à accès contrôlé.

À chaque utilisateur correspond un mot de passe et non pas un mot de passe par point d'accès : ceci évite que le mot de passe soit collé sur le poste de travail et nous permet de remonter facilement vers l'utilisateur en cas de problème.

La politique des mots de passe est bâtie sur le principe de durée de validité limitée, comportant au moins 6 caractères, avec obligation de contenir des caractères spéciaux ou chiffres et sans répétition de lettres.

Sur les serveurs, les systèmes sont sauvegardés régulièrement sur plusieurs générations. Les bandes sont conservées dans une pièce spéciale différente de celle contenant les bandes source et qui n'est pas celle qui héberge les serveurs. Des scripts de surveillance de l'utilisation des serveurs et du réseau ont été écrits, pour déceler rapidement tout comportement anormal, tel qu'une forte augmentation de débit, de requêtes, de connexions, de courrier, etc. qui sont autant de symptômes de tentative de piratage.

La sécurité des accès aux serveurs

Pour cela nous avons organisé la sécurité suivant le schéma standard, c'est-à-dire en protégeant notre serveur par un « Pare-feu » et en créant une zone démilitarisée entre le routeur du Centre de Calcul et notre garde-barrière pour y installer nos serveurs « grand public ».

Conclusion

La sécurité n'est pas un vain mot et les intrusions n'arrivent pas qu'aux autres, je peux en témoigner. Cela demande une attention de tous les jours, car les pirates ne connaissent pas de relâche. En plus des règles de sécurité, il faut se doter de moyens pour se rendre compte de toute intrusion ou tentative. Il existe des quantités de logiciels permettant de surveiller les réseaux et les serveurs ; cependant leur mise en œuvre est délicate car il faut savoir à partir d'où et jusqu'où on fait remonter l'information, pour éviter de submerger de messages le responsable de la machine qui par conséquent ne pourrait plus assumer une surveillance efficace. Nous, au CIMM, allons dans un futur proche étudier quel type de logiciel de contrôle nous pouvons mettre en œuvre, car nous sommes conscients que nos mesures de sécurité, couplées à nos scripts de surveillance ne suffisent pas. De plus, toute publicité faite autour de notre serveur – et cet article en fait partie – va créer une recrudescence d'attaques, mais c'est la rançon du succès.

Pierre Vatton
Ingénieur de recherche
Pierre.Vatton@ujf-grenoble.fr

- **Le Pare-feu** (Firewall) assure le tri des informations entrantes, sortantes et en transit sur le réseau et joue le rôle de mandataire pour les accès aux bases via les sessions distantes. Le pare-feu est installé sur un PC Pentium III 530 avec 128 Mo de RAM et 9 Go de disques SCSI, tournant sous Linux et utilisant les logiciels IPchains pour le tri et Socks5 pour le mandatement.

- **Les serveurs « grand public »** assurent la gestion du Web qui donne accès aux informations relatives à la vie du serveur des bases et doit être accessible par tout le monde. Il en va de même pour les serveurs « ftp » qui délivrent les programmes clients et leur mise à jour aux utilisateurs. Deux IBM RS6000 assurent les fonctions de serveur HTTP, Mail, ftp, de liste, etc.

- **Le serveur principal** doit pouvoir permettre 1000 connexions/jour avec en pointe 50 utilisateurs simultanés. Nous avons installé pour cela un IBM H50 biprocesseur avec 768 Mo de RAM et 127 Go de disques organisés suivant l'architecture SSA pour garantir les temps de réponse lors des montées en charge.

La confidentialité des accès réseau est assurée par le logiciel TCPWrapper et le contrôle de l'accès aux bases par des scripts du fournisseur de la base.

- **Le serveur auxiliaire** sert de secours en cas de problème sur le serveur principal, et nous permet de descendre, à partir de bandes, les mises à jour des bases. Ces mises à jour portant sur 74 Go sont toujours globales et peuvent prendre plusieurs jours. Il nous sert aussi de station de test pour les mises à jour des systèmes et des applications. C'est un IBM G40 biprocesseur avec 512 Mo de RAM et 75Go de disques qui assure cette fonction.

L'INSERM, ou la sécurité réseau en réseau

L'Institut National de la Santé Et de la Recherche Médicale (INSERM) est organisé en onze régions administratives. Il représente 282 formations de recherche pour 2 165 chercheurs et 2 795 ITA. Le réseau est l'épine dorsale de cette organisation éclatée, son bon fonctionnement est donc essentiel. David Maillard (dm@hoedic.idf.insem.fr) assume la tâche cruciale de responsable de la sécurité de ce réseau.

Sécurité informatique : Pour les réseaux qui vous sont propres, quels sont les problèmes que vous rencontrez ?

David Maillard : Vous avez raison de préciser que, du fait de notre imbrication avec les structures d'autres organismes de recherche (CNRS, Université surtout), nous n'avons pas toujours la maîtrise des réseaux sur lesquels nous travaillons. Pour ceux dont nous assurons intégralement l'administration, les attaques sont très diverses, vous vous en doutez, nous tentons par l'installation systématique des correctifs systèmes, une meilleure structuration de nos réseaux et surtout une sensibilisation accrue de nos utilisateurs. Un exemple de malveillance à laquelle nous avons dû faire face : les bombardements de courriers (spam). Cette malveillance est à la fois facile à mettre en œuvre et constitue une menace importante pour le bon fonctionnement de nos communications.

SI : …Et comment avez-vous résolu ce problème ?

DM : Les sites ne sont pas tous gérés de la même manière… Certains sites n'ont qu'un administrateur à temps partiel… Bref, la situation était très différente d'un site à l'autre, qu'il s'agisse de l'architecture réseau, des applications, de la sensibilité des fichiers… et du degré de coopération des utilisateurs. Pour sortir de cet imbroglio, nous avons décidé de proposer un abonnement à un concentrateur de messagerie (mailhub) unique pour tout l'INSERM, les administrateurs ayant alors le choix de rediriger ou non leurs messages vers ce concentrateur pour qu'ils y soient filtrés. Si l'administrateur fait ce choix, il doit modifier le DNS de sa zone INSERM et rediriger les messages qui lui étaient initialement destinés vers le concentrateur. Celui-ci rejette les courriers indésirables et renvoie les autres vers le site destinataire. L'administrateur n'a plus qu'à modifier les listes d'accès (access-list) de son routeur pour que seuls les messages en provenance de ce concentrateur soient acceptés. Le concentrateur est un PC ordinaire (PIII 400Mhz, 64 Mo, 3 Go) sous Unix libre, faisant tourner l'Agent de Transport de Messages « Sendmail » configuré avec le kit du CCR de Jussieu. Le système est doublé par un concentrateur miroir, sur un site de province géré localement par Jean-François Fady, afin d'assurer la redondance en cas de panne.

SI : Les sites continuent donc à fonctionner strictement comme avant, le « spam » en moins ?

DM : Oui, c'est là l'intérêt de la solution, mais cela impose une petite difficulté : la manœuvre doit être faite simultanément sur le site et dans le DNS1. Précisons que ce service n'a pas pour objectif de fonctionner longtemps, mais plutôt de donner aux administrateurs un sursis pour leur permettre de repenser complètement la sécurité de leur site contre les bombardements de courriers mais aussi contre tout autre type d'attaques, en particulier contre les intrusions sur la machine d'administration, voire le routeur ! Finalement notre message a bien été compris puisque seuls cinq sites de l'INSERM n'utilisent pas ce service.

SI : Quelle alchimie permet de faire le tri dans les messages et de rejeter les courriers indésirables ?

DM : Quelques critères simples : la machine est-elle référencée dans le DNS ? Le nom annoncé existe-t-il ? Cette machine figure-t-elle dans une « liste noire » répertoriant les adresses douteuses ? Enfin, ce message est-il destiné à un utilisateur réel du sous-domaine INSERM annoncé ?

SI : Cela induit-il un délai supplémentaire dans l'acheminement des messages ?

DM : Le délai supplémentaire est, en général, de moins d'une seconde. Cependant la charge du réseau reste à évaluer car le trafic arrive et repart (purgé des courriers indésirables) sur le même accès Renater du concentrateur. Pour les sites actuellement abonnés, en 9 mois il y a eu 500 000 messages rejetés sur 1,9 millions traités. Ce qui donne un total (avec les documents attachés) de 90 Go de données. On en déduit la charge du réseau et on voit qu'elle reste relativement faible.

SI : Dans cette expérience, vous démontrez que la sécurité n'entrave pas toujours la liberté des chercheurs !

DM : Effectivement, ainsi le concentrateur dit « anti-spam » ne gène personne, il est transparent à l'utilisateur et contribue à la disponibilité des réseaux ! Le principe de cette architecture pourrait être étendu à d'autres fonctions comme la détection des virus dans les pièces attachées, les caches WWW et ftp… Malgré le caractère centralisateur de cette mesure, la politique réseau de l'INSERM repose sur les Administrateurs Réseau de Site et les Responsables Régionaux de l'Informatique qui, seuls, apprécient l'adéquation des contraintes et des apports d'une telle solution.

■

1. Domain Name Server : c'est le serveur de nom qui permet de transformer une adresse de type IP (des groupes de chiffres) en une adresse « littérale » plus significative.