

Honeypot, le vrai-faux réseau charmeur de pirates

Par Marc OLANIE le 21/09/2001

Pour se protéger du cheval de Troie, il n'y a qu'une seule parade fiable : construire un décor hollywoodien ressemblant à Troie, avec ses habitants, ses guerriers et les charmes de la belle Hélène. C'est la fonction des "réseaux virtuels", ou honeypots (pots de miel) , destinés à attirer les pirates et analyser leurs méthodes d'attaque.

En matière de sécurité des réseaux, il n'est que peu de certitudes. Sauf peut-être celles-ci : aucun système n'est infaillible, et la solidité d'une architecture se dégrade irréversiblement avec le temps. Les vérités d'un moment s'évanouissent à la moindre alerte du Cert, à l'apparition d'une faille de sécurité révélée par l'éditeur d'un noyau ou d'une nouvelle génération d'outils d'intrusion. Autre lapalissade, les mécanismes de protection les plus réputés finissent toujours par succomber sous les coups de boutoir des "malfaisants" qui parcourent la Toile. Ainsi, pendant longtemps, le mot firewall suffisait à rassurer le plus paranoïaque des administrateurs système. Rares sont, de nos jours, les responsables informatiques qui méconnaissent les problèmes liés à un paramétrage tout chirurgical des passerelles de protection, et plus rares encore ceux qui prennent pour argent comptant les vertus d'une technologie "infaillible" - PKI, VPN, cryptage... Autres constats, la compétence toujours accrue du pirate, le perpétuel changement de ses méthodes d'attaque. Et, face à cela, l'extraordinaire réactivité des "sapeurs-pompier" de réseaux qui, trop souvent, opèrent avant même que de consciencieux administrateurs n'aient pu appliquer un service pack, un hot fix, un correctif ou une nouvelle compilation de noyau. A tel point que les principaux experts du domaine, s'ils ne nient pas l'utilité des programmes commerciaux de protection, en viennent à estimer que la seule défense réellement efficace consiste à surveiller de visu les activités des crackers, d'agir au coup par coup et de colmater les brèches au fur et à mesure de leur découverte. Le travail "à la main", dans cette guerre numérique, ne sera pas de sitôt supplanté par un programme standard. Un seul et unique outil de détection (ou IDS, pour Intrusion Detection System) ne saurait faire face à la diversité des méthodes vicieuses de pénétration de machines. Mais pour mesurer le bien-fondé de telles assertions, il faut connaître les us et coutumes de ceux que les DSI américaines dénomment "chapeaux noirs".

Contrôler les pirates en épiant leurs faits et gestes

Las, tout le monde ne s'appelle pas Bruce Schneier ou Chris Klaus (patrons de Counterpane et d'ISS, respectivement), et les pirates ne sont pas réputés pour leur inclination aux confidences. Dès lors, il n'y a plus qu'une solution : examiner, à leur insu, les faits et gestes des flibustiers du code et en tirer les leçons qui s'imposent. Pour cela, on attirera lesdits crackers sur un système d'apparence normale, mais aussi surveillé que le QHS de la Santé. C'est le honeypot, la "chèvre" des chasseurs de lions (voir schéma ci-contre). Il en va des honeypots comme des outils de cryptage. Certains sont grossiers et piègent tous les gibiers possibles, d'autres sont subtilement évolués et garantissent des résultats ciblés. Bien sûr, plus l'outil sera évolué, plus il coûtera, en temps, en difficulté d'analyse, en perfectionnement. Les "faux réseaux" exigent presque autant de travail administratif qu'une architecture de production et un temps d'analyse de dix à cinquante fois plus important. Ce luxe doit donc demeurer proportionnel à la valeur des informations à protéger. Le plus simple des "pots de miel", c'est la faille visible, le système apparemment déjà violé sur lequel se jeteront les pirates de petite envergne.

Ainsi de Back Officer Friendly, un programme qui simule parfaitement un système compromis par la "porte dérobée" Back Orifice. Un outil qui a souvent fait ses preuves lors de tentatives d'espionnage "internes". Plus intelligents sont les deception tools de Fred Cohen, un pionnier du honeypot. Il s'agit d'un ensemble de scripts en Perl capable de fournir des réponses plausibles à des requêtes lancées sur ports TCP "virtuellement utilisés". Cet utilitaire, gratuit, est accompagné d'une série d'accessoires destinés à enregistrer les activités des éventuels pirates, à avertir l'administrateur ou à égarer le "chapeau noir" dans les arcanes d'une table de mots de passe inexploitable. L'auteur précise que, avec dix services TCP réellement utilisés et dix services "bidons", il y aurait 50 % de chances qu'un attaquant tombe sur un leurre dès sa première tentative et se fasse détecter. Dans le cas contraire, et en appliquant consciencieusement les correctifs publiés par les éditeurs de systèmes, la probabilité que le cracker puisse exploiter une faille connue réduit de 80 % son efficacité d'action... et le pousse à prendre pour cible un autre port, ce qui augmente d'autant les chances de le détecter. DTK, le Deception Tool Kit, peut être mis en œuvre en moins d'une demi-journée de travail et ne requiert que très peu d'attention quotidienne. C'est l'outil idéal pour une petite entreprise travaillant avec un accès Internet peu important et théoriquement déjà sécurisé par le fournisseur d'accès ou de services.

Prêcher le vrai pour offrir du faux plus vrai que nature

Mais DTK, estiment les professionnels, n'est jamais qu'une série de "failles apparentes" susceptibles d'attirer les pirates par sa simple présence. Or, le propre du honeypot, c'est de préserver le plus discrètement possible l'existence d'un véritable réseau. Si la structure informatique est réputée importante, le hacker se doutera que les compétences de son service informatique sont à la mesure de la taille du réseau protégé, et qu'une liaison Telnet ouverte à tous vents, ou un port TCP béant, n'est qu'un panneau grossier dans lequel il ne tombera pas. A quoi bon, en effet, appâter de "petits" pirates qui, de toute façon, n'auraient pas la compétence requise pour violer un Firewall-1 correctement paramétré ? Le miel attire les mouches, mais seules les mouches vraiment nuisibles retiennent l'attention des responsables sécurité. Cette escalade dans l'armement, c'est ce que préconise le Sans Institute ou encore le site Root Prompt.org. Le jeu, ici, consiste non plus à "faire tourner" une suite de programmes, mais à monter un véritable système, un site "sacrificiel", normalement protégé par son propre firewall et réagissant comme un réel serveur d'entreprise. Peu de choses différencient un dispositif honeypot d'un système de production. Tout au plus y ajoute-t-on un serveur de logs, chargé d'enregistrer de façon exhaustive toutes les actions du pirate et indépendant du serveur "chèvre". En outre, chaque fichier de log est très discrètement dupliqué, en évitant d'utiliser si possible des trames IP au profit de protocoles du genre IPX ou Appletalk - surtout pas Netbios, c'est une des denrées préférée des intruders ! La première action des intrus est, très souvent, de faire disparaître ledit journal afin d'effacer toute trace de leur passage. Cette surveillance est complétée par une lecture attentive des alertes du firewall, par de nombreux relevés de doutes à l'aide d'un sniffer multiprotocole et par un IDS classique. L'armure peut être renforcée d'un logiciel surveillant les modifications des fichiers sensibles (profils, fichiers système, tables des mots de passe, DLL et équivalents...) tel que Tripwire. Pourtant, malgré toutes ces précautions, le rôle de kamikaze que tient l'appât ne doit pas faire oublier que le danger n'est jamais écarté. Ainsi, on ne reliera jamais, par quelque moyen que ce soit, le "pot de miel" à un réseau de production. De même, on s'assurera que le monde extérieur n'est pas vulnérable à une attaque générée à partir du système en question. Ce serait en effet un comble de voir utiliser, dans le cadre d'une attaque en déni

de services, un serveur leurre dûment relié à Internet et originellement conçu pour combattre le vandalisme informatique. Enfin, certaines absences ou présences d'activités précises peuvent éveiller les soupçons de l'attaquant. Dans le meilleur des cas, il abandonnera le système sans jamais rien révéler, et le honeypot n'aura servi à rien.

Trompe-l'œil en volume et fausses perspectives

Il peut arriver bien pire encore. Par exemple que le hacker en profite non seulement pour ne rien laisser transpirer d'intéressant, en restreignant ses pseudo-attaques à des classiques du genre, mais encore qu'il en profite pour étudier le profil psychologique et le niveau technique de l'équipe de sécurité, en évaluant la manière dont le honeypot a été monté. Scanners de ports furtifs tel NMAP, méthodes d'intrusion à trames fragmentées comme Fragrouter de Dug Song, camouflage de signature interdisant la capture de données à l'instar du scanner Whisker... autant d'armes de piratage aussi évoluées que les méthodes modernes de défense. Après les ports fantômes, les systèmes virtuels, les vrais-faux serveurs, voici venus des réseaux entiers destinés à tromper l'ennemi. C'est le projet Honeynet (voir schéma page 70), une maquette reproduisant fidèlement l'outil de production, avec ses programmes de protection et ses applications, ses services et l'intégralité de son activité. Si cette expérience ne concerne qu'une trentaine d'entreprises spécialisées dans la sécurité, les retombées de ses travaux sont exploitables par tous, et la méthodologie de mise en œuvre est communiquée dans ses moindres détails.

Un ouvrage de référence

Concrètement, cela se traduit par une grande œuvre épique en plusieurs épisodes, intitulée Know your enemy : une série d'articles pour mesurer l'étendue des connaissances nécessaires pour monter un Honeynet et, surtout, l'utiliser. Trois hackers internes, travaillant respectivement pour le compte d'un opérateur, d'un grand média télévisuel et d'une ancienne entreprise d'Etat, déclarent à l'unisson : "Un réseau factice, c'est trois ou quatre mois de travail au montage, puis, lors de chaque attaque, entre dix et quarante minutes de "jus de crâne" pour l'équivalent de une à deux minutes de trames offensives. Un vrai travail de Sisyphe. C'est aussi des années d'expérience, une vision "instinctive" de l'octet vicieux ou de la chaîne de caractères capable de contourner une limitation de service. Mais c'est surtout deux ou trois personnes - nul ne peut humainement passer vingt-quatre heures sur vingt-quatre sur des logs qui n'en finissent pas - qui se relaient sans cesse sur un système non opérationnel, une escouade perdue dans le désert des Tartares, qui attend un ennemi invisible et représente une charge salariale d'ingénieur de haut niveau." Leur métier paraît encore plus difficile à défendre que celui de directeur de service informatique. Il s'agit d'une de ces fonctions qui, paradoxalement, ne se justifient que par l'absence de problèmes. "Le rôle de certains d'entre nous est même remis en question par leur hiérarchie, à tel point qu'il leur arrive de souhaiter qu'une catastrophe survienne durant leurs vacances, ou qu'ils rêvent que leur direction générale est frappée d'une soudaine crise d'intelligence et parvient à comprendre le sens caché d'un SYN sauvage." Ce malaise des hommes de l'ombre profite, on l'imagine, aux espions du numérique et autres barbouzes de l'information. "Le vrai cracker est un professionnel, travaillant parfois pour le compte d'un

concurrent, d'un service gouvernemental étranger ou d'un groupe d'activistes. Il ne laisse jamais de trace visible et ne provoque rien qui justifie l'usage d'un honeypot ou d'un Honeynet."

Quand on attrape les pirates...

Que faire en cas de détection d'intrusion ? Sur ce point, les avis des utilisateurs interrogés ne divergent guère. "Surtout, absolument rien, si ce n'est, une fois la méthode d'attaque découverte, colmater la brèche." Pas de contre-attaque ? "Jamais, au grand jamais !", répondent les hommes de l'ombre des grands réseaux français. Le propre d'un honeypot est de demeurer anodin, de ne jamais se dévoiler. C'est une taupe, un agent dormant. Certes, par moments, on serait tenté de "bombarder" l'attaquant. Mais, nous risquerions de dévoiler nos positions. Il existe toujours un risque de voir déferler une monstrueuse attaque en DoS par un biais que nous n'avions pas prévu. Dans la plupart des cas, lorsque l'analyse est achevée, on expédie un message broadcast, du genre "fermeture du serveur pour maintenance", identique à celui que nous pourrions envoyer à nos administrés, et nous tombons le système. A son redémarrage, la faille est comblée, et nous n'avons plus qu'à attendre que le pirate travaille pour nous et découvre une nouvelle fissure. Si l'attaque est concertée et semble provenir d'un point précis, ce qui est exceptionnel, il nous reste l'espoir de nous adresser aux autorités judiciaires." Mais, selon toutes les personnes interrogées, le cas ne s'est jamais présenté, du moins officiellement. "La seule action d'éclat que nous nous permettons de temps à autre est de communiquer à certains de nos confrères une nouvelle méthode de protection. Parfois, nous sommes confrontés à de vrais dilemmes... Par exemple, nous possédons une parade. Faut-il la divulguer à un organisme public au risque que les crackers, lecteurs assidus de ce genre de publications, aient vent de la chose et adaptent leurs offensives ?"

repères

Le marché

... Est indéfinissable. Si des éditeurs commencent à commercialiser des simulateurs de réseaux et de machines capables de créer une parfaite illusion d'existence, bon nombre de honeypots sont le fruit d'une alchimie où se côtoient de vieilles machines de rebut, des routeurs en fin de course, pour la partie matériel, des scripts et codes très personnels. Paradoxalement, plus le responsable sécurité recherchera l'efficacité de son leurre, moins il fera appel à des solutions commerciales... et plus l'administration dudit leurre coûtera cher. Le prix du logiciel mis en œuvre dépasse rarement 10 % du coût du service de protection/prévention exploitant ces techniques.

Les enjeux

Populariser largement l'usage des réseaux "cibles"... Plus cette mode se répand, plus les pirates douteront du terrain sur lequel ils s'aventurent, jusqu'à éviter, on peut toujours l'espérer, les systèmes ne possédant aucun honeypot. Ce paradoxe de l'"invisible danger" constitue probablement la plus élégante parade contre les "chapeaux noirs". Bien que remontant aux années soixante-dix, l'idée des réseaux factices et des machines sacrificielles commence seulement à apparaître dans le monde des réseaux de micros. En outre, cette pratique connaît un succès relatif outre-Atlantique, et seules quelques grandes entreprises françaises peuvent s'offrir le luxe d'une cellule de veille anti-hackers permanente. Il s'agit bien plus d'une question de mentalité que d'une question de compétence technique.

La cible

Débutants s'abstenir, petits réseaux, passer au large... Les "outils de déception" exigent une très solide expérience dans l'art du décodage de trame, un budget souvent important pour maintenir et utiliser les réseaux leurres. Ce cocktail exige aussi des nerfs d'acier pour supporter sans broncher les assauts des crackers, une abnégation et un optimisme inébranlables pour entretenir un service "non productif" face, bien souvent, à une direction générale hermétique à l'intérêt de cette guerre des ombres.

