Déni de service distribué (*DDoS*)

NICOLAS FORTIER
FRANCOIS-PHILIPPE IL GRANDE

EPITECH - Promotion 2004

2 mars 2003

Table des matières

Chapitre 1

Qu'est-ce que le déni de service ?

Une attaque par déni de service consiste comme son nom l'indique à rendre indisponible un service. Par exemple bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou encore empêcher la distribution des mails dans une entreprise.

Pour cela le pirate sature les ressources nécessaires au bon fonctionnement du service. Il peut par exemple submerger la bande passante du réseau de traffic inutile, consommer au maximum les ressources mémoire et processeur de la machine victime etc...

Les motivations du pirate sont nombreuses, allant du simple vandalisme gratuit aux enjeux éthiques, économiques à l'espionnage. Les moyens employés pour parvenir à son but sont donc aussi nombreux ; il existe des outils développés par des *Hackers* qu'utiliseront les *Scripts Kiddies* et les attaques plus complexes élaborées par un pirate voulant attaquer une ou plusieurs cibles avec un but précis.

Les attaques par déni de service utilisent plusieurs techniques, parmi lesquelles l'attaque distribuée à laquelle nous allons plus particulièrement nous intéresser.

Chapitre 2

Historique

Tout débute officiellement en avril 1992, avec les premières attaques de type DoS. Un certain *Nuke*, encore appelé *Tueur de Windows*, sévit en bloquant une machine victime saturant la connexion de paquets. *Nuke* est un petit logiciel, aujourd'hui très commun, qui permet l'envoi de ce type d'attaque. C'est la préhistoire des agents distribués, dans le sens où la personne utilise consciemment et manuellement son attaque DoS. Se succèdent ensuite de nombreuses attaques de ce type : *Octopus*, *Ping of Death*, *Teardrop*, *Snort*, etc...

En 1999, le blocage de l'accès à Internet de l'université du Minnesota pendant trois jours, constitue la première agression officielle massive par DDoS. Une armée de machines bombarde simultanément des paquets contre les serveurs de l'université.

L'attaque la plus médiatisée reste toutefois celle de février 2000. Durant quelques jours, les sites de géants de l'Internet comme Amazon, CNN ou eTrade ont été rendus inaccessibles. Depuis l'an 2000, selon le **C.E.R.T.**, de plus en plus d'outils de DDoS permettent de prendre le contrôle non seulement de machines Unix, mais aussi de machines Windows. Avec l'explosion du marché de l'Internet, la faible prévention de la sécurité au niveau grand public, tout est prêt pour créer des armées d'agents de plus en plus importantes.

De plus, les techniques des pirates s'améliorent en permanence, et vulgarisent la propagation des agents par le biais de logiciels . Répondant aux noms de Stacheldraht, Trinoo ou TFN (Tribal Flood Network), leurs outils tirent profit de chaque défaut de conception des protocoles liés à IP (*Internet Protocol*), de TCP (*transfert Control Protocol*) à UDP (*User Datagram Protocol*) en passant par ICMP (*Internet Control Message Protocol*).

Avec l'apparition et la distribution du logiciel *Trinity*, les agents DDoS rendent compte directement à un canal IRC (*Internet Relay Chat*). Le pirate n'a alors plus besoin de prendre contrôle à distance de l'agent. Il suffit d'aller sur son canal IRC pour donner des ordres et réveiller une armée.

En septembre 2001, un certain virus *Code Red* infecte quelques milliers de systèmes, et une seconde version, intitulée *Code Red II*, installe un agent DDoS, désamorcé à temps. Les rumeurs prétendent qu'il devait lancer une attaque contre la Maison Blanche. Dans un contexte politique de crise, le gouvernement américain annonce que des mesures de sécurité vont être prises.

Mais dès l'été 2002, c'est au tour d'Internet de subir une attaque DDoS à l'encontre de ses 13 serveurs racines. Ces serveurs sont les points clés du système d'aiguillage de l'Internet, appelé Domain Name System (DNS). Cette attaque ne durera qu'une heure mais aurait pu paralyser l'ensemble du réseau Internet. L'incident est pris au sérieux par les experts qui affirment renforcer à l'avenir la sécurité de leurs machines.

La première version de *Slapper*, apparue à la mi-septembre 2002, a contaminé plus de 13 000 serveurs Linux, en deux semaines. *Slapper* utilise un trou de sécurité présent dans le module OpenSSL[1], et véhicule un agent DDoS. Celui-ci est détecté et stoppé à temps.

Malgré tout, le lundi 21 octobre 2002, les administrateurs qui gèrent les 13 serveurs clefs voient 9 des hôtes bloqués, en subissant à nouveau une attaque par déni de service. Leurs ressources sont inaccessibles, pendant trois heures. Une partie des entreprises et organismes gérant ces serveurs clés réagit et décide de revoir ses dispositifs de sécurité. Le FBI a ouvert une enquête, mais localiser le ou les auteurs de l'attaque s'annonce difficile.

Des serveurs de bases de données MS-SQL de la société Microsoft, mal configurés, ont été infectés par le ver *SQL-Slammer* extrêmement virulent. Ce dernier transporte un agent DDoS, qui lance une attaque le 25 janvier 2003 contre Internet. Cette fois ci, seuls 4 des 13 serveurs racines responsables du routage d'Internet ont été affectés. Malgré la virulence de l'attaque, la performance globale du réseau a été à peine réduite de 15%.

[1] implémentation Open Source des protocoles Secure Sockets Layer et Transport Layer Security

Chapitre 3

Les différentes techniques d'attaque

Il existe deux types de dénis de services : le déni de service applicatif et le déni de service réseau.

Le déni de service applicatif exploite les vulnérabilités d'une application comme par exemple des dépassements de tampon (*buffer overflow*), ou encore la saturation de ressources. Les dénis de service applicatifs exploitent les faiblesses de la conception d'un protocole ou de son implémentation.

Les attaques par déni de service réseau se distinguent en différentes techniques :

l'attaque directe La cible est attaquée directement, dans ce cas l'attaquant dispose d'une bande passante supérieure ou égale à la cible.

l'attaque par rebond Pour une action de l'attaquant, la cible recoit N attaques, provenant de plusieurs autres machines intermédiaires, comme par exemple dans le cas du *smurf*.

l'attaque par réflexion L'attaquant ne contacte pas directement la victime, mais génère des paquets spoofés avec comme adresse source celle de la victime. Il envoie alors les paquets à des serveurs légitimes qui répondront à la victime.[1]

l'attaque distribuée (DDoS) L'attaquant dirige plusieurs machines qui servent de relais et agissent en même temps dans le but d'amplifier l'attaque [2] et de multiplier les origines de ces attaques.

[1] L'article *Application-Level Reflection Attacks* **[4]** traite ce sujet de façon plus détaillée.

[2] Par la multiplication du nombre de connexions à un serveur, du nombre de requêtes etc...

3.1 Déni de service distribué (Distributed Denial Of Service)

Ce sont actuellement les attaques les plus dévastatrices. Elle reposent sur l'utilisation d'agents aussi appelés *daemons* qui sont déployés sur le maximum de machines possible. Le pirate installe le *daemon*[3] sur des machines mal sécurisées connectées à internet, soit en les piratant, soit à l'aide d'un ver. Les agents exécuteront alors simultanément les commandes ordonnées par le pirate pour attaquer une cible prédéfinie.

3.1.1 L'agent (le *daemon*)

Les premiers types d'agents étaient des applications complètes dédiées à l'attaque. Aujourd'hui ils prennent la forme de chevaux de troie et sont souvent combinés avec les fonctionnalités de virus et de ver pour s'approprier rapidement un maximum de machines via le réseau internet : ordinateurs personnels, serveurs, routeurs, assistants personnels, téléphones portables... [4]

Les moyens à la disposition du pirate pour répandre ses agents sont nombreux :

- les réseaux peer-to-peer tels que *kazaa*, *GNUtella*, *audiogalaxy*...[5]
- les fichiers humoristiques aux formats word, flash etc.[6]
- les sites pirates
- les sites de téléchargement de jeux
- les sites à caractère pornographique

Cette liste est loin d'être exhaustive. L'agent peut avoir été écrit de facon à être très léger pour s'introduire dans un système via une application anodine (*cheval de troie*), puis une fois installé récuperer les *exploits* nécessaires[7] via le réseau en fonction des informations récoltées sur la machine compromise.

3.1.2 Les architectures

Les pirates exploitent des techniques de plus en plus élaborées. Par exemple *Tribal Flood Network* (TFN), un système en architecture deux tiers (client-serveur) permet à un client de contrôler plusieurs *daemons* qui vont attaquer la cible (voir figure 3.1). *Trin00* un autre système, fonctionne lui,

[3] Un cheval de Troie

[4] Les nouvelles génération de téléphones portables intègrent un système d'exploitation ou une machine virtuelles Java, permettent de se connecter à internet, de télécharger des applications. Toutes ces possibilités favorisent le développement d'applications malicieuses.

[5] Services distribués d'échange de fichiers en peer-to-peer

[6] Ce genre de fichiers circulent beaucoup dans les grandes entreprises, favorisant la possibilité de compromettre beaucoup de machines

[7] Système d'exploitation, version, services, protocoles...

en architecture trois tiers : le pirate dirige des serveurs maîtres (*masters*) qui contrôlent les *daemons*. Le troisième tiers augmente la difficulté à tracer la source de l'attaque en ajoutant une couche aux communications (voir figure 3.2). De plus les moyens de communication entre le pirate et les agents sont nombreux et très difficiles à détecter : messages ICMP (*Internet Control Message Protocol*), segment TCP (*Transfert Control Protocol*), datagramme UDP (*User Datagram Protocol*), IRC (*Internet Relay Chat*), messagerie instantanée, noeud peer-to-peer...

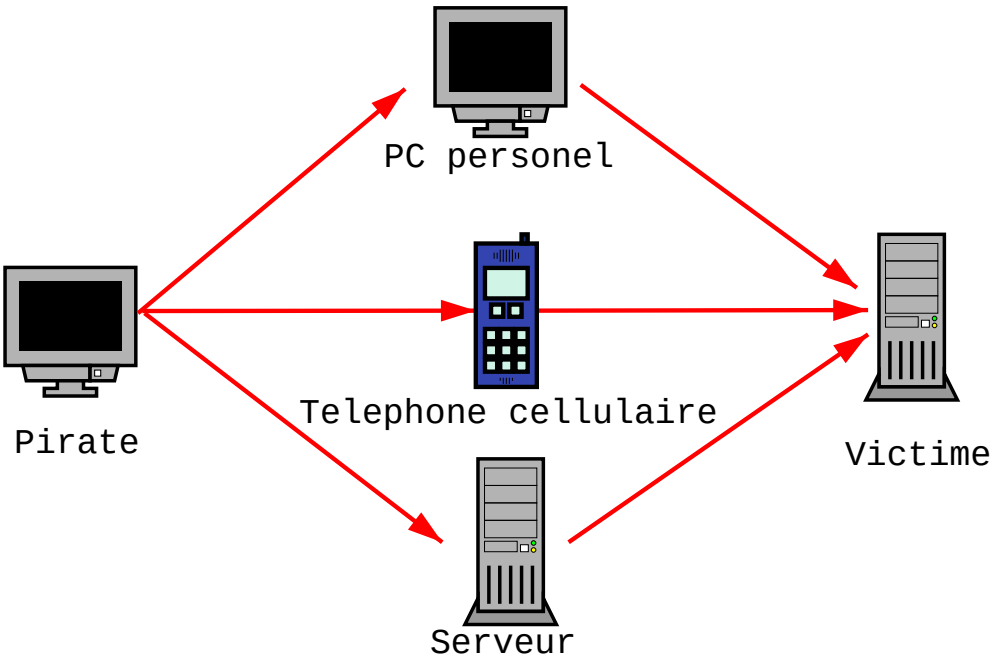

FIG. 3.1 – Architecture 2 tiers

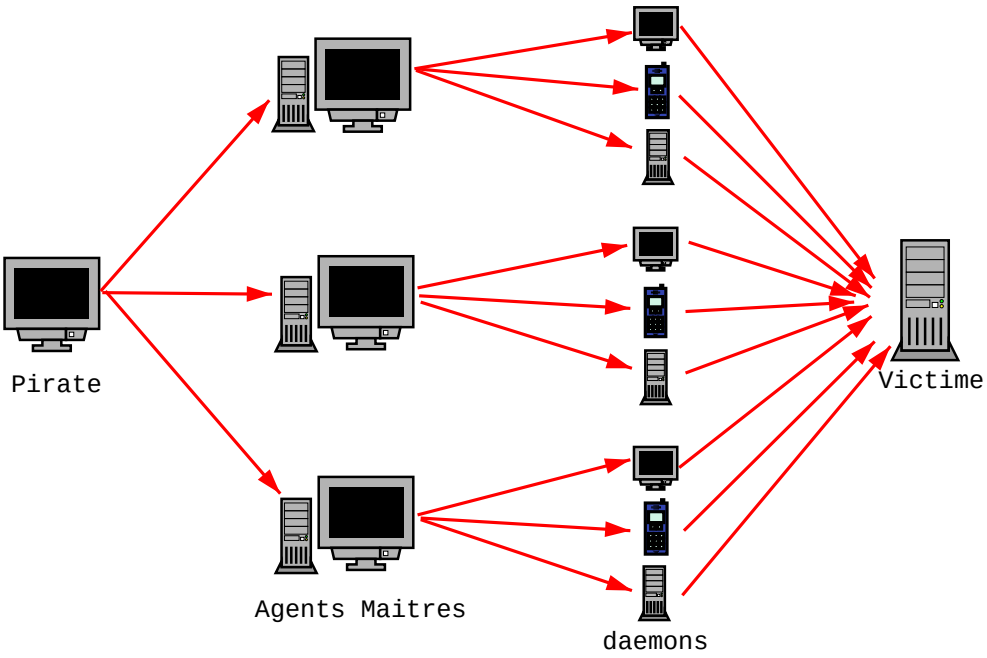

FIG. 3.2 – Architecture 3 tiers

Plusieurs milliers de machines peuvent ainsi être contrôlées à partir d'un point unique de contact. Le pirate peut se constituer une véritable "armée". Avec suffisamment de machines n'importe quel type d'attaque devient efficace : requêtes HTTP (*Hyper Text Transfert Protocol*) buggées, fragmentation de paquets, traffic aléatoire, dans tous les cas la cible sera submergée et ne pourra faire face au flot de données. Tous les types d'équipements peuvent être touchés : les routeurs (dans ce cas ce n'est plus un service qui est atteint mais un ou plusieurs réseaux entiers), les serveurs DNS (*Domain Name System*), mail, Web, les firewall, les IDS (*Intrusion Detection System*)...

Le document *Distributed Denial of Service Attack Tools***[1]**, décrit plus en détail les différents outils et architectures existants.

Chapitre 4

Les enjeux et les motivations

4.1 Les conséquences économiques et politiques

Les attaques DDoS ont des conséquences économiques non négligeables. En effet le réseau *internet* est vital pour certaines entreprises qui l'ont pleinement intégré dans leurs outils de communication et dans la gestion de leur système d'information (e-mails, personnel nomade, VPN, etc.).

Le réseau a été concu à l'origine pour résister en cas de destruction physique de voies de communications, cependant il est encore relativement fragile en raison de la conception des protocoles qui le régissent à certains types d'attaques, dont les attaques par déni de service.

En octobre 2002, les treize serveurs DNS racines ont subi une attaque d'une violence sans précédent, sept d'entre eux ont été mis hors service et deux ont subi des défaillances par intermittence. Une attaque plus longue aurait tout simplement paralysé tout le réseau *internet* avec les conséquences économiques que cela implique.

Les attaques sont de plus en plus nombreuses, en 2001, plus de 12 800 attaques sur plus de 5000 cibles ont été recensées sur une période de 3 semaines par l'Université de Californie San Diego. Selon une enquête CSI/FBI Computer Crime and Security, 40% des entreprises victimes d'une attaque DoS auraient perdu 287 000 $ en moyenne par attaque.[1]

4.2 Les motivations du pirate

4.2.1 Le mercenariat

On parle de plus en plus de "Guerre de l'information", voire même de "pirates mercenaires". Pourquoi ne pas envisager d'employer officieu-

[1] source NetCost and Security : http ://www.netcost-security.fr

sement des pirates, capables de lancer des attaques par DDoS, contre une entreprise concurrente ? Les victimes de ces attaques étant complètement paralysées, voire balayées d'Internet, il est alors facile de les discréditer.

Sans comptersur le fait que l'on peut difficilement remonter aux auteurs des attaques DDoS, il est quasi impossible de déterminer les commanditaires. Après tout, on évoque bien la reconversion de *Hackers* dans des entreprises de sécurité informatique. Un autre avantage de cette pratique mafieuse est que l'on peut la renouveler à volonté, aucune parade à long terme n'ayant été trouvée. Le pirate peut tout aussi bien déclancher une guerre d'entreprise, en attaquant l'une et faisant porter le chapeau à l'autre.

Enfin, outre les enjeux lucratifs, un nouveau courant a fait son apparition : le cyber-terrorisme. Les américains crient au loup, surtout depuis le contexte du 11 septembre, mais on peut trouver de nombreux groupes pirates qui agissent dans des intérêts politiques autant qu'éthiques.

4.2.2 La destruction gratuite

Les plus dangereux à utiliser ces outils sont sans doute les *Scripts Kiddies*, en français gamins du script. Adolescents doués ou non, débutant en connaissance de programmation et sécurité des réseaux. Des pirates expérimentés leur remettent un outil de destruction simple, avec lequel ces *Scripts Kiddies* vont se défouler, sans vraiment comprendre l'impact de leurs actes. Et même en cas d'arrestation par les forces de l'ordre, ils sont protégés par la loi. Tant qu'ils ne sont pas majeurs, ils ne risquent rien. Quoi de mieux que de manipuler un adolescent en flattant son ego, alors que celui-ci cherche la reconnaissance en s'amusant ! Et puis, il est toujours possible de laisser un agent dormant dans la machine de l'apprenti-pirate pour relancer une attaque à son insu. Ceci constitue le moyen idéal pour brouiller les pistes et éviter que l'on remonte à la véritable source.

Les attaques DDoS répétées contre le site `grc.com`, Gibson Research Corporation, dédié à la sécurité informatique, sont un exemple typique d'une manifestation d'un Script Kiddie. Un adolescent de 13 ans, muni de programmes fournis par un pirate expérimenté, proclame sur un forum être l'auteur de ces attaques en ajoutant qu'il est meilleur en sécurité que le propriétaire du site.

Les moyens de diffusion sont nombreux et variés, nul besoin d'aller bien loin pour obtenir des outils d'attaque DDoS. D'ailleurs, il suffit de taper les mots *Nuke* et *DDoS* sur un moteur de recherche (Google par exemple) pour obtenir la page d'un site avec la dernière version de *Win-*

dows Nuke it. C'est un petit logiciel qui gère l'IP Spoofing [2], l'envoi de paquet contre une machine victime, avec même une gestion d'erreur. Il est tout aussi facile d'obtenir des outils plus dangereux, qui lèvent des armées de machines, sur des forums spécifiques ou via IRC.

4.2.3 Le pouvoir et la reconnaissance

En commettant ces actes criminels, nombreux sont ceux qui cherchent à obtenir une reconnaissance sociale. Les raisons profondes de tels actes sont très variées et font ressortir un problème humain basique : montrer aux autres sa puissance, sa position dans la société. C'est l'éternelle lutte contre le système social.

Ces attaques sont aussi nées par simple jeu ou défi intellectuel, bien évidemment ce jeu peut vite mal tourner avec un esprit de compétition entre différents groupes de pirates.

On peut assimiler ces attaques sauvages à un profond besoin d'expression vis à vis de l'extérieur. Je suis vivant, je peux agir sur toi. De plus, s'il est assez simple de réaliser des choses de façon anonyme sur Internet, les gens cherchent un minimum de reconnaissance . On s'invente alors un pseudonyme, on attaque des sites connus (voire Internet dans son ensemble), puis on s'en vante sur les forums, salon de chat etc. Ce besoin de se distinguer de la masse, en nuisant à autrui, est pourtant réprimable.

La justice internationale étant loin d'être au point, le danger se résume à un jeu de cache-cache d'autant plus excitant pour qui veut augmenter sa réputation.

[2] Masquage de son adresse IP par une adresse IP factice

Chapitre 5

Peut-on lutter contre ce type d'attaque ?

5.1 La détection d'un déni de service

Il y a peu de moyens de détecter une attaque par déni de service, par exemple dans le cas d'un site de commerce en ligne comment savoir si le flot de requêtes est légitime ou non ? En effet il est normal que ce genre de site soient très fréquentés à certaines heures.

5.2 L'impact sur les performances

Le facteur le plus visible est l'impact de l'attaque sur les performances, qui peut alerter l'administrateur.

5.3 Les outils

Certains outils tels que les systèmes de détection d'intrusion (NIDS), les Parefeux (Firewall) ou les NMS, peuvent en établissant la corrélation entre les différentes informations recueillies dans les fichiers de logs permettre d'identifier une attaque et les sources potentielles.

Par exemple on peut déduire de la réception de datagrammes de taille maximum que l'on subit une attaque visant à saturer la bande passante. Si les datagrammes sont de petite taille il peut s'agir d'un déni sur un service ou une application.

5.4 Les difficultés globales

Il est tout de même très difficile de lutter contre ce type d'attaque, compte tenu de la complexité de la mise en oeuvre de moyens pour la dis-

tinguer du traffic légitime. Il est de plus en plus facile de mettre en oeuvre une attaque DDoS sans avoir de réelles connaissances techniques sur les protocoles réseau et en programmation, en effet des outils "prêts à l'emploi" existent.

La sécurité d'Internet dépend de chacun des maillons qui le composent, il est impossible de résister à une attaque de cette nature. Le seul moyen de s'en prémunir consisterait donc à agir en amont, en mettant en place une politique de sécurisation globale visant à limiter la propagation des *agents*.

Il faudrait faire de la prévention sur les éventuelles utilisations malicieuses des nouvelles technologies comme par exemple la possibilité d'installer des programmes en Java sur les téléphones portables de dernière génération qui deviennent de nouveaux *hôtes* pour des agents malveillants de tout type.

Chapitre 6

Glossaire

Buffer Overflow *dépassement de tampon* en français, ce qui arrive lorsque plus de données sont stockées dans un tampon qu'il ne peut en recevoir. Ce problème est souvent exploité par les *crackers* pour faire exécuter des commandes par un programme ayant des droits administrateur.

C.E.R.T. *Computer Emergency Response Team*, organisme américain d'expertise en sécurité Internet

Cheval de Troie Programme malicieux qui est camouflé en un programme bénin, tel qu'un jeu, un utilitaire.

Cracker 1. Pirate informatique. 2. Individus malicieux qui essaie de découvrir des informations sensibles en fouillant. 3. Personne qui s'introduit dans des systèmes informatiques en exploitant leurs vulnérabilités.

Exploit 1. Vulnérabilité dans un logiciel qui peut être utilisée pour outrepasser la sécurité ou attaquer un hôte connecté à internet via le réseau. 2. Programme qui exploite un *exploit* dans le sens de la première définition.

Hacker 1. Personne qui aime explorer les détails des systèmes programmables et comment étendre leurs possibilités, contrairement à la majorité des utilisateurs, qui préfèrent apprendre seulement le minimum nécessaire. 2. Personne qui programme avec enthousiasme (voire avec obsession) ou qui aime programmer plutôt que simplement théoriser la programmation. 3. Personne capable d'expertiser un hack. 4. Personne qui programme bien et rapidement. 5. Personne ayant une expertise dans l'utilisation d'un programme particulier, ou travaillant souvent dessus ou avec. 6. Expert ou enthousiaste de toute nature, un hacker en astronomie, par exemple. 7. Personne qui apprécie les défis intellectuels ou le fait de surmonter de façon créative les difficultés.

Peer-to-Peer Liaison poste à poste par opposition au modèle client-serveur. Dans ce type de réseau les ordinateurs sont connectés les uns aux autres sans passer par un serveur central. Ce type de réseau est très utilisé pour les échanges de fichiers pirates (MP3, Films, Images, Livres...), en raison de l'impossiblilité de mettre un terme à ces échanges car il n'y a pas de serveur central.

Script Kiddie Le plus bas niveau parmis les crackers ; un script kiddie (gamin du script) commet des actes malicieux en utilisant des scripts et des programmes écrits par d'autres, souvent sans comprendre l'*exploit*.

Smurf Technique d'attaque DoS par rebond.

Spoofing Capturer, alterer et retransmettre un flux de communication de façcon a tromper la personne qui le reçoit. Pour cela le cracker falsifie l'adresse de l'expediteur dans les packets TCP/IP.

VPN *Virtual Private Network*, réseau privé virtuel sur Internet, utilisation des outils de cryptographie pour créer un réseau invisible des autres utilisateurs connectés.

Chapitre 7

Références

[1] Internet Security Systems, *Distributed Denial of Service Attack Tools (PDF)*,
http ://documents.iss.net/whitepapers/ddos.pdf
Une bonne présentation générale de plusieurs outils de DDoS.

[2] Steve Gibson, *GRC Denial of Service Attacks*,
http ://grc.com/dos/grcdos.htm
Site informatif sur les attaques DDoS.

[3] David Dittrich, *David Dittrich DDoS Page*,
http ://staff.washington.edu/dittrich/misc/ddos/
Page de David Dittrich, spécialiste sécurité et DDoS.

[4] Tom Vogt, *Application-Level Reflection Attacks*,
http ://web.lemuria.org/security/application-drdos.ps
Document sur les attaques par réflexion.

[4] MISC (*Multi-system & Internet Security Cookbook*) no. 4, *Attaque par déni de service*, Magazine français de sécurité informatique.