est cinglante : «Espèce de marin d'eau douce ! Pensais-tu vraiment trouver un passage secret ?» Puis le programme associé au canal transmet des données incohérentes et envoie un courrier électronique au système administrateur du fournisseur d'accès dénonçant la tentative de piratage. Quelques minutes plus tard, la connexion de Nau est supprimée.

Mieux vaut contourner le pare-feu sur la pointe des pieds plutôt que de le passer en force. D'un autre compte, également piraté, Nau tente, par une simple commande saisie sur le clavier, de dresser la liste des ordinateurs du réseau boucanier.fr.

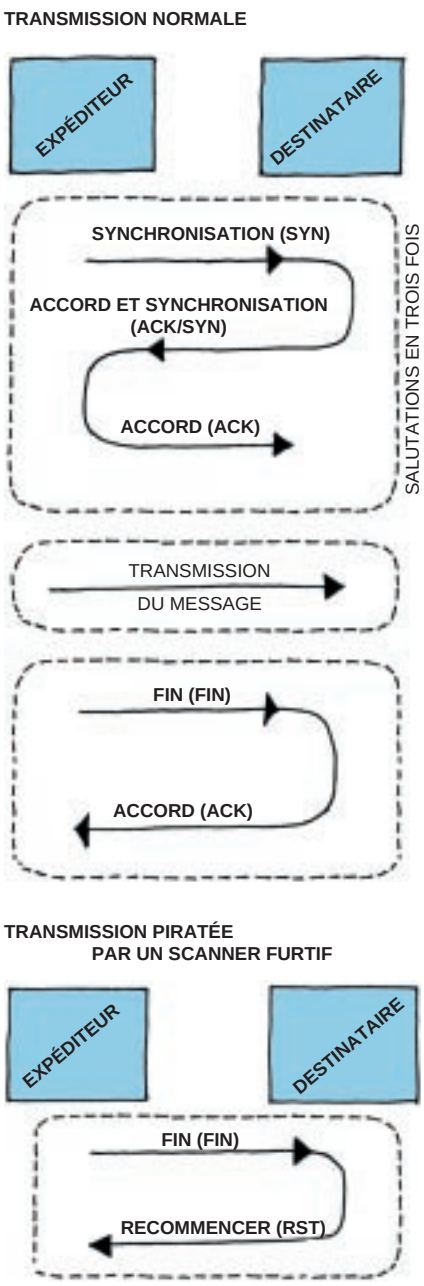
La commande ne fournit aucun résultat utilisable : Surcouf a probablement configuré le réseau de sorte que les données adressées à n'importe quel ordinateur transitent d'abord par un programme central, qui les redistribue ensuite. Cette méthode empêche les intrus d'accéder à l'intérieur du pare-feu.

Après avoir converti l'adresse informatique boucanier.fr en un nombre, Nau utilise un scanner d'adresses informatiques, puis il teste les 50 adresses numériques immédiatement inférieures et supérieures. Peut-être appartiennent-elles à des ordinateurs du réseau boucanier.fr, car les adresses numériques des ordinateurs d'un réseau sont souvent proches ? Hélas, non.

Avec une autre commande, il découvre alors un second réseau appartenant à la Société *Boucaniers* : boucanum.fr, dont l'adresse numérique est éloignée de celle de boucanier.fr. Le scanner d'adresses découvre alors cinq ordinateurs dont l'adresse est numériquement proche de celle du réseau boucanum.fr.

Par précaution, Nau se connecte de son compte piraté à un autre compte piraté et, de là, vers un autre compte, d'où il exécute d'autres scanners de ports furtifs. Ces étapes supplémentaires engorgeront toute procédure judiciaire, puisque celle-ci nécessiterait trois mandats de perquisition. Échaudé, il utilise également un programme nommé *Root kit*, grâce auquel il effacera toute trace de son activité dans les comptes rendus utilisés pour détecter les activités douteuses et les modifications des fichiers de configuration de cet ordinateur.

De son galion, Nau examine les ordinateurs de boucanier.fr et de boucanum.fr connectés au réseau Internet. Le scanner de ports furtif se glisse au



2. LES TRANSMISSIONS DE MESSAGES obéissent à un protocole rigide. L'expéditeur envoie un signal de synchronisation (SYN) des communications à venir *(en haut)*. Le destinataire retourne alors un double signal (ACK/SYN) d'accord et de synchronisation pour accepter la demande. Enfin, l'expéditeur envoie à son tour un signal d'accord (ACK). Le message lui-même est alors transmis. Un signal de fin (FIN) le suit de peu. Le destinataire répond par un autre signal d'accord qui clôt définitivement la correspondance. Un pirate corrompt cet échange *(en bas)* en envoyant immédiatement un signal FIN auquel le destinataire est obligé de répondre par un signal pour recommencer (RST). La réponse – ou l'absence de réponse – fournit des informations sur le destinataire. Cependant, l'absence des triples salutations empêche la transmission d'être enregistrée dans les comptes rendus du destinataire. Le pirate sonde ainsi un ordinataire avec une certaine discrétion.

travers du pare-feu vers chacun d'eux. Cependant la manœuvre a été détectée par le programme *Etherpeek*, qui prévient à nouveau Surcouf.

Celui-ci déboule dans son bureau ; il identifie rapidement l'origine du scanner et alerte l'administratrice du système du troisième compte de Nau. Cependant, le programme *Root kit* dissimule Nau, qui continue avec impudence, grâce au scanner furtif et au logiciel *Strobe*, de chercher une adresse informatique non protégée par le pare-feu. Celui-ci ne fait que lui transmettre un flot de données incohérentes.

Cet afflux soudain convainc l'administratrice du compte de Nau qu'un agresseur est à l'œuvre. Elle déconnecte alors tout le système du réseau : la connexion de Nau s'arrête dans un sifflement.

À la recherche d'horaires décalés

Nau suppose alors que de nombreuses stations de travail non connectées au réseau boucanier.fr sont utilisées par des employés de la Société *Boucaniers* pour travailler chez eux. Ces ordinateurs, reliés directement, ne sont pas protégés par le pare-feu. La probabilité est grande : avec un modem, n'importe qui peut relier un ordinateur personnel à une ligne téléphonique.

Grâce à un logiciel de numérotation téléphonique automatique nommé *Shokdial*, Nau appelle chacune des lignes téléphoniques de la Société *Boucaniers*. Au siège de la société, les gardiens de nuit entendront sonner successivement les postes sans comprendre de quoi il retourne.

À 2 heures 57, un modem répond au programme *Shokdial* : Nau est alors face à une station de travail de la marque *Silicon Graphics* : «Boucaniers SA. Département mercatique. Irix 6.3» (*Irix* est une forme d'*Unix*). Nau a enfin trouvé une porte d'accès au fief de Surcouf.

Assez d'élégance ; Nau décide d'utiliser la force. Il exécute un programme qui se connecte autant de fois que nécessaire pour découvrir le mot de passe d'un compte administrateur, c'est-à-dire un accès sans restrictions dans ses possibilités d'action, duquel il pourra agir en toute liberté. Le possesseur de cet ordinateur *Irix* aura peut-être autorisé la connexion à distance sur le compte administrateur.

La recherche de mot de passe commence avec les mots et les noms courants,

puis le programme teste des groupes de signes moins naturels ; l'exploration peut durer des mois, voire des années. Cependant Nau est chanceux. Vers 5 heures, le prénom «Nancy» est identifié : le compte administrateur est accessible!

Nau est ravi. Il crée une fenêtre de dialogue entre lui et le système d'exploitation de l'ordinateur, d'où il dispose des mêmes pouvoirs que l'administrateur. Puis il renforce sa position en transférant un programme *Root kit* pour la discrétion et un programme *Sniffer* sur l'ordinateur de sa nouvelle victime : toute saisie et toute connexion seront enregistrées par le programme *Sniffer* dans un fichier dissimulé. Le programme *Root kit* permet également de créer un chemin d'accès supplémentaire que Nau baptise «revanche» ; mot de passe «MoRtSurCf».

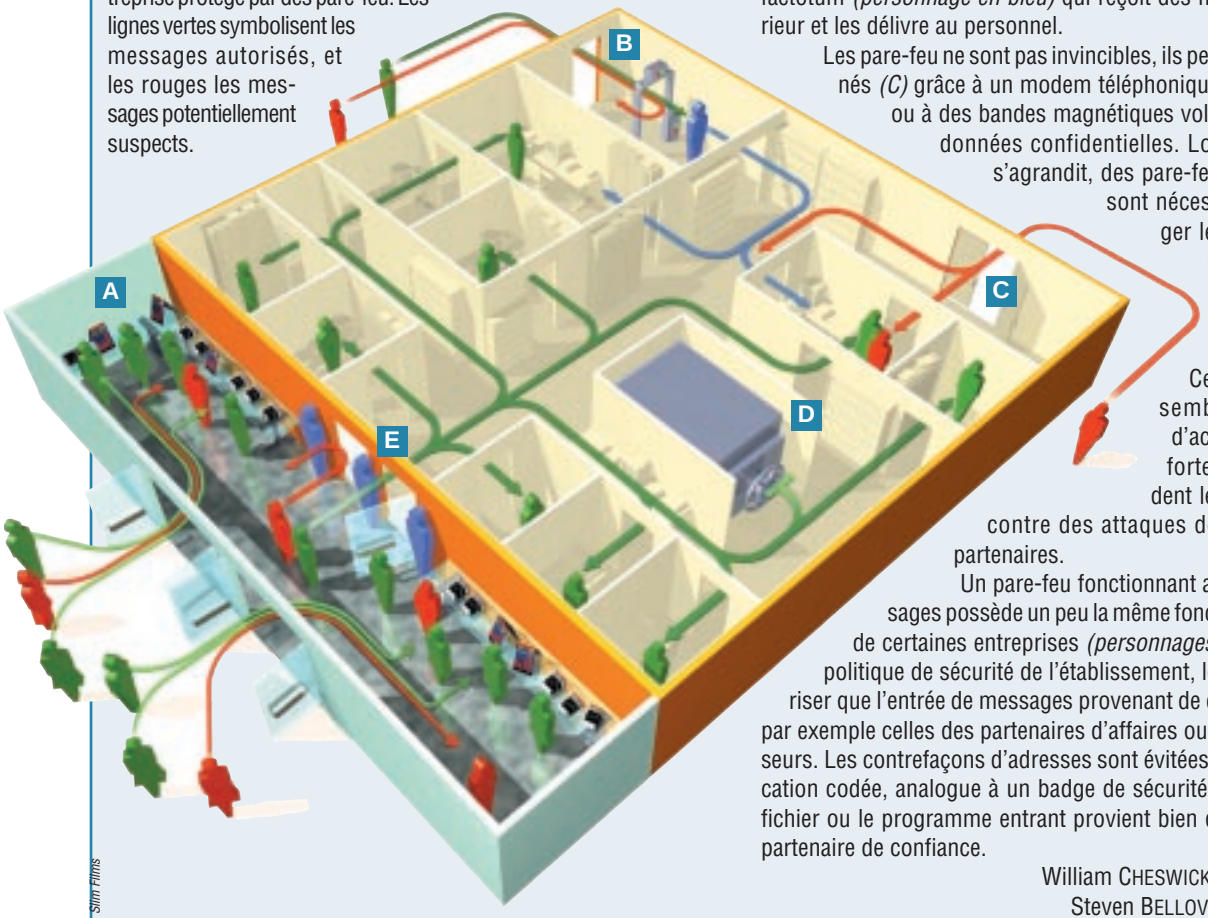
Nau termine sa nuit en déterminant que le compte administrateur auquel il a accédé est connecté sur l'ordinateur picasso du réseau boucanum.fr. Grâce au programme *Root kit*, l'utilisateur normal de l'ordinateur picasso ne remarquera pas que son ordinateur est maintenant commandé par quelqu'un d'autre. Surcouf ne détecte qu'une tentative d'intrusion dans boucanum.fr à partir du réseau Internet. Ce nouvel incident l'inquiète, mais, faute d'informations suffisantes, il ne peut rien faire.

Deux nuits plus tard, Nau se connecte sur l'ordinateur picasso et examine les comptes rendus du programme *Sniffer*. Toutes les informations concernant le trafic interne du réseau sont codées, mais le programme *Sniffer* a enregistré la connexion de quelqu'un, de l'ordinateur picasso sur un autre ordinateur du nom de fantasia.

Les pare-feu

Aucun réseau informatique relié au réseau Internet n'est invulnérable, mais des protections peuvent être installées. La première ligne de défense est le pare-feu, dont les deux types le plus fréquemment utilisés agissent soit au niveau des messages transmis, soit au niveau des logiciels. Le premier fonctionne sur une machine nommée routeur. Il examine dans chaque message entrant ou sortant les adresses de la source et de la destination, qu'il compare à des règles d'accès. Les messages autorisés sont transmis, les autres sont bloqués. Le second examine les adresses et le contenu des messages. Plus lent qu'un filtre de messages, il permet toutefois une politique de sécurité plus raffinée.

L'illustration représente un réseau informatique d'entreprise protégé par des pare-feu. Les lignes vertes symbolisent les messages autorisés, et les rouges les messages potentiellement suspects.



Slim Films

À l'extérieur du pare-feu *(en orange)*, l'entreprise possède un réseau accessible au public, qui permet aux clients d'envoyer des courriers électroniques vers l'entreprise ou de naviguer sur ses différents sites informatiques. Cette zone *(A)* est analogue à l'espace d'accueil réservé au public que l'on trouve à l'entrée de certains établissements : aucune information confidentielle n'y est présente.

Un pare-feu fonctionnant au niveau des logiciels ressemble aux salles de police des aéroports *(B)* : les courriers électroniques sont inspectés. Les programmes reçus par le réseau Internet, qui peuvent contenir des instructions néfastes, sont envoyés sur un serveur mandataire, puis à un programme mandataire qui fonctionne en toute sécurité sur le réseau. Un programme mandataire est l'analogue du factotum *(personnage en bleu)* qui reçoit des messages de l'extérieur et les délivre au personnel.

Les pare-feu ne sont pas invincibles, ils peuvent être contournés *(C)* grâce à un modem téléphonique, à des disquettes ou à des bandes magnétiques volées, contenant des données confidentielles. Lorsque l'entreprise s'agrandit, des pare-feu supplémentaires sont nécessaires pour protéger les systèmes informatiques de services importants, tel celui de la comptabilité. Ces protections ressemblent à la porte d'acier d'une chambre forte *(D)* ; elles défendent les systèmes vitaux contre des attaques de l'intérieur ou de partenaires.

Un pare-feu fonctionnant au niveau des messages possède un peu la même fonction que les gardes de certaines entreprises *(personnages en bleu)*. Selon la politique de sécurité de l'établissement, le filtre peut n'autoriser que l'entrée de messages provenant de certaines adresses, par exemple celles des partenaires d'affaires ou celles des fournisseurs. Les contrefaçons d'adresses sont évitées par une authentification codée, analogue à un badge de sécurité, qui assure que le fichier ou le programme entrant provient bien d'une adresse d'un partenaire de confiance.

William CHESWICK, Laboratoires *Bell*
Steven BELLOVIN, *AT&T Research*