

La sécurité informatique à l'IN2P3

(«logs») des routeurs d'interconnexion entre les laboratoires et l'extérieur. Ces logs sont prélevés avec une périodicité de vingt minutes, et centralisés pour archivage. L'archivage est fait à la fois sur cartouches magnétiques (pour le long terme), et sur cédérom (pour faciliter l'analyse en ligne). Ces logs sont extrêmement riches d'informations, par exemple pour déterminer le volume de données échangées lors d'une intrusion, pour y détecter la présence (l'adresse) de machines suspectes, pour détecter le piratage de machines par rebonds. Un projet est actuellement en cours pour compléter ces logs par d'autres prélèvements, plus complets, effectués par une machine connectée en «sniffer» juste derrière les routeurs afin de journaliser l'activité entrante et sortante avec plus de précision (informations sur les protocoles utilisés, les sessions, etc.).

La gestion de la sécurité informatique nécessite du temps et des personnes pour faire le travail : il

n'y a pas plethore d'informaticiens à l'IN2P3, mais nous avons cependant la chance d'être moins démunis que beaucoup d'unités du CNRS. Sans doute est-ce là une des raisons qui font que l'IN2P3 n'est pas trop mal loti en traitement de la sécurité informatique, qu'il a réussi à acquérir une certaine expérience (malheureusement par la pratique et la force des choses), et obtenu quelques succès. Il n'est pas possible de gérer correctement la sécurité informatique sans prise de conscience et motivation de la hiérarchie et des informaticiens eux-mêmes : la Direction et les informaticiens de l'IN2P3 ne font pas défaut sur ce point. Il reste cependant un gros travail à effectuer pour sensibiliser les utilisateurs.

Bernard Perrot
Chargé de mission
pour la sécurité informatique à l'IN2P3
perrot@la.l.in2p3.fr

Routeurs ou «gardes-barrières» ?

Seul un «coupe feu» permet de filtrer le trafic réseau ? NON ! Hervé Schauer (Herve.Schauer@hsc.fr) remet une fois encore les points sur les «i» : «La majorité des routeurs du marché savent analyser les trames au niveau applicatif (NSC, 3COM, CISCO, etc.). Ils savent même avec des options faire du filtrage de session (*stateful inspection*) qui fait plus de contrôle dans la continuité de la session que des produits dits «firewall»... Donc, s'il n'y a pas besoin d'authentification et d'analyse de contenu de type recherche d'anti-virus, par exemple, un routeur filtrant fait désormais aussi bien - si ce n'est pas mieux - qu'un produit appelé «firewall» par du marketing.» ■

R. L.

..... suite de la page 1

bâtiment 123 sont fermées depuis le début de la semaine (pour cause de vacances), et qu'il lui a été dit d'aller à la salle restée ouverte du bâtiment 250. Je lui réponds qu'il s'est trompé, le bâtiment 250 est celui de l'autre côté de la rue, il est ici au 240. Je le prie donc de ne pas rester ici. Comme il s'apprête à fermer les fenêtres ouvertes sur le terminal, je l'en empêche, un doute soudain... Comme il prend mal la chose, je lui demande alors de me montrer sa carte d'étudiant, qu'il n'a pas. Il me présente un récépissé de perte de papier d'identité, que je photocopie et le prie de quitter enfin les locaux. Je reviens sur le terminal, trouve des sessions ouvertes vers une école parisienne et une activité manifestement inamicale dévoilée par les historiques : je comprends que je viens de laisser partir l'auteur du piratage du compte de Patricio.

Un outil va se révéler une fois de plus très utile : à l'IN2P3, nous prélevons les fichiers journaux (les «logs») de nos routeurs avec une périodicité de 30 minutes, et ils sont tous archivés sur une machine de service pour le court terme, et sur bande et cédérom pour le long terme. Ces logs contiennent les paires d'adresses IP des machines communicantes durant la période de temps, ainsi que le volume de paquets et octets échangés. Une analyse de ces logs permet de connaître les adresses des machines avec qui des connexions ont été établies depuis le termi-

nal utilisé par notre visiteur dans la nuit. Ensuite, je recherche s'il y a eu une activité avec les machines découvertes les jours précédents : il apparaît effectivement qu'une activité similaire à celle de la nuit avait lieu depuis déjà quatre jours, et depuis plusieurs terminaux X du laboratoire. Il apparaîtra que l'intrus se faisait enfermer dans les locaux le soir, cherchait des terminaux avec des sessions non fermées (fenêtres «telnet» sur des terminaux X), et les récupérait pour pirater les machines sur lesquelles les sessions étaient ouvertes ! Pas besoin de connaître les mots de passe, les sessions étaient déjà ouvertes... grave «négligence» de la part des utilisateurs de ces terminaux. Il est possible de constater que l'intrus «possède» des accès sur de nombreuses machines, dont une récurrente, très au nord du continent européen.

Contact est pris avec les autorités de police spécialisées : il apparaît alors que l'individu est déjà «connu» (les papiers qu'il m'a présentés étaient authentiques, il ne manquait pas d'assurance ni d'audace !). Une plainte est déposée.

Craignant un retour du pirate, je contrôle les semaines suivantes les logs des routeurs pour y détecter une éventuelle activité similaire à la sienne (il se connectait beaucoup sur des serveurs Web pomographiques, des serveurs IRC, et certaines machines récurrentes) : nulle trace. Affaire bouclée.

Il sera interpellé quelques mois plus tard. Où l'on découvrira alors qu'il est revenu dans nos locaux régulièrement pendant plus de trois semaines après le dépôt de plainte sans être remarqué : la nuit, il passait par les toits ou le week-end par la fenêtre pour entrer dans le bureau fermé d'un collaborateur en congé. Qu'il avait déjà «visité» ce bureau lors de sa première incursion, et avait alors (toujours en récupérant des sessions non fermées sur un terminal) obtenu l'accès sur des ordinateurs d'un grand centre de recherche avec lequel l'occupant habituel du bureau avait un contrat. Que cette nouvelle série de visites était exclusivement ciblée sur le piratage discret de ce centre à l'exclusion de toute autre connexion (ce qui explique que je n'ai pas pu détecter son activité dans le trafic réseau). Qu'au retour de congé du locataire du bureau, il a continué plusieurs semaines à pirater ce centre de recherche depuis d'autres sites franciliens (universitaires, écoles). Que sa première visite était prospective. Qu'il était manipulé. Que la machine sur laquelle il se connectait, celle très au nord, il ne l'avait pas piratée, celle-là... c'était celle de ses commanditaires, qui lui avaient passé une commande (pénétrer des ordinateurs du centre de recherche en question). Qu'il était en fait très bien renseigné. Que ça n'arrive pas qu'aux autres, ni que dans les romans...

Bernard Perrot