Magiciens des câbles

Une aide de jeu pour jeux contemporains par Mario Heimburger

Que ce soit dans les films ou dans les reportages télévisés, on nous montre fréquemment des petits génies du piratage qui rentrent dans un système en quelques minutes, et récupèrent toutes les données qu'ils souhaitent… Évidemment, les joueurs tentent de faire de même, souvent face à un meneur qui ne sait pas trop comment réagir…
Cette aide de jeu fait un petit tour d'horizon du piratage informatique, des techniques majeures et des idées reçues, sans rentrer heureusement dans des détails techniques trop pénibles. Certains points sont volontairement simplifiés pour constituer la base des connaissances pour tout joueur ou meneur souhaitant mettre en scène un adversaire « informatisé ».

OBJECTIFS

Attaquons-nous d'abord à la définition des objectifs d'un pirate. Ceux-ci peuvent être de plusieurs types aussi bien pour la cible de l'attaque que l'utilisation que le pirate souhaite faire de sa cible. Les techniques d'attaques varieront fortement en fonction de ces objectifs.

♦ Cible

On pourrait classer les cibles en deux catégories quant à l'importance dans le processus de piratage.

D'un côté, il y a les **cibles indéterminées**. Entendez par-là qu'il faut trouver une cible pour effectuer une action depuis quasiment n'importe quel système informatique.
Le pirate va partir à la « pêche » pour trouver un hôte adéquat. Il commencera par chercher une faille de vulnérabilité connue, listée sur des sites spécialisés dans la sécurité informatique, qu'il pourra exploiter. De préférence, cette faille doit être assez récente, et sur un système très répandu.
Une fois la faille connue, le pirate scanne le réseau à la recherche des *fingerprints* du système concerné, un faisceau d'indices qui permettent d'identifier le système utilisé sur la cible potentielle. Quand il trouve une machine adéquate, le pirate peut exploiter la faille de vulnérabilité pour agir sur le système.
Précisons que le pirate déterminé arrive presque toujours à ses fins : il finira toujours par trouver une machine correspondant à ses besoins quelque part dans le monde. Le seul risque serait que ses recherches soient repérées par le prestataire de service à partir duquel il opère, mais ce risque est faible.

Le second cas de figure est déjà beaucoup plus complexe : on admet que le pirate vise une **cible particulière**. C'est aussi le cas le plus fréquent dans un jeu de rôle. Bien sûr, cela signifie que le pirate a préalablement localisé et identifié sa cible, ce qui n'est déjà pas une mince affaire.

Ce que cette aide de jeu n'est pas

Un guide complet du piratage : il s'agit juste de quelques pistes et méthodes employées.

Un exposé technique : il n'a pas sa place dans un webzine consacré aux jeux de rôles. Cet article reste donc volontairement dans le vague concernant l'application des méthodes.

Un exposé de techniques high-tech : il existe des moyens fous pour intercepter des données, décrypter des appels téléphoniques, casser des codes cryptés avec des clés « inviolables » et lire l'affichage des écrans à travers les murs… Mais ces moyens sont réservés à des gens très riches ou très officiels. Cet article traite de ce qu'on peut faire avec un bon ordinateur et une bonne dose d'intelligence.

Une incitation au piratage : en tant qu'administrateur système, l'auteur ne peut que condamner le piratage qui amène des conséquences économiques néfastes (et tout ce qui s'en suit en terme d'emploi et de progrès) et une méfiance peu justifiée de la part des usagers moyens.

Il faut bien sûr que la cible soit accessible (autrement dit qu'elle est reliée au pirate par une succession de câbles et d'équipements intermédiaires), sinon la tentative est automatiquement vouée à l'échec. Dans un contexte où toute l'informatique est reliée au réseau, cette condition n'est pas trop complexe à remplir.
Une action déterminée est beaucoup plus complexe que l'attaque « au hasard » et a peu de chances d'aboutir.

♦ Action

Là encore, en fonction de la cible, le pirate pourra effectuer plusieurs types d'actions, plus ou moins complexes.

Les **opérations de relais** sont destinées à couvrir le pirate pour d'autres types d'actions. En gros, il s'agit de prendre le contrôle d'une machine pour cacher la véritable source du piratage ou pour garantir l'anonymat du pirate. Trouver des relais est assez facile, puisqu'on s'attaque à des cibles indéterminées. Le pirate préfèrera toutefois les systèmes sur lesquels il obtient un contrôle total afin d'avoir la plus grande liberté d'action. Il est possible d'utiliser plusieurs relais, mais la complexité de l'attaque augmente…
Par une opération de relais, un utilisateur peut aussi propager des informations erronées, virus ou messages en brouillant les pistes.

Les **dénis de services** sont des attaques frontales destinées à empêcher un système de fonctionner normalement. On se contente en général de bombarder la cible d'informations ou de demandes qui vont l'amener à planter ou à interrompre le service. Ce type d'attaque nuisible peut être pratiqué pour nuire à une entreprise en particulier, par exemple en empêchant un site de vente de fonctionner. Il peut aussi s'agir d'une diversion pour une attaque plus discrète. Dans tous les cas, la source est facile à identifier, et la plupart du temps, des défenses efficaces sont mises en place. Certains dénis de services peuvent toutefois rendre un système vulnérable. On parle également d'attaques incapacitantes.

Les **attaques destructives** sont beaucoup plus graves, puisque non contentes d'interrompre un service, elles le rendent de plus défectueux. Il s'agit de rentrer dans un système et de causer des dégâts irréparables. Évidemment, dans le monde virtuel, l'irréparable se chiffre en heures, le temps que le système soit réinitialisé ou restauré depuis une sauvegarde. Néanmoins, les dégâts provoqués peuvent être très importants et amener un coût assez élevé.

Enfin, l'attaque la plus fréquente dans les scénarios est la recherche de **données** (ou la modification de ces données). Dans ce type d'attaque, le plus dur est de trouver les données.
Y accéder représente également un défi non négligeable, et l'on peut facilement passer à côté de ce qu'on cherche. Il s'agit vraisemblablement de l'attaque la plus difficile.

Il existe toutefois quelque chose de plus complexe : **exécuter un code malveillant** sur la cible. Il faut en effet non seulement accéder à la machine (et donc connaître ses faiblesses), mais également disposer de hauts privilèges qui permettent d'exécuter ce que l'on souhaite en toute discrétion.

CONNAITRE SA VICTIME

Une fois l'objectif déterminé, il convient d'en apprendre le maximum sur la cible et plus particulièrement son système informatique, mais également – et c'est parfois important – sur son organisation interne. Plusieurs techniques existent pour cela.

♦ Les portes d'entrées

La première chose à faire lorsqu'on souhaite attaquer un système particulier est de connaître les portes d'entrées qui vont déjà limiter les actions possibles ou les techniques applicables.
Par porte d'entrée on entend deux choses : d'une part les équipements qui se trouvent en entrée du réseau à attaquer (que ce soit un simple équipement de routage ou un système de défense évolué comme un *firewall*), d'autre part les interfaces réseaux en écoute. Sans rentrer dans les détails, lorsqu'une machine est connectée à un réseau, elle utilise pour communiquer différents protocoles (ou langages), qui peuvent donc être utilisés ou non. Sur ces protocoles cohabitent plusieurs services ou « ports d'écoutes » qui peuvent être exploités pour certaines attaques.

Pour connaître les portes d'entrées, il s'agit de faire une reconnaissance aussi discrète que possible. Ce qui engage le moins (mais est le plus difficile) est de se renseigner sur place. Évidemment, il faut ruser pour soutirer des informations sans éveiller les soupçons, mais c'est encore ce qui marche le mieux (soyons franc, la vantardise des experts en sécurité est parfois un précieux allié).
Dans la plupart des cas, toutefois, on se contentera d'utiliser des outils disponibles pour tous sur Internet, et qui permettent d'effectuer différents *scans* du réseau. Il existe des outils pour déterminer le nombre d'équipements entre le pirate et sa cible (et donc les failles potentielles), d'autres pour déterminer les protocoles utilisés et d'autres plus complexes pour renseigner sur les limites mises en place et les sécurités actives.

Attention : il existe aussi fréquemment des voies d'accès cachées, secondaires ou de secours. Il arrive souvent que ces voies soient moins protégées car plus secrètes, mais les découvrir est alors plus dur…

♦ Les systèmes

Autre point essentiel : la connaissance du système informatique à attaquer. Un pirate n'a aucune chance de rentrer dans un système inconnu de lui.
La première étape consiste à l'identifier. Pour cela, on a recours aux *fingerprints* déjà évoqués plus haut. En effectuant une succession de tests, le pirate va éliminer les systèmes au fur et à mesure jusqu'à déterminer avec la plus grande probabilité le système cible.
Un exemple : la cible héberge un serveur internet. En surfant sur le site, vous constatez que les pages ont l'extension aspx. Vous pouvez en déduire que le serveur internet est un serveur Microsoft, et donc, que le système sous-jacent est une version de Windows. Reste à savoir laquelle, mais d'autres indices permettent de le repérer… sauf si les administrateurs ont été plus malins et pour brouiller les pistes ont appelé leurs pages aspx (il y a toujours plus malin que soit).

Une fois le système reconnu, il faut l'étudier. Plus la peine de s'intéresser à la cible pour le moment : direction les milliers de sites webs parlant de ce système. Si le pirate le connaît bien, cela peut aller vite. Dans le cas contraire, il lui faudra ingérer des tonnes de connaissances sur le fonctionnement de ce système, sa structure interne, ses capacités, ses failles potentielles, etc.
En identifiant un système, le pirate peut essayer les failles de sécurité connues pour s'introduire dans le système. Si les administrateurs ont bien protégé leur système, il lui faudra innover, et seuls les petits génies ou les gens patients peuvent trouver de nouvelles failles…

Notons qu'une fois le système connu, le pirate évitera certainement de se compromettre, et installera une copie du système pour faire des tentatives d'attaque, jusqu'à trouver une technique qui pourrait marcher. Inutile d'attirer les soupçons en attaquant à répétition…

♦ L'organisation

On sous-estime toujours le rôle humain du piratage : la plupart des failles sont en effet provoquées par un défaut humain.
Première faiblesse : les administrateurs qui se ménagent des facilités au mépris de la sécurité. Deuxième faiblesse : les utilisateurs qui ont accès à la cible.

Lorsqu'on veut accéder à des données personnelles, on peut passer des semaines à tenter d'attaquer la cible, alors que comprendre que le chef du personnel utilise pour mot de passe le prénom de sa femme est beaucoup plus rapide pour le même résultat… et en prenant beaucoup moins de risques !
Pire : se faire passer pour un administrateur et demander à un utilisateur son mot de passe par messagerie donne souvent des résultats surprenants !
Bref, connaître la structure interne d'une organisation, savoir qui a accès à quoi, permet de repérer des failles beaucoup plus efficaces que les failles informatiques… Et l'organigramme d'une société est souvent décrit sur leur site web !

ATTAQUER

La phase de collecte d'informations terminée, reste à exploiter les données recueillies et mettre en place une stratégie d'attaque. Celle-ci peut être simple et directe, mais la plupart du temps, il s'agit de ruser et de tenter de contourner les problèmes plutôt que de les attaquer de front.

♦ L'attaque frontale

L'attaque frontale a le moins de chance de réussir, sauf si bien sûr l'objectif est de créer un déni de service.
Elle consiste à exploiter une **faille connue** (ou espérée) de la cible pour atteindre son objectif. Sur une machine protégée efficacement (et les machines sensibles le sont en général), il est peu probable que les failles ne soient pas corrigées, mais on ne sait jamais !
Les attaques frontales laissent assez souvent des « signatures » reconnaissables. Entendez par-là que l'on identifiera probablement l'attaque pour ce qu'elle est, et donc que les systèmes de défense éventuels pourraient déclencher des alarmes.
De plus, l'attaque a souvent des effets secondaires pas forcément désirés. Il est assez pénible de faire planter une machine alors qu'on souhaite y lire des données… d'autant plus qu'on a rarement droit à une deuxième chance dans des délais raisonnables.

♦ L'attaque intermédiaire

L'attaque intermédiaire existe sous différentes formes.

Quelques chiffres

Voici quelques chiffres tirés de différentes lectures… ils peuvent être assez édifiants.
- Lorsqu'une vulnérabilité est détectée, il faut en moyenne 30 jours pour qu'elle soit corrigée sur 50 % des systèmes concernés. Sur certains systèmes, elles ne sont jamais corrigées.
- plus de la moitié des messages électroniques échangés dans le monde sont des messages indésirables. Une bonne partie véhicule des virus ou des programmes malveillants.
- Le CERT (un des principaux organismes de surveillance de la sécurité) a recensé plus de 137 000 incidents liés à la sécurité en 2003 (contre 21 000 en 2000).
- le même CERT a recensé 3 784 vulnérabilités dans des logiciels en 2003. Pour en savoir plus : http://www.cert.org/.
- D'après le CSI (Computer Security Institute), une étude menée avec le FBI donne les informations suivantes : le vol d'informations propriétaires a coûté 70 milliards de dollars aux entreprises victimes. Les dénis de service arrivent en second avec 65 milliards. 53 % des attaques venaient de l'extérieur, 18 % combinaient extérieur et intérieur. Le rapport complet est téléchargeable sur le site http://www.gocsi.com

En gros, il s'agit de parier sur le cheminement réseau d'une information souhaitée entre la cible et un demandeur autorisé et de s'arranger pour se trouver entre les deux afin de l'**intercepter**. À noter qu'un mot de passe est une information comme une autre…
Si on a la chance de se trouver sur le même réseau qu'un utilisateur accédant à la ressource (ou mieux, sur le même réseau qu'un serveur cible), on peut tenter de *sniffer* les données (autrement dit, de voir ce qui passe sur le réseau et de lire les données). Cela ne fonctionne que lorsqu'on se trouve très proche soit du client, soit du serveur. À moins que les transmissions ne soient cryptées, on peut alors accéder à tout…

Une autre solution consiste à créer une **déviation** : on appelle ça la technique du *man in the middle*. Que ce soit en interceptant des messages ou en s'insérant au milieu d'une communication, on peut ainsi jouer le rôle de « relais » entre le serveur et le client. Simple à énoncer, cette technique n'est pas si évidente à réussir car les communications intègrent un certain nombre de sécurités pour garantir la liaison… mais avec de la chance, une bonne connaissance du système et de bonnes connaissances, tout est possible.
Il reste toutefois un risque de détection non négligeable dans ce cas de figure.

♦ L'attaque de Troie

Tout le monde connaît la technique du cheval de Troie : tout est toujours beaucoup plus simple quand on l'attaque de l'intérieur, et pour cause : les systèmes de défenses périphériques sont ignorés et les défenses restantes sont plus fréquemment « dirigées » vers l'extérieur.
Là encore, on peut effectuer cette attaque de deux façons.
La première consiste à se **déplacer physiquement sur place**. Le pirate pénètre (ou se trouve) dans les locaux où se trouve la cible, trouve un ordinateur disponible et discret et commence son attaque. La chose est risquée, évidemment, et le temps est limité. Mais contre les systèmes extrêmement bien sécurisés, c'est encore ce qui marche le mieux.
L'autre option consiste à attaquer une cible secondaire et moins protégée afin d'y installer **un programme de type « cheval de Troie »,** autrement dit, un programme qui permettra au pirate d'utiliser la machine comme relais pour ses attaques. Ce n'est pas toujours très complexe à faire : il suffit généralement d'envoyer un virus aux employés et de compter sur leur bêtise pour que le virus s'installe et installe également des accès cachés qu'un pirate va exploiter. Sur une centaine d'utilisateurs, ce serait bien la mort s'il n'y avait personne pour exécuter une pièce jointe portant le nom « blague.exe » ou encore « Rapport.doc.scr ».
L'attaque se fait alors tranquillement, soit pendant qu'un utilisateur travaille sur la machine (eh oui : les ordinateurs sont multitâches), soit la nuit si la machine reste allumée.

♦ L'attaque dormante

Variante du cheval de Troie, l'attaque dormante est très lente, mais souvent efficace. Là encore, le point de départ consiste souvent à implanter un **virus** et du **code malveillant**. Rien de plus facile : un message envoyé avec une jolie animation peut cacher l'installation d'un programme sournois, et l'utilisateur en faisant suivre le message peut très bien le diffuser sur d'autres postes.
L'action du programme malveillant est évidemment dictée par le pirate qui l'implante, mais cela peut consister à enregistrer toutes les touches frappées par l'utilisateur (et donc les mots de passes) ou de faire une copie du carnet d'adresses ou encore de faire suivre des données vers une adresse extérieure.
Plus le réseau cible est grand et possède d'utilisateurs, plus l'attaque est efficace, mais également détectable.
De manière générale, il y a plus de failles sur les clients (comprendre les simples ordinateurs) que les serveurs (souvent bien protégés par les administrateurs). Ce sont ces failles qui sont exploitées.

♦ L'attaque sournoise

Enfin, parfois, le moyen le plus simple d'obtenir une information est de demander… Dans une grande structure où les administrateurs ne connaissent pas tout le monde, il est possible d'envoyer un message de la part d'un utilisateur précis pour demander une réinitialisation du mot de passe : si l'usurpation d'identité est bien faite et les conditions de sécurité peu regardantes, on dispose rapidement d'un accès à travers le compte utilisateur. Mieux : un coup de fil fait souvent l'affaire : *« j'ai perdu mon mot de passe ! Oui, je prends note du nouveau que vous venez de me réinitialiser… ».*

Bref, parfois il est plus simple de faire appel à la **crédulité** des gens pour obtenir ce qu'on veut. On peut par exemple provoquer un déni de service, et appeler l'équipe technique qui, occupée et stressée par la panne provoquée, sera moins regardante sur les conditions de sécurité…

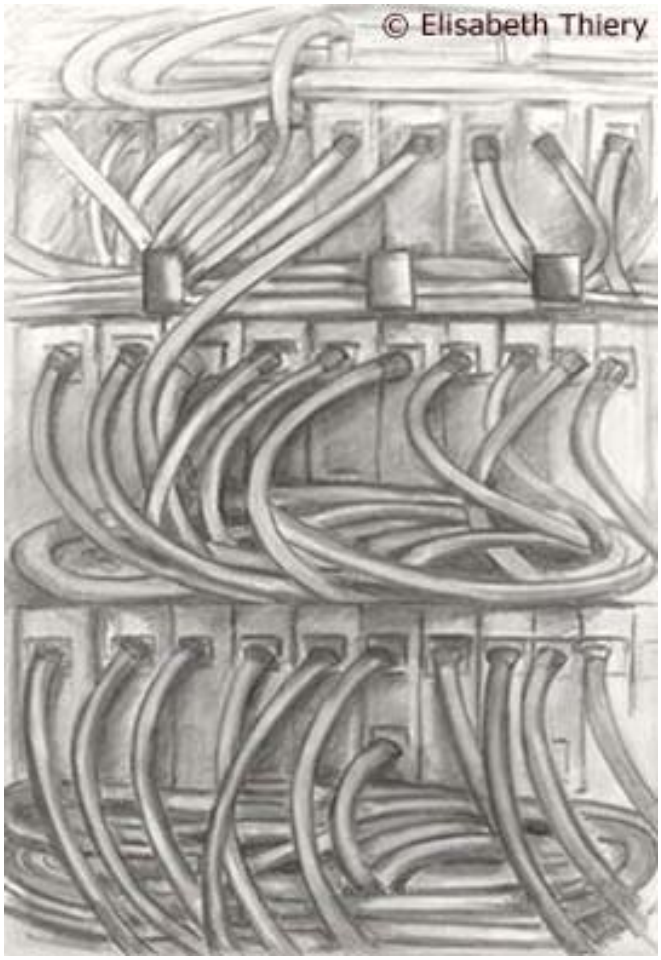
DEFENSES

Bien sûr, qui dit attaque, dit défense. Dans un environnement de plus en plus virtuel, les systèmes de plus en plus complexes intègrent une multitude de défenses plus ou moins bien gérées. Sans prétendre donner des indications sur les techniques utilisées, cette partie se veut surtout informative par rapport aux types de défenses que les joueurs vont rencontrer en face d'eux.

♦ Moyens de la défense

Sans parler des techniques, la première chose à prendre en considération est la politique interne au niveau de la cible, son budget et l'importance du système.

Une société basant beaucoup d'éléments essentiels sur l'informatique investira probablement plus dans la sécurité. Une société qui est pingre sur le personnel n'aura pas de spécialiste sécurité ou une équipe réduite. Si le directeur de la compagnie est paranoïaque, la sécurité sera un point important même pour une PME… Bref, pour savoir quelle résistance rencontreront les pirates joueurs, il faut connaître l'organisme cible et sa politique de sécurité.



Une société riche pourra par exemple mettre en place des honeynets ou des réseaux faussés destinés uniquement à tromper les pirates. Ils sont protégés aussi bien que les vrais serveurs, mais contiennent des données volontairement fausses ou des systèmes de détections poussés.
À l'inverse, une société pauvre n'aura peut-être même pas de protection antivirale (et risque de couler dès la première épidémie).

Le nombre de personnes dans l'équipe informatique est également important : si le personnel gère également le tout venant, et que le personnel est calibré en fonction du besoin des utilisateurs internes, il est peu probable que le réseau soit correctement protégé.

♦ Les bloqueurs

Au niveau des équipements de défenses, on trouve des machines destinées à bloquer les attaques en provenance de l'extérieur. Que ce soit un simple routeur d'accès avec des restrictions ou un firewall élaboré qui surveille le trafic, ces machines sont souvent onéreuses et mal installées mais diablement efficaces lorsqu'elles sont bien utilisées.
Le pirate doit alors tenter de les contourner. Très souvent en effet, une attaque frontale amène le système à couper la liaison ou à interdire la source de l'attaque pour couper court à toute malveillance. Tout est alors à refaire. De plus, ces équipements ont parfois la capacité de fausser les données, autrement dit de faire croire qu'ils sont d'autres systèmes pour ne pas faciliter le travail des intrusions…
Les bloqueurs efficaces sont souvent chers, aussi sont-ils souvent hors de portée des petites entreprises, qui peuvent néanmoins attendre ce type de services de leur fournisseur d'accès au réseau… Là encore, c'est une question de prix.
Les bloqueurs sont parfois doublés d'un système filtrant permettant d'éliminer les virus ou les pièces jointes de messages.

♦ Cryptographie

Pour empêcher les attaques intermédiaires, une bonne solution consiste à crypter les communications. Bien qu'il ne soit pas impossible de décrypter, l'opération peut prendre entre quelques minutes et plusieurs années en fonction du code utilisé et de la puissance des machines de décryptage.
Il existe de nombreux algorithmes de codages qui constituent une science mathématique et informatique à part… Le cryptage permet souvent de décourager les pirates et de rendre inutile l'interception de données.
Il est également possible de crypter les données écrites sur les disques. Seuls ceux qui disposent d'une clé particulière peuvent alors comprendre les données. Y accéder par piratage est donc inutile sans les clés de décodages. Là encore le décryptage est possible, mais il est souvent plus simple d'essayer d'obtenir la clé depuis l'utilisateur accrédité.
Notons aussi que le cryptage des données nécessite une administration informatique beaucoup plus pointue et rigoureuse, et que par conséquent, les cryptages forts sont réservés à des systèmes aux équipes nombreuses.

♦ Surveillance et alertes

Évoquons un peu les sondes de détection d'intrusions. Elles servent à surveiller le réseau à la recherche de traces d'éventuelles tentatives de piratages. En gros, elles effectuent le travail d'un homme qui scruterait constamment les informations qui transitent sur le réseau pour trouver les anomalies et déclencher l'alerte.

Comme tout système automatisé, elles sont à la fois plus efficaces et moins fines qu'un humain : trop paranoïaques, elle crient au loup tellement souvent qu'on n'y fait plus attention, pas assez, elles laissent passer des attaques discrètes ou indirectes. Leur calibrage est donc une affaire de spécialiste.
Toute action informatique laisse une trace quelque part. La plupart du temps, cette trace persiste une semaine ou un mois, puis est effacée. Le pirate a donc intérêt à faire en sorte que ses traces soient les moins visibles possibles.
Des outils existent toutefois qui fouillent les traces et recherchent des corrélations étranges, indiquant le passage d'un pirate.

♦ Défenses postérieures

Enfin, une fois l'attaque finie, tout n'est pas terminé pour le pirate : la fierté des administrateurs systèmes étant blessée, ils feront tout pour retrouver le coupable a posteriori, en particulier si des dégâts économiques importants entraînent un dépôt de plainte.
Les opérateurs peuvent être amenés à communiquer des informations dans ce cadre, et des services spécialisés existent pour mener les enquêtes sur internet. Ainsi, en France, la DST dépêche généralement un agent spécialiste dans les 24 heures (en cas de demande de la victime) pour tenter de pister le pirate.
Evidemment, la plupart des infractions restent impunies, mais c'est généralement parce que la source de l'attaque est située à l'autre bout du monde, dans des zones de non droit. Néanmoins, certaines arrestations importantes ont eu lieu, même si elles restent le plus souvent discrètes.
Il faut aussi avouer qu'il y a rarement dépôt de plainte contre un pirate, car cela serait avouer des défauts de sécurité et donc inquiéter les potentiels clients…

CONCLUSIONS

On le voit, la tâche du pirate est loin d'être aisée. Les intrusions effectuées en une minute montre en main dans les films restent de la science-fiction. Attention toutefois à ne pas perdre le côté amusant du piratage dans le jeu de rôle (et uniquement dans le jeu de rôle) : parfois, un simple jet de dé doit permettre d'avancer une enquête.
Un meneur soucieux de réalisme, toutefois, peut faire comprendre que le piratage reste une affaire de grands spécialistes, et qu'il demande souvent beaucoup de temps pour aboutir. Le pirate du dimanche ne risque ni de faire des dégâts, ni même d'inquiéter les administrateurs d'un réseau sécurisé.
Reste que le piratage est et reste une activité illégale, quelque soit le but de la manœuvre, et que les conséquences pour un personnage peuvent être graves. En espérant que ces quelques éléments (très simplifiés) fourniront des pistes pour mieux comprendre ce qu'implique le piratage…