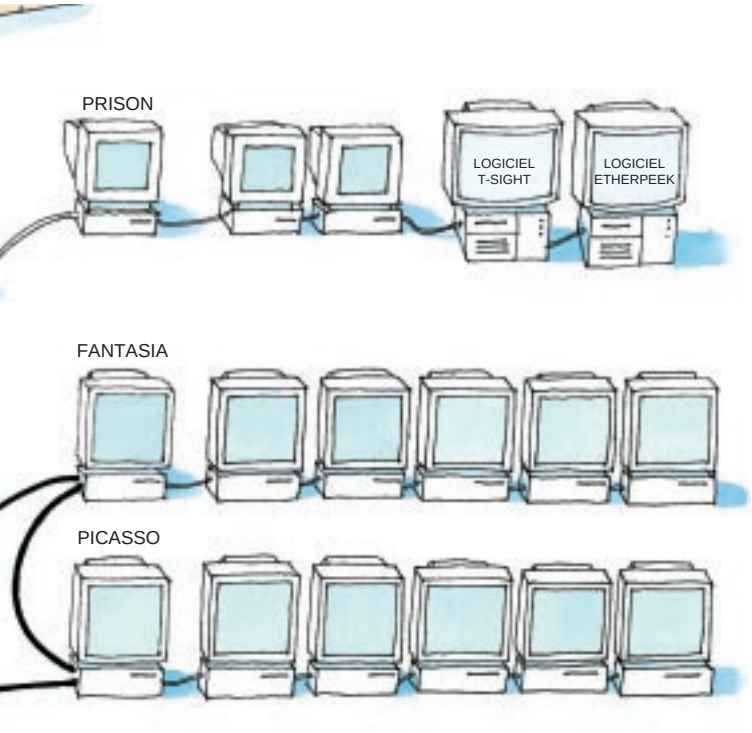
Malgré la rapidité des représailles, Nau n'est pas neutralisé : ce n'est que l'un de ses nombreux comptes piratés qui est clôturé. La fermeture de ce compte l'élimine de la causette, où il apparaît comme un cuistre ou un lâche. Il est temps d'utiliser une autre arme : un scanner de ports furtif.

Ce programme est plus subtil que *Strobe*, car il manipule les informations échangées lors des communications entre les ordinateurs. Lorsqu'un ordinateur souhaite transmettre un message, il envoie tout d'abord un signal nommé SYN, destiné à la synchronisation des deux ordinateurs. Le programme qui le reçoit répond par un double signal (un d'accord, ACK, et un de synchronisation, SYN), et par une valeur de temporisation qui sera utilisée pour régler la transmission des données *(voir la figure 4)* et, en outre, ralentir le temps de réaction de l'ordinateur émetteur. Ce dernier envoie enfin un signal d'accord, ACK ; puis les salutations achevées, il transmet son message, qui se termine par un signal FIN. Le destinataire retourne alors un signal d'accord, pour indiquer qu'il a bien reçu le message.

Un scanner de ports furtif ne respecte pas ce protocole *(voir la figure 2)* : il envoie un signal FIN prématuré à plusieurs canaux de connexion de l'ordinateur récepteur. De ce fait, le programme récepteur n'envoie aucune réponse, mais il transmet sur chaque canal un signal RST pour demander de recommencer la procédure. Ce signal RST, contrairement aux signaux ACK et SYN est caractéristique de l'ordinateur qui l'envoie : il fournit des informations importantes au pirate, telles le type d'ordinateur et les démons en service. Cependant, sans les triples salutations, il n'identifie aucune connexion et n'enregistre pas la transmission dans ses comptes rendus d'opérations. Le scanner de port furtif sonde un ordinateur en toute discrétion.



1. MALGRÉ LES PUISSANTS LOGICIELS DE DÉFENSE, par exemple les pare-feu qui stoppent les intrus non autorisés, les systèmes informatiques connectés au réseau Internet ont presque toujours plusieurs points faibles que les pirates exploitent.

Sur un site du réseau Internet, Nau trouve un scanner de port furtif performant écrit en langage C. Nau doit le compiler, c'est-à-dire le traduire dans le langage de son ordinateur. Cependant, chaque version d'*Unix* est unique, et Nau n'a jamais étudié la programmation. Il n'en a jamais eu besoin, car tous les logiciels qu'un pirate désire sont en libre-service gratuit sur le réseau Internet. Reste à savoir les traduire.

Le jeune Surcouf a suivi un parcours différent. Un ami technicien lui a appris comment gérer un système informatique. Puis il s'est perfectionné en affrontant son ami dans des jeux d'attaque et de défense de systèmes informatiques. Ils ont ensuite aidé le fournisseur d'accès Internet à renforcer sa propre sécurité. Surcouf a alors été embauché à temps partiel, en parallèle avec des études d'informatique.

Nau le pirate a donc commis sa première erreur : attaquer Surcouf, corsaire confirmé.

Le repérage des lieux

Au petit matin, Nau a traduit le programme. En quelques minutes, le scanner de ports furtifs lui fournit la liste des services proposés par boucanier.fr à des personnes dûment répertoriées. Un programme assurant la sécurité de l'interpréteur des commandes – pour qu'elles soient exécutables – grâce à des connexions codées et un serveur de site Internet retiennent son attention. Le cœur de Nau s'accélère. Un canal de connexion s'est entrouvert au moment de son examen. Un autre intrus l'a-t-il précédé? A-t-il maintenu une porte dérobée pour pénétrer dans le système?

La sonnerie d'un messager de poche réveille Surcouf. Un programme de détection nommé *Etherpeek*, installé sur le réseau d'ordinateurs boucanier.fr, a décelé l'examen des canaux de connexion par Nau. Surcouf se précipite au bureau et, assis devant sa station de travail (un ordinateur performant), il fait le guet. Installés uniquement sur son propre ordinateur, ses meilleurs programmes de défense ne fonctionnent que lorsqu'il est aux commandes, afin d'éviter tout assaut de l'extérieur. Cependant, Surcouf n'observe aucune manœuvre : malgré la tentation, Nau, guidé par son intuition de pirate, a abandonné l'assaut.

Tout de même intrigué, Surcouf analyse les comptes rendus d'opérations de son ordinateur et retrouve l'adresse du message pirate. Par courrier électronique, il informe le fournisseur d'accès de Nau de la tentative d'effraction et lui demande des informations sur le compte du pirate. La clause de confidentialité des clients empêche la requête d'aboutir.

Toutefois, trois soirs plus tard, Nau découvre que son mot de passe n'est plus valable : son fournisseur d'accès lui apprend que son compte a été supprimé parce qu'il a utilisé un scanner de ports furtif.

Plus déterminé que jamais, Nau revient quelques minutes plus tard sur le réseau Internet grâce à un téléphone et à une carte bancaire. Il doit être prudent. De ce nouveau compte, il se connecte sur un de ses comptes piratés chez un autre fournisseur d'accès, et il apprend que le site informatique boucanier.fr appartient à la Société *Boucaniers*, qui produit de la viande fumée.

Nau tente alors de se connecter au réseau boucanier.fr par le canal inhabituel repéré trois nuits plus tôt. La réponse

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.

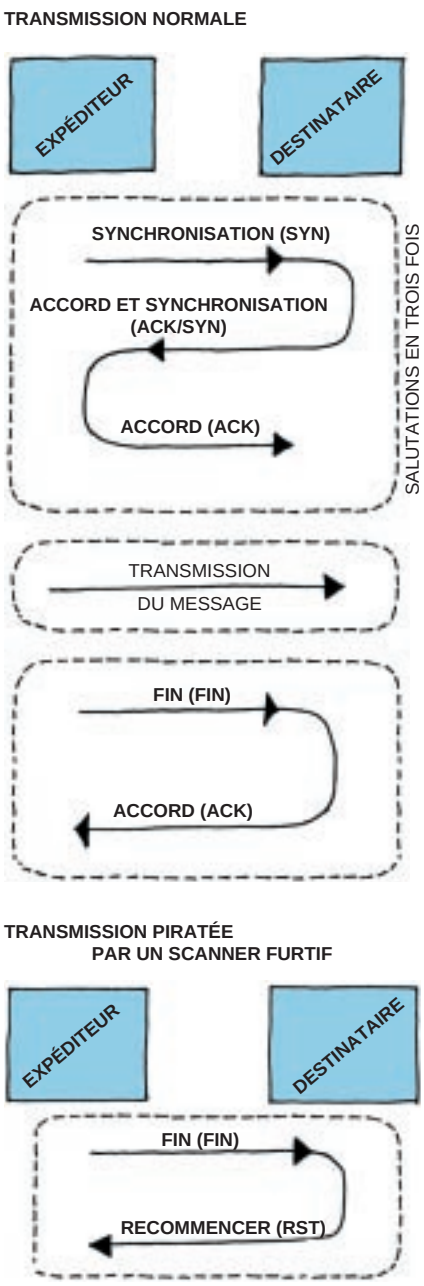
Avec une autre commande, il découvre alors un second réseau appartenant à la Société *Boucaniers* : boucanum.fr, dont l'adresse numérique est éloignée de celle de boucanier.fr. Le scanner d'adresses découvre alors cinq ordinateurs dont l'adresse est numériquement proche de celle du réseau boucanum.fr.

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 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.



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.

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,