Halte aux hackers

4e édition

Stuart McClure
Joel Scambray
George Kurtz

ISBN : 2-7464-0486-9

OEM
EYROLLES

12

Déni de service (DoS)

Smurf, Fraggle, boink et teardrop. Non, il ne s'agit pas de sodas pour pré-adolescents, mais d'outils utilisés ces dernières années par des pirates pour semer le désordre absolu sur Internet. Les attaques par déni de service coûtent aux entreprises des millions d'euros par an – temps d'arrêt, chiffre d'affaires non réalisé, main d'œuvre –, et représentent une menace sérieuse pour tous les systèmes ou réseaux quels qu'ils soient. Une attaque par déni de service gêne ou interrompt totalement les services fournis à des utilisateurs, des réseaux, des systèmes ou d'autres ressources légitimes. Ce type d'attaque est généralement malveillant et ne nécessite que de maigres compétences, les outils requis étant disponibles pour qui souhaite les utiliser.

Ces dernières années, de nombreuses attaques ont fait les gros titres des journaux, comme celles contre Yahoo!, eBay, Buy.com, CNN.com, E*TRADE, ZDNet et PANIX.c6+ pour n'en citer que quelques-unes. Ces attaques ont paralysé leurs victimes pendant une courte période et ont été immédiatement identifiées comme des attaques par déni de service distribué (DDoS, Distributed Denial of Service), leur virulence dépassant largement celle d'attaques par déni de service courantes.

Le plus inquiétant avec ces attaques, c'est qu'elles exploitent les faiblesses inhérentes au protocole sur lequel repose Internet, TCP/IP. Plus précisément, ces attaques se concentrent sur une faiblesse de la gestion des requêtes SYN, ce qui signifie que le problème provient de la conception même du réseau. En outre, dans les cas mentionnés précédemment, les pirates avaient falsifié leurs adresses source de façon à masquer leur identité. Ainsi, ces attaques, et toutes celles qui ont suivi, ont été extrêmement difficiles à repérer et personne n'a réussi à remonter jusqu'aux vrais coupables. Cet événement a eu un effet dévastateur sur la communauté des internautes et a mis en lumière la fragilité du réseau Internet. Les utilisateurs avaient

beau savoir depuis plusieurs années que ces attaques étaient théoriquement possibles, ils ont alors pris douloureusement conscience des risques liés au commerce électronique.

Motivations des assaillants

Dans ce livre, nous vous présentons divers outils et techniques utilisés par les pirates pour briser la sécurité des systèmes cible. Un administrateur système ou réseau compétent peut déjouer la plupart des attaques, laissant ainsi au hacker un sentiment d'impuissance et de frustration qui l'incite souvent à lancer une attaque par déni de service.

Outre cette motivation née de la frustration, certains individus mènent des combats personnels ou politiques contre d'autres individus ou organisations. De nombreux experts en sécurité estiment que ce type d'attaque augmentera nécessairement à cause de la prolifération des systèmes Microsoft Windows. En effet, l'omniprésence et la position de leader incontesté de Microsoft et de ses systèmes en font la cible privilégiée de nombreux pirates. Ces attaques sont de plus en plus aisées grâce aux outils de déni de service qui reposent sur le concept simple de pointer-cliquer et ne requièrent aucune compétence technique particulière.

Bien que la plupart des attaques soient motivées par les situations mentionnées ci-dessus, les pirates cherchent parfois à infiltrer réellement un système vulnérable. La plupart des administrateurs système Windows savent pertinemment qu'il est nécessaire de redémarrer un système Windows pour appliquer un grand nombre de modifications. Ainsi, après avoir modifié un paramètre du système NT en vue de s'octroyer des droits administrateur, les pirates devront parfois planter le système pour provoquer un redémarrage par l'administrateur système. Cette action devrait attirer l'attention des administrateurs sur la présence d'un serveur vulnérable et de pirates potentiels, mais ils choisissent généralement d'ignorer cet incident et redémarrent joyeusement le système sans aucune arrière-pensée.

Nous ne pouvons pas présenter ici toutes les motivations susceptibles d'inciter un pirate à lancer une attaque par déni de service, mais sachez simplement que le cyberespace est calqué sur la vie réelle. Certaines personnes aiment nuire aux autres et éprouvent un sentiment de puissance en effectuant une attaque DoS. Mais l'ironie de la situation est que la plupart des hackers compétents méprisent les attaques de ce type, ainsi que leurs auteurs.

Types d'attaques par déni de service

Malheureusement, les attaques par déni de service sont devenues la solution de repli préférée des cyberterroristes du nouveau millénaire. Il est souvent bien plus simple d'interrompre le fonctionnement d'un réseau ou d'un système que d'y avoir un accès réel. Avec l'arrivée des systèmes d'acquisition et de contrôle des données (SCADA, Supervisory Control and Data Acquisition) raccordés en réseau, les conséquences des attaques DoS peuvent être catastrophiques. Les systèmes SCADA servent à relier des réseaux d'ordinateurs destinés à gérer les infrastructures d'un pays, notamment l'eau, l'électricité, etc.

Les protocoles réseau comme TCP/IP ont été conçus pour une utilisation au sein d'une communauté ouverte et sûre, d'où les failles inhérentes au protocole le plus courant sur Internet, IPv4. En outre, de nombreux systèmes d'exploitation et d'équipements réseau reposent sur des piles de protocoles vulnérables qui affaiblissent leur capacité à résister aux attaques par déni de service. Nous avons vu plusieurs dispositifs de commande de processus équipés de piles IP rudimentaires s'effondrer sous nos yeux à la suite d'un simple renvoi de paquets ICMP avec un paramètre non valide. Bien que de nombreux outils soient capables de lancer des attaques par déni de service, il est important de connaître les différents types d'attaques possibles pour être en mesure de les détecter et de les éviter. Nous allons commencer par explorer les fondements théoriques des types d'attaques par déni de service les plus courants.

Utilisation de la bande passante

La forme la plus insidieuse d'attaque par déni de service est l'attaque par saturation de la bande passante. Il s'agit pour les assaillants d'utiliser toute la bande passante sur un réseau donné. Cette opération peut être réalisée sur un réseau local, mais les pirates choisissent généralement de saturer vos ressources à distance. Ce type d'attaque peut se dérouler selon deux scénarios de base.

Scénario 1

Les attaquants parviennent à inonder la connexion réseau de la victime parce que leur bande passante est plus importante. Imaginez, par exemple, un pirate avec une connexion réseau T1 (1,544 Mbit/s) ou plus qui inonde une liaison de réseau de 56 ou128 Kbit/s ; c'est un peu comme si un semi-remorque entrait en collision frontale avec une fourgonnette. Résultat, le véhicule le plus imposant, dans notre cas le plus gros tuyau, remporte nécessairement la bataille. Ce type d'attaque n'est pas limité aux connexions réseau à faible débit. Nous avons vu des cas où les pirates obtenaient l'accès à des réseaux disposant d'une bande passante de 100 Mbit/s. Citons ici l'exemple de pirates qui sont parvenus à lancer des attaques par déni de service contre des sites équipés de connexions T1 et à saturer complètement la liaison réseau de la victime.

Scénario 2

Les pirates amplifient leur attaque par déni de service en regroupant plusieurs sites pour inonder la connexion réseau de la victime. Un pirate qui possède une seule liaison réseau de 56 Kbit/s est capable de saturer complètement un réseau disposant d'un accès T3 (45 Mbit/s). Comment est-ce possible ? S'il a recours à d'autres sites pour amplifier l'attaque par déni de service, un pirate disposant d'une bande passante limitée peut aisément récupérer jusqu'à 100 Mbit/s de largeur de bande. Pour accomplir cet exploit, il doit convaincre les systèmes amplificateurs d'envoyer du trafic vers le réseau de la victime. Les techniques d'amplification sont plus faciles à mettre en œuvre que vous le pensez, comme nous allons le voir dans ce chapitre.

Nous vous rappelons encore ici que le trafic ICMP est dangereux. En effet, s'il joue un rôle précieux en termes de diagnostic, il reste facile à exploiter abusivement et sert souvent de munition aux attaques par saturation de bande passante. En outre, il est d'autant plus difficile d'identifier les auteurs de ces attaques qu'ils falsifient leur adresse source.

Épuisement des ressources

Une attaque par épuisement des ressources se distingue d'une attaque par saturation de la bande passante dans la mesure où elle se concentre sur les ressources système plutôt que sur les ressources réseau, notamment sur l'utilisation de l'unité centrale, de la mémoire, des quotas de fichiers système, etc. Les pirates bénéficient souvent d'un accès légitime à une quantité donnée de ressources système, mais ils profitent ensuite de cet accès pour utiliser des ressources supplémentaires. Dès lors, le système ou les utilisateurs légitimes sont privés de leur part de ressources. Les attaques par déni de service par épuisement des ressources conduisent généralement à l'indisponibilité de certaines ressources parce que le système se bloque, le système de fichiers est saturé ou des processus sont interrompus.

Défauts de programmation

Les défauts de programmation sont des incapacités à gérer des conditions exceptionnelles liées à une application, à un système d'exploitation ou à une puce à logique incorporée. Ces conditions exceptionnelles sont généralement provoquées par l'envoi de données imprévues vers le programme vulnérable. Les pirates envoient souvent des paquets bizarres, non conformes aux RFC, vers un système cible pour déterminer si la pile réseau est en mesure de traiter cette exception ou si cette situation va provoquer une erreur fatale au niveau du noyau (*kernel panic*) et un blocage du système. À travers des applications spécifiques s'appuyant sur les entrées utilisateur, les pirates peuvent envoyer des chaînes composées de plusieurs milliers de lignes. Si le programme utilise un tampon de taille fixe, par exemple 128 octets, les pirates provoquent un dépassement de tampon qui entraîne une défaillance complète du programme. Mais la situation peut encore empirer si les pirates réussissent à exécuter des commandes avec des droits élevés, comme nous l'avons expliqué dans les chapitres 5 et 7. Par ailleurs, vous aurez parfois affaire à des défauts de programmation dans les composants électroniques. La tristement célèbre attaque par déni de service du Pentium f00f a permis à un processus de type utilisateur de bloquer tout un système d'exploitation en exécutant l'instruction non valide 0xf00fc7c8.

Comme la plupart d'entre nous ont pu le constater, il n'existe pas de programme, de système d'exploitation, ni même d'unité centrale sans défaut. Les pirates connaissent également cet axiome et profitent pleinement des conséquences du blocage d'applications critiques ou de systèmes sensibles. Malheureusement, ces attaques surviennent généralement aux moments les plus inopportuns.

Attaques par routage et DNS

Pour procéder à une attaque par déni de service sur le système de routage, un pirate doit manipuler les entrées de la table de routage afin d'empêcher les systèmes ou réseaux légitimes d'accéder aux services. La plupart des protocoles de routage, comme RIP (Routing Information Protocol) v1 et BGP v4 (Border Gateway Protocol) disposent d'une authentification faible, voire inexistante. De plus, cette authentification est rarement utilisée. Ce scénario est idéal pour les assaillants souhaitant modifier des routes légitimes, souvent en falsifiant leur adresse IP source, pour créer les conditions d'un déni de service. Les victimes de ces attaques verront leur trafic acheminé vers le réseau des pirates ou vers un trou noir, c'est-à-dire un réseau qui n'existe pas.

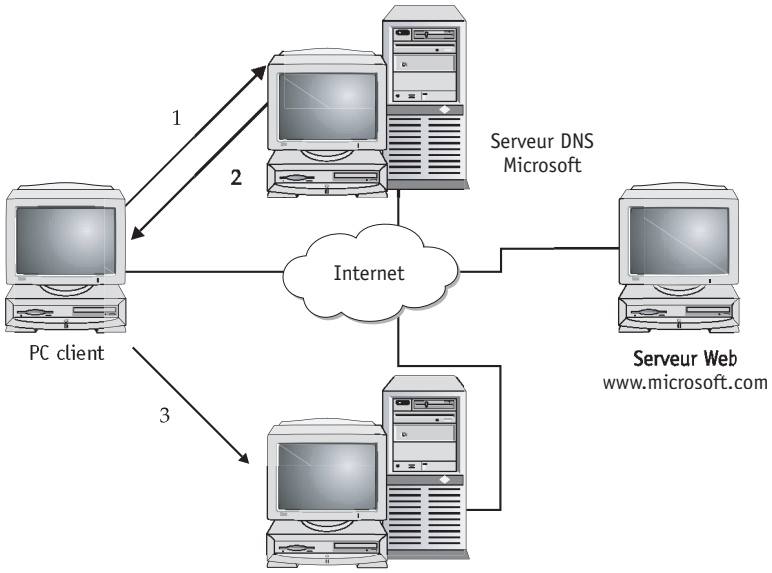
Les attaques par déni de service sur des serveurs de noms de domaine (DNS) sont aussi dévastatrices que les attaques sur le routage. Pour les mettre en œuvre, il est généralement nécessaire de convaincre le serveur victime d'enregistrer des informations d'adresse fictives. Lorsqu'un serveur DNS effectue ensuite des résolutions de noms, les pirates peuvent réacheminer les données vers le site de leur choix ou, dans certains cas, vers un trou noir. Plusieurs attaques DoS liées aux DNS ont rendu inaccessibles des sites importants pour une durée assez longue. La figure 12.1 vous explique comment contaminer un tampon DNS.

Attaques génériques par déni de service

Certaines attaques par déni de service sont capables d'affecter de nombreux types de systèmes différents : il s'agit d'attaques génériques qui appartiennent généralement à la catégorie des dénis de service par saturation de bande passante et par épuisement des ressources. Leur point commun : elles manipulent souvent le protocole. Si un protocole comme ICMP est utilisé à des fins malveillantes, il a la capacité d'affecter simultanément plusieurs systèmes. Ainsi, un pirate pourrait utiliser des bombes e-mail pour envoyer des milliers de messages électroniques à un système victime dans le but d'accaparer toute la bande passante, puis d'épuiser toutes les ressources du serveur de courrier. Le virus Melissa, qui est en réalité un ver, n'a pas été conçu comme une attaque par déni de service, mais il a certainement mis en évidence la simplicité avec laquelle une vague de messages électroniques peut faire mordre la poussière à des serveurs de messagerie. Il s'est reproduit dans de telles proportions que les serveurs de courrier électronique ont fini par se bloquer par manque de ressources disponibles.

Comme nous ne pourrons pas aborder toutes les situations de déni de service possibles, ce chapitre sera consacré aux attaques par déni de service les plus intéressantes à nos yeux pour la plupart des environnements informatiques.

Figure 12.1
Pollution du cache DNS.



1) Le PC client demande à accéder au site Web de Microsoft. Le navigateur essaie de résoudre le nom www.microsoft.com en adresse IP.
2) Le cache du serveur DNS a été contaminé par un pirate et renvoie l'adresse IP www.hacker.com au lieu de celle de Microsoft.
3) Le système des pirates se fait maintenant passer frauduleusement pour www.microsoft.com.

Smurf

Popularité :	*9*
Simplicité :	*8*
Impact :	*9*
Niveau de risque :	***9***

L'attaque Smurf figure parmi les plus effrayantes en raison de ces capacités d'amplification. Cet effet amplificateur est dû à l'envoi d'une requête ping de diffusion ciblée vers un réseau de systèmes qui répondra. Une requête ping de diffusion ciblée peut être envoyée soit à l'adresse de réseau, soit à l'adresse de diffusion du réseau et nécessite l'utilisation d'un dispositif exécutant la fonction de diffusion de la couche 3 (IP) vers la couche 2 (réseau). Consultez la RFC 1812 Requirements for IP Version 4 Routers pour plus d'informations. Si nous supposons que ce réseau a une adresse standard de classe C sur 24 bits, l'adresse réseau sera .0 et l'adresse de diffusion .255. Les diffusions ciblées sont généralement utilisées à des fins de

diagnostic, dans le but de connaître les hôtes actifs du réseau sans effectuer de ping sur chaque adresse de la plage.

Une attaque Smurf tire profit des diffusions ciblées et requiert la participation d'au moins trois acteurs : le pirate, le réseau amplificateur et la victime. Un pirate envoie des paquets ICMP ECHO falsifiés à l'adresse de diffusion du réseau amplificateur. L'adresse source des paquets est falsifiée de façon à donner l'impression que le système victime est l'auteur de la requête. Et le chaos commence ! Comme le paquet ECHO a été envoyé à l'adresse de diffusion, tous les systèmes du réseau amplificateur répondent à la victime (sauf s'ils sont configurés pour ne pas le faire). Si un pirate envoie un paquet ICMP à un réseau amplificateur de 100 systèmes, qui répondront à un ping envoyé à l'adresse de diffusion, il multiplie l'envergure de son attaque par 100. Le coefficient d'amplification est le rapport entre le nombre de paquets envoyés par le pirate et ceux envoyés par le système amplificateur. Par conséquent, un pirate qui réussit à trouver un réseau amplificateur avec un fort taux d'amplification a plus de chances de saturer le réseau de la victime.

Examinons un exemple qui nous permettra de mieux comprendre le fonctionnement de ce type d'attaque. Supposons qu'un pirate envoie 14 Ko par seconde de trafic ICMP vers l'adresse de diffusion d'un réseau amplificateur comprenant cent systèmes. Le réseau des pirates est connecté à Internet via une liaison RNIS à deux canaux, le réseau amplificateur via une liaison T3 de 45 Mbit/s et le réseau de la victime via une liaison T1 de 1 544 Mbit/s. Si vous extrapolez ces chiffres, vous constaterez que les pirates peuvent générer 14 Mbit/s de trafic vers le réseau de la victime. Dans ces conditions, ce dernier a peu de chances de résister à une attaque qui s'appropriera rapidement toute la bande passante disponible de sa liaison T1.

Fraggle est une variante de cette attaque qui utilise des paquets UDP au lieu des paquets ICMP. Les pirates peuvent envoyer des paquets UDP falsifiés à l'adresse de diffusion d'un réseau amplificateur, généralement sur le port 7 (ECHO). Tous les systèmes du réseau dont l'écho est activé répondront à l'hôte de la victime, créant ainsi d'énormes quantités de trafic. Si l'écho n'est pas activé ou si un système réside sur le réseau amplificateur, il génère un message ICMP inaccessible qui consomme également la bande passante.

Parades à Smurf

Pour éviter d'être utilisée comme site amplificateur, la fonctionnalité de diffusion ciblée doit être désactivée au niveau du routeur frontière. Avec les routeurs Cisco, entrez la commande suivante :

```
no ip directed-broadcast
```

Elle désactive la diffusion ciblée. À partir de la version 12 de Cisco IOS, cette fonctionnalité est activée par défaut. Pour d'autres dispositifs, consultez la documentation utilisateur correspondante afin d'apprendre comment désactiver les diffusions ciblées. En outre, des systèmes

d'exploitation spécifiques peuvent être configurés de façon à rejeter discrètement des paquets d'écho ICMP ECHO de diffusion :

Solaris 2.6, 2.5.1, 2.5, 2.4 et 2.3 – Pour empêcher les systèmes Solaris de répondre aux requêtes ECHO de diffusion, ajoutez la ligne suivante à /etc/rc2.d/S69inet :

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

Linux – Pour empêcher les systèmes Linux de répondre aux requêtes ECHO de diffusion, utilisez les fonctions de pare-feu du noyau. Les paquetages de pare-feu varient suivant les versions du noyau, mais les plus courants sont iptables et ipchains. Vous trouverez plus d'informations sur leur configuration sur http://www.redhat.com/support/resources/networking/firewall.html. Les commandes suivantes fonctionnent avec iptables :

```
iptables -A INPUT -p icmp -d 192.168.1.1/32 -j DROP
iptables -A FORWARD -p icmp -d 192.168.100.255/24 -j DROP
```

La première commande rejette tous les messages ICMP adressés à l'hôte lui-même (dans notre exemple, il s'agit de 192.168.1.1). La seconde empêche la transmission des requêtes ECHO de diffusion au réseau interne si le système est utilisé comme pare-feu ou comme routeur.

FreeBSD – Sur la version 2.2.5 de FreeBSD et sur les versions ultérieures, les diffusions ciblées sont désactivées par défaut. Cette fonctionnalité peut être activée ou désactivée en modifiant le paramètre sysctl appelé net.inet.icmp.bmcastecho**.**

AIX – Par défaut, sur AIX 4.*x*, les réponses aux adresses de diffusion sont désactivées. La commande no permet d'activer ou de désactiver cette fonctionnalité à l'aide de l'attribut bcastping. Elle est en outre utilisée pour configurer les attributs de réseau dans un noyau exécuté. Ces attributs doivent être paramétrés à chaque redémarrage du système.

Toutes les variantes UNIX – Pour empêcher les hôtes de répondre à des attaques Fraggle, désactivez echo et chargen dans /etc/inetd/conf en insérant le caractère # devant le nom du service.

Sites attaqués

Bien qu'il soit important de savoir comment empêcher l'utilisation de votre site comme amplificateur, il est encore plus crucial d'apprendre à réagir à ce type d'attaque. Comme indiqué dans les chapitres précédents, vous devez limiter le trafic ICMP et UDP entrant au niveau des routeurs frontières aux systèmes indispensables de votre réseau et à des types de paquets ICMP spécifiques. Bien sûr, cela n'empêchera pas les attaques Smurf et Fraggle d'utiliser votre bande passante. Nous vous conseillons de collaborer avec votre fournisseur de services Internet pour limiter autant que possible le trafic ICMP autorisé en amont. Afin de

renforcer ces parades, certaines organisations ont activé la fonction Committed Access Rate (CAR, taux d'accès déterminé) offerte par Cisco IOS 1.1CC, 11.1CE et 12.0 et permettant de limiter le trafic ICMP à une taille raisonnable, par exemple 256 ou 512 Ko.

Si votre site devait subir une attaque, nous vous conseillons de commencer par contacter le centre d'exploitation de réseau de votre fournisseur de services Internet. Rappelez-vous qu'il est très difficile de remonter jusqu'au coupable lors d'une attaque, mais cela reste possible. Qu'il s'agisse de vous ou de votre fournisseur d'accès Internet, il sera nécessaire de travailler en étroite collaboration avec le site amplificateur puisqu'il est le récepteur des paquets falsifiés. N'oubliez pas que les paquets responsables de l'attaque proviennent en toute légalité du site amplificateur qui reçoit des paquets falsifiés prétendument émis par votre réseau.

Si vous inspectez systématiquement chaque routeur en commençant par le site amplificateur, puis en remontant vers l'amont, vous parviendrez à retracer l'attaque jusqu'au réseau agresseur. Pour cela, il est nécessaire de déterminer l'interface de réception des paquets falsifiés, puis de remonter la piste. Pour faciliter l'automatisation de ce processus, l'équipe de sécurité de MCI a développé un script Perl, dostracker, capable de se connecter à un routeur Cisco et de remonter la piste d'une attaque par mystification jusqu'à sa source. Malheureusement, ce programme est d'un intérêt limité si vous n'êtes pas propriétaire de tous les routeurs impliqués ou que vous n'y avez pas accès.

Nous vous conseillons également de consulter le document RFC 2267, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (Filtrage de réseau entrant : contrer des attaques par déni de service qui exploitent l'usurpation d'adresses source IP), par Paul Ferguson de Cisco Systems et Daniel Senie de Blazenet, Inc.

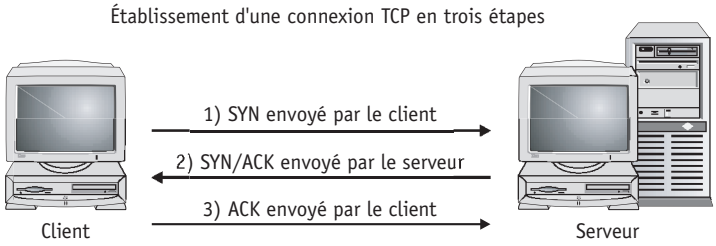
Inondation SYN

Popularité :	*7*
Simplicité :	*8*
Impact :	*9*
Niveau de risque :	***8***

Avant l'arrivée de Smurf sur le devant de la scène, l'attaque par inondation SYN était la plus dévastatrice. L'attaque PANIX.com évoquée dans les premières lignes de ce chapitre est un exemple éloquent des ravages provoqués par une inondation SYN bien menée. Voyons ce qui se passe exactement lorsqu'une attaque par inondation SYN est lancée.

Comme nous l'avons indiqué précédemment, l'établissement d'une connexion TCP se déroule en trois étapes (voir la figure 12.2), c'est pourquoi ce processus est généralement qualifié de poignée de main en trois étapes. Dans des conditions normales, un paquet SYN est envoyé depuis un port spécifique du système A vers un port spécifique à l'écoute du système B. À ce stade, cette connexion potentielle au système B a un statut SYN_RECV. Le système B tente ensuite de renvoyer un paquet SYN/ACK au système A. Si tout se déroule correctement, le système A renvoie un paquet ACK, et la connexion passe au statut ESTABLISHED.

Figure 12.2
Connexion SYN.



Si ce mécanisme fonctionne parfaitement bien la plupart du temps, il présente quelques points faibles intrinsèques susceptibles d'être exploités pour créer une situation de déni de service. À l'origine du problème, le fait que la plupart des systèmes allouent une quantité de ressources limitée à l'établissement d'une connexion potentielle, c'est-à-dire une connexion qui n'est pas encore totalement établie. Bien que la plupart des systèmes soient en mesure de prendre en charge des centaines de connexions parallèles vers un port donné (par exemple, 80), une dizaine de requêtes de connexions potentielles peut suffire à épuiser toutes les ressources allouées à l'établissement d'une connexion. C'est précisément le mécanisme SYN que les pirates exploiteront pour rendre le système indisponible.

Lorsqu'il souhaite lancer une inondation SYN, le pirate envoie un paquet SYN depuis un système A vers un système B, en prenant soin de mystifier son adresse source au préalable pour qu'elle pointe vers un système inexistant. Le système B essaie ensuite de renvoyer un paquet SYN/ACK vers la fausse adresse. Si ce système existait, il répondrait en envoyant un paquet RST vers le système B puisqu'il n'a pas amorcé de connexion. N'oubliez pas cependant que les pirates ont choisi un système inaccessible. Ainsi, le système B envoie un paquet SYN/ACK et ne reçoit en retour aucun paquet du système A. Cette connexion potentielle est à présent maintenue dans l'état SYN_RECV et se trouve placée dans la file d'attente des connexions. Le système B s'est maintenant engagé à établir une connexion qui sera purgée de la file d'attente uniquement lorsque le temporisateur d'établissement de connexion aura expiré. Ce temporisateur varie d'un système à l'autre, mais peut aller de 75 secondes à 23 minutes sur certaines implémentations IP. Comme la file d'attente des connexions est généralement très courte, les pirates n'ont qu'à envoyer quelques paquets SYN toutes les dix secondes pour paralyser totalement un port spécifique. Le système attaqué ne parviendra jamais à purger les connexions accumulées dans la file d'attente avant de recevoir les nouvelles requêtes SYN.

Vous commencez probablement à comprendre pourquoi ce type d'attaque peut être si dévastateur. En premier lieu, une quantité infime de bande passante suffit pour lancer une inondation SYN fructueuse. Certains pirates sont capables de mettre à genoux le serveur Web d'une grande entreprise à partir d'une simple liaison modem à 14,4 Kbit/s. En second lieu, cette attaque est furtive : les pirates falsifient l'adresse source du paquet SYN, ce qui complique singulièrement l'identification du coupable. Ironie du sort, cette attaque avait été envisagée par de nombreux experts en sécurité il y a quelques années et a été réalisée concrètement en exploitant des relations de confiance (voir http://www.phrack.org/show.php?p=48&a=14.)

Parades aux inondations SYN

Pour déterminer si vous faites l'objet d'une telle attaque, utilisez la commande netstat -na si elle est acceptée par votre système d'exploitation. Si vous trouvez un grand nombre de connexions dans l'état SYN_RECV, une attaque SYN est probablement en cours.

Nous vous proposons ci-dessous quatre solutions de base contre les attaques par inondation SYN. Bien que chacune de ces parades présente ses avantages et ses inconvénients, elles permettent toutes de réduire les effets d'une attaque ciblée par inondation SYN. N'oubliez pas qu'il est très difficile de remonter la piste d'une attaque jusqu'à son auteur parce que la source du paquet est falsifiée. Toutefois, l'outil dostracker de MCI peut vous aider à accomplir cette tâche (si vous avez accès au routeur de chaque segment du trajet).

Allongement de la longueur de la file d'attente des connexions – Bien que la pile IP de chaque fabricant ait ses particularités, il est possible de régler la longueur de la file d'attente des connexions pour atténuer les effets d'une attaque par inondation SYN. Bien qu'elle soit utile, cette mesure est loin d'être idéale car elle accapare des ressources système supplémentaires et peut avoir un effet négatif sur les performances.

Réduction de la durée de temporisation d'établissement d'une connexion – Réduire la durée de temporisation d'établissement d'une connexion peut également participer à la réduction des effets d'une attaque par inondation SYN, bien que cette solution, là encore, ne soit pas optimale.

Application de correctifs logiciels fournis par les éditeurs pour détecter et contrecarrer d'éventuelles attaques par inondation SYN – Au moment où nous écrivons ces lignes, la plupart des systèmes d'exploitation modernes mettent en œuvre des mécanismes de détection et de prévention contre les attaques par inondation SYN. Reportez-vous à l'avis du CERT CA-96:21 TCP SYN Flooding and IP Spoofing Attacks (attaques par inondations TCP SYN et mystification IP) qui contient une liste de correctifs et d'astuces concernant les systèmes d'exploitation.

Comme les attaques par inondation SYN ont commencé à se multiplier sur Internet, d'autres solutions ont été développées pour traiter ces situations de déni de service. Par exemple, les noyaux Linux modernes 2.0.30 et supérieurs proposent une option appelée SYN cookie. Lorsque cette option est activée, le noyau détecte et enregistre les attaques SYN éventuelles. Il utilise un aléa cryptologique (*SYN cookie*) pour permettre aux utilisateurs légaux de continuer à se connecter, même lors d'attaques intenses.

D'autres systèmes d'exploitation, comme Windows NT4.0 SP2 et les versions ultérieures, appliquent un mécanisme dynamique de traitement des connexions en attente (voir l'article Q142641 de la base de connaissances Microsoft). Dès que la file d'attente de connexion atteint un seuil prédéfini, le système alloue automatiquement des ressources complémentaires. Ainsi, la file d'attente de connexion n'est jamais saturée.

Utilisation d'un IDS de réseau – Certains systèmes de détection d'intrusion de réseau sont capables de détecter et de répondre activement à des attaques SYN. Ce type d'attaque est

généralement détecté par un flux de paquets SYN sans réponse. Un IDS peut envoyer des paquets RST au système attaqué en réponse à la requête SYN de départ. Cette opération permet au système attaqué de réduire la file des connexions en attente.

Attaques de serveurs de noms de domaine

Popularité :	*6*
Simplicité :	*4*
Impact :	*9*
Niveau de risque :	***6***

Les versions de BIND antérieures à 4.9.5+P1 plaçaient en mémoire cache des informations temporaires lorsque la récursivité de DNS était activée. La récursivité permet à un serveur de noms de gérer les requêtes de zones et de domaines qu'il ne dessert pas. Lorsqu'un serveur de noms reçoit une requête pour une zone ou un domaine dont il n'est pas responsable, il la transmet au serveur de noms concerné. Dès qu'une réponse est reçue de ce serveur de nom, le premier serveur l'envoie à l'auteur de la requête.

Malheureusement, lorsque la récursivité est activée sur une version vulnérable de BIND, un pirate peut corrompre le cache du serveur de noms en effectuant une consultation récursive. Cette opération est connue sous le nom de corruption de pointeurs d'enregistrements (PTR record spoofing) et exploite le processus de mise en correspondance d'adresses IP et de noms d'hôtes. Non seulement l'exploitation des chemins de confiance basés sur la simple consultation de noms d'hôtes peut avoir de sérieuses conséquences en matière de sécurité, mais elle ouvre également certaines portes aux attaques par déni de service sur les serveurs DNS. Ainsi, un pirate peut essayer de convaincre un serveur de noms cible de placer dans sa mémoire tampon des informations qui font correspondre www.exemple.com à 0.0.0.10, une adresse IP inexistante. Par la suite, lorsque les utilisateurs du serveur de noms corrompu tenteront de consulter le site www.exemple.com, ils ne recevront aucune réponse de 0.0.0.10, ce qui constituera un déni de service réel interdisant l'accès à www.exemple.com.

Parade DNS

Pour résoudre ce problème posé par BIND, installez la version BIND 4.9.6 ou 8.1.1 et toute version ultérieure. Bien que ces versions de BIND corrigent les vulnérabilités liées à la corruption du cache, il est préférable d'installer la dernière version de ce produit car elle intègre d'autres correctifs de sécurité (consultez http://www.isc.org/bind.html pour plus d'informations). Vous trouverez d'autres informations sur les correctifs des différents fabricants dans l'avis du CERT CA-97.22 (BIND – The Berkeley Internet Name Daemon).

Déni de service pour UNIX et Windows

Au cours des 25 dernières années, UNIX a gagné en popularité grâce à sa puissance, à son élégance et à sa capacité à effectuer des tâches parfois inconcevables. Bien entendu, cette

liberté et cette puissance entraînent des risques potentiels. Au cours de cette même période, des centaines de situations de déni de service ont été dénombrées sur une multitude d'installations UNIX différentes.

À l'instar d'UNIX, Microsoft Windows a connu une croissance fulgurante de sa popularité au sein des entreprises américaines. De nombreuses sociétés ont ainsi confié aux systèmes d'exploitation Windows le soin de faire prospérer leurs affaires. Même si certains puristes se chamaillent pour savoir lequel de ces deux systèmes est le plus puissant, personne ne remet en doute la richesse des fonctionnalités et la complexité de Windows. C'est pourquoi, comme UNIX, Microsoft est victime des pirates qui exploitent ces nombreuses fonctionnalités afin de lancer des attaques par déni de service au sein du système d'exploitation Windows et des applications associées.

La plupart des attaques par déni de service peuvent être classées en deux catégories : conditions locales et condition distantes de déni de service. À son tour, chacune de ces catégories comprend un grand nombre de situations. Notre objectif est de vous expliquer, par le biais des exemples présentés, les aspects théoriques de chaque attaque plutôt que de détailler chacune d'elles de façon approfondie. Ces attaques sont amenées à évoluer au fil du temps. Si vous en comprenez les bases théoriques, vous serez en mesure de mettre en pratique les principes énoncés ici au fur et à mesure de la découverte de nouvelles attaques. Examinons quelques situations types de déni de service pour chaque catégorie.

Attaques par déni de service à distance

À l'heure actuelle, la plupart des situations de déni de service sont liées à des défauts de programmation associés à la mise en œuvre de la pile IP propre à chaque fabricant. Comme nous l'avons signalé au chapitre 2, chaque fabricant implémente sa pile IP différemment, d'où l'efficacité de la prise d'empreinte de pile. Comme les implémentations IP sont complexes et en constante évolution, de nombreux défauts de programmation existent ou risquent de faire leur apparition. La plupart de ces attaques commencent par l'envoi d'un paquet donné ou d'une séquence de paquets vers le système cible afin d'exploiter des défauts de programmation spécifiques. Lorsque le système cible reçoit ces paquets, il peut agir de différentes façons, du traitement incorrect de ces paquets au blocage complet du système.

Superposition de la fragmentation IP

Popularité :	*7*
Simplicité :	*8*
Impact :	*9*
Niveau de risque :	***8***

Teardrop et ses attaques associées exploitent les vulnérabilités du code de réassemblage de paquets propres à certaines implémentations de piles IP. Lorsque les paquets circulent sur certains réseaux, il est parfois nécessaire de les subdiviser en entités plus petites (fragments)

selon l'unité de transmission maximale (MTU) des réseaux. L'attaque teardrop visait les noyaux Linux anciens qui ne prenaient pas correctement en compte la superposition de fragments IP. En effet, ces noyaux Linux vérifiaient si la longueur de la fragmentation était trop grande, mais pas si elle était trop petite. Ainsi, des paquets soigneusement construits et envoyés vers un système Linux vulnérable provoquaient un redémarrage ou un blocage du système. Mais Linux n'était pas le seul système d'exploitation vulnérable à ce type d'attaque : Windows NT/95 ont également été touchés, d'où les attaques dérivées mentionnées précédemment (newtear.c, syndrop.c, boink.c).

Parade à la superposition de la fragmentation IP

Les vulnérabilités précédentes ont été corrigées dans les noyaux ultérieurs 2.0.x et 2.2.x. Nous vous conseillons d'installer ces dernières versions qui possèdent de nombreux correctifs de sécurité supplémentaires, outre les correctifs des vulnérabilités de fragmentation IP.

En ce qui concerne les systèmes Windows, les vulnérabilités de la fragmentation IP ont été résolues grâce aux correctifs qui ont suivi le Service Pack 3. Les utilisateurs de Windows NT sont encouragés à installer le pack de service le plus récent puisqu'il corrige d'autres vulnérabilités liées à la sécurité. Quant aux utilisateurs de Windows 95, nous leur conseillons d'installer tous les packs de service proposés.

SMBdie

Popularité :	*8*
Simplicité :	*9*
Impact :	*9*
Niveau de risque :	***9***

Windows NT/2000/XP/.NET RC1 sont tous potentiellement vulnérables à une attaque par déni de service bien connue, lancée en 2002 et baptisée SMBdie. La version 0.1 du programme prend comme arguments une adresse IP et le nom NetBIOS associé afin d'envoyer une charge mortelle (et le terme est particulièrement bien choisi). À l'instar des anciennes attaques contre Windows que tout le monde pensait ne jamais revoir, SMBdie exploite une faille dans l'implémentation de TCP/IP qui permet à un pirate de faire apparaître un « écran bleu de la mort » sur le système visé, forçant ainsi l'utilisateur à le redémarrer.

Parade à SMBdie

La seule véritable parade à cette attaque consiste à appliquer le correctif de Microsoft (windowsupdate.microsoft.com) ou à désactiver les ports TCP NetBIOS (139 et 445).

« Fuite » dans la gestion de la mémoire dynamique du spool de Windows NT : canaux nommés sur RPC

Popularité :	*4*
Simplicité :	*8*
Impact :	*7*
Niveau de risque :	***6***

Windows NT souffre d'une fuite de mémoire dans spoolss.exe qui permet à un utilisateur non autorisé de se connecter à \\server\PIPE\SPOOLSS et d'accaparer toute la mémoire disponible du système cible. Pour compliquer la situation, cette attaque peut être lancée via une session nulle même si les connexions RestrictAnonymous sont activées. Cette attaque peut mettre un certain temps à paralyser le système cible, démontrant ainsi que des ressources peuvent être consommées lentement sur des périodes prolongées dans le but d'éviter toute détection.

Parade à la fuite dans le spool de Windows NT

Pour désactiver cette attaque par le biais d'une session nulle, vous devez supprimer SPOOLSS de la clé de registre HKLM\System\CCS\Services\LanmanServer\Parameters\NullSessionPipes(REG_MULTI_SZ). N'oubliez pas que cette parade n'empêche pas des utilisateurs authentifiés d'exécuter cette attaque.

Déni de service par dépassement de tampon sur un serveur FTP IIS

Popularité :	*5*
Simplicité :	*3*
Impact :	*7*
Niveau de risque :	***5***

Comme nous vous l'avons vu au chapitre 7, les attaques par dépassement de tampon sont extrêmement efficaces dès qu'il s'agit de compromettre la sécurité de systèmes vulnérables. Outre leur impact incroyable sur la sécurité, ces attaques permettent de créer des conditions de déni de service. Si la situation de dépassement de tampon ne fournit pas un accès de niveau superutilisateur, elle peut souvent être exploitée afin de bloquer à distance une application vulnérable.

Le serveur FTP d'IIS 3.0 et 4.0 est vulnérable à une situation de dépassement de tampon dans la commande list qui donne aux pirates la possibilité de bloquer le serveur à distance. La commande list est accessible aux utilisateurs uniquement après authentification, mais cela ne s'applique pas aux utilisateurs anonymes FTP qui peuvent y accéder directement. Il est important de noter que le risque reste relativement limité tant que l'on affaire à une attaque par déni de service. Ce niveau augmenterait significativement si l'utilisateur avait la possibilité d'exécuter du code arbitraire sur le système cible via la situation de dépassement de tampon.

Parade au déni de service par dépassement de tampon sur un serveur FTP IIS

Le Service Pack 5 et les correctifs qui ont suivi le Service Pack 4 permettent de pallier cette vulnérabilité de Windows NT 4.0.

Attaques stream et raped

Popularité :	*5*
Simplicité :	*6*
Impact :	*9*
Niveau de risque :	***7***

Stream.c (dont on ne connaît pas l'auteur) et raped.c de Liquid Steel ont fait leur apparition sur Internet au début de l'année 2000. Ces deux attaques similaires sont à la fois simples et très efficaces. Elles relèvent du type épuisement de ressources qui exploite l'incapacité du système à gérer des paquets mal formés envoyés simultanément. Conçus à l'origine comme des outils d'attaque contre les systèmes FreeBSD uniquement, les outils stream et raped sont capables de porter atteinte à de nombreux systèmes d'exploitation, y compris (mais pas uniquement) Windows NT. L'utilisation excessive du processeur (voir la figure 12.3) indique généralement que ce type d'attaque est en train de se produire. Cependant, une fois l'attaque terminée, le système revient à son état normal. L'attaque stream.c envoie des paquets TCP ACK vers une série de ports associés à des numéros de séquence et des adresses IP source aléatoires. Quant à l'attaque raped.c, elle envoie des paquets TCP ACK avec des adresses IP source falsifiées.

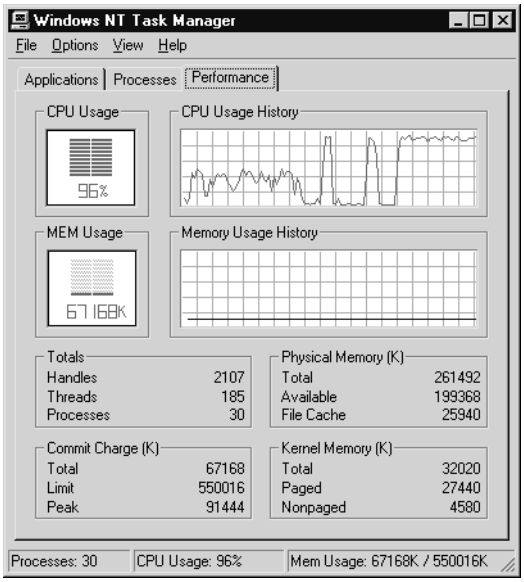


Figure 12.3
L'utilisation excessive du processeur signale souvent une attaque de type stream ou raped.

Parades aux attaques stream et raped

Malheureusement, peu de systèmes d'exploitation proposent de correctifs contre ces attaques. Nous ne connaissons aucun correctif pour Windows NT. En revanche, dans le cas de FreeBSD, vous pouvez appliquer le correctif officieux disponible sur http://www.freebsd.org/~alfred/tcp_fix.diff.

Attaque ColdFusion Administrator

Popularité :	*7*
Simplicité :	*8*
Impact :	*9*
Niveau de risque :	***8***

Découverte par Foundstone en juin 2000, cette vulnérabilité exploite une faiblesse de programmation qui permet de bloquer le serveur. Le déni de service se produit lors du processus de conversion des mots de passe saisi et enregistré dans des formats appropriés à une comparaison lorsque le mot de passe saisi est particulièrement grand (plus de 40 000 caractères). La réalisation de cette attaque est simple et elle est présentée au chapitre 15 « Piratage du Web ».

Parades à l'attaque ColdFusion Administrator

Les parades à cette vulnérabilité sont détaillées au chapitre 15 « Piratage du Web ».

Attaques par déni de service distribué

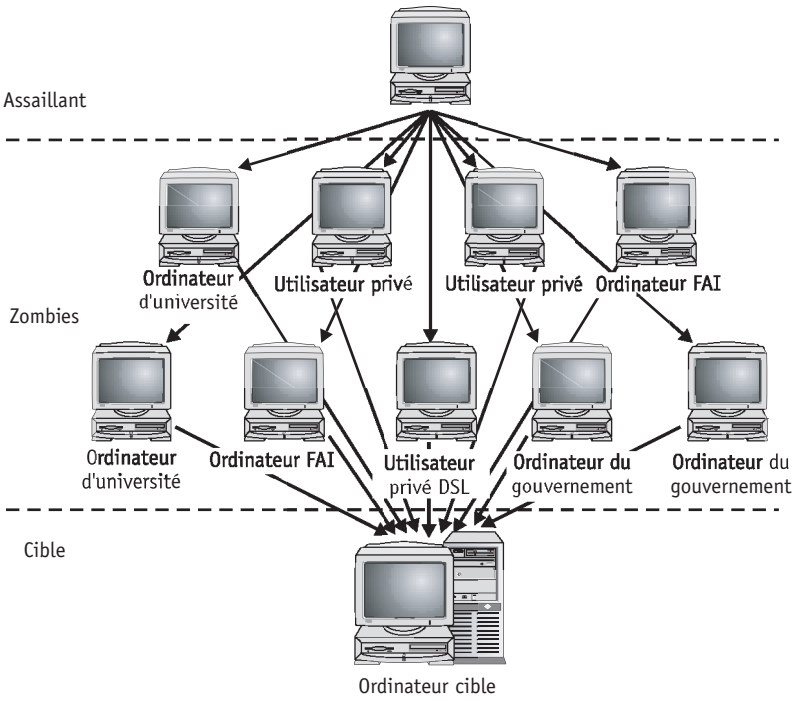
Lors de la sortie de la première édition de ce livre en septembre 1999, le concept de déni de service distribué n'était qu'une simple théorie à l'état de rumeur. Aujourd'hui, l'acronyme DdoS (pour Distributed Denial of Service)fait presque partie du vocabulaire courant. Comme pour les virus étrangleurs qui poussent aussi vite que les mauvaises herbes sur Internet, les médias se sont rués sur les attaques par déni de service distribué. La première attaque massive par déni de service distribué s'est produite en février 2000. Lancée d'abord contre Yahoo!, puis contre E*TRADE, eBay, buy.com, CNN.com et d'autres, elle a bloqué sept sites Web très connus et un nombre incalculable d'autres sites dont nous n'entendrons jamais parler. Nous aimerions pouvoir vous dire que ces attaques émanent d'une équipe experte en piratage qui impose ses caprices aux pauvres utilisateurs Internet, mais cela n'est pas le cas. La vérité est même bien différente.

Les attaques par déni de service distribué se produisent lorsqu'un utilisateur (généralement un adolescent désabusé) se sert d'un logiciel accessible librement pour inonder de paquets le réseau ou l'hôte de destination dans le but d'accaparer ses ressources. Mais, dans le cas d'une attaque par déni de service distribué, la source de l'attaque est multiple. Or, cela implique nécessairement l'infiltration de plusieurs ordinateurs présents sur Internet.

La première opération par déni de service distribué effectuée par un attaquant consiste à obtenir un accès administrateur sur le plus grand nombre possible de systèmes. Cette tâche, qui ne laisse rien présager de bon, est généralement effectuée au moyen d'un script d'attaque personnalisé qui permet d'identifier des systèmes vulnérables éventuels. Nous vous avons déjà expliqué à plusieurs reprises dans ce livre comment un assaillant concevait ces scripts d'attaque. Il vous suffit de consulter vos fichiers journaux et de pare-feu DSL pour comprendre ce qui se passe. Dans le monde entier, les apprentis hackers parcourent ces sous-réseaux anodins à la recherche d'un système mal configuré ou d'un logiciel vulnérable qui leur donnera un accès instantané à l'ordinateur cible.

Une fois l'accès au système obtenu, ils peuvent charger leur logiciel de déni de service distribué et l'exécuter. La plupart des serveurs de déni de service distribué (ou démons) attendent des instructions avant d'attaquer. Les assaillants ont alors tout loisir de charger le logiciel requis sur les hôtes infiltrés, puis d'attendre le moment opportun pour ordonner le lancement de l'attaque. La figure 12.4 présente le déroulement type d'une attaque complète, de l'infiltration de plusieurs systèmes jusqu'à l'assaut final.

Figure 12.4
Une attaque par déni de service distribué.



Le nombre d'outils de déni de service distribué augmente tous les mois ou presque. Nous ne sommes donc pas en mesure de vous fournir une présentation complète et actualisée de ces

outils. C'est pourquoi nous nous contenterons de décrire les plus importants à nos yeux, à savoir TFN (Tribe Flood Network), Trinoo, Stacheldraht, TFN2K et WinTrinoo. D'autres outils tels que Shaft et mStreams sont également à votre disposition, mais ils reposent sur les outils mentionnés ci-dessus. Pour plus d'informations sur mStreams, consultez l'adresse http://staff.washington.edu/dittrich/ddos/mstream.analysis.txt.

Tribe Flood Network (TFN)

Popularité :	*7*
Simplicité :	*5*
Impact :	*9*
Niveau de risque :	***7***

Écrit par un hacker du nom de Mixter (l'un des spécialistes les plus redoutés en matière d'attaques par déni de service), TFN est le premier outil de déni de service distribué à avoir été diffusé publiquement pour UNIX (vous le trouverez principalement sur les systèmes Solaris et Red Hat). TFN possède une composante client et serveur, ce qui permet à un assaillant d'installer le serveur sur un système distant infiltré puis, au moyen d'une simple commande sur le client, de lancer une attaque par déni de service distribué à grande échelle. TFN permet entre autres le lancement d'attaques telles que ICMP, Smurf, UDP et les inondations SYN. Outre ses composantes d'attaque, cet outil comprend un shell root pointant sur un port TCP.

Pour plus de renseignements concernant TFN, consultez l'analyse fournie par Dave Dittrich sur http://staff.washington.edu/dittrich/misc/ddos/.

Parades à TFN

Détection – Un certain nombre de mécanismes de détection de TFN sont disponibles sur Internet. Plusieurs d'entre eux méritent le détour, notamment DDOSPing de Foundstone (http://www.foundstone.com), Zombie Zapper de l'équipe Razor de Bindview (http://razor.bindview.com) et find_ddos (http://www.nipc.gov) du NIPC (National Infrastructure Protection Center).

Prévention – La meilleure défense contre l'utilisation de vos systèmes comme zombies pour ce type d'attaque consiste à éviter les infiltrations dès le départ. Pour cela, il est important de mettre en œuvre toutes les mesures décrites dans le chapitre consacré à UNIX (chapitre 7), c'est-à-dire limiter les services, appliquer les correctifs destinés aux applications et aux systèmes d'exploitation et définir des autorisations d'accès aux fichiers/répertoires (entre autres recommandations).

Pour vous protéger contre TFN, désactivez également tout le trafic ICMP entrant sur votre réseau puisque la communication TFN passe par ICMP. Toujours dans la même optique, vous pouvez appliquer une forme de filtrage de débit à vos routeurs de frontière (par exemple, le filtrage de débit ICMP pour limiter les attaques ICMP et Smurf), c'est-à-dire le filtrage disponible sur le système d'exploitation Cisco IOS 12.0, puis configurer l'option Context Based Access Control (CBAC) dans Cisco IOS 12.0 afin de limiter le risque d'attaques SYN.

Trinoo

Popularité :	*7*
Simplicité :	*5*
Impact :	*9*
Niveau de risque :	***7***

Sur le modèle de TFN, Trinoo fait communiquer un programme de commande à distance (client) et un programme maître qui donne l'ordre aux démons (serveurs) d'attaquer. La communication entre le client et le maître passe par le port TCP 27665 et demande généralement le mot de passe « betaalmostdone ». Les communications du maître vers le serveur se font via le port UDP 27444, et celle des serveurs vers le maître via le port statique UDP 31335.

Parades à Trinoo

Détection – Un certain nombre de mécanismes de détection de Trinoo sont à votre disposition, notamment DDOSPing de Foundstone (http://www.foundstone.com), Zombie Zapper de l'équipe Razor de Bindview (http://razor.bindview.com) et find_ddos (http://www.nipc.gov) du NIPC (National Infrastructure Protection Center).

Prévention – Tout comme pour TFN, la meilleure prévention consiste à éviter l'infiltration de vos systèmes UNIX grâce à la mise en œuvre des mesures de protection décrites dans le chapitre consacré à UNIX (chapitre 7). Pour protéger vos systèmes contre des attaques Trinoo, vous pouvez appliquer une forme de filtrage de débit à vos routeurs de frontière (par exemple, le filtrage de débit ICMP pour limiter les attaques ICMP et Smurf), c'est-à-dire le filtrage disponible sur le système d'exploitation Cisco IOS 12.0, puis configurer l'option Context Based Access Control (CBAC) dans Cisco IOS 12.0 afin de limiter le risque d'attaques SYN.

Stacheldraht

Popularité :	*7*
Simplicité :	*5*
Impact :	*9*
Niveau de risque :	***7***

L'outil Stacheldraht regroupe les fonctions de Trinoo et de TFN dans un outil de destruction riche en fonctionnalités comprenant notamment une session telnet chiffrée entre esclaves et maîtres. L'assaillant peut dorénavant aveugler les systèmes de détection d'instruction de type réseau et mettre en œuvre des capacités de déni de service sans être gêné. À l'instar de TFN, Stacheldraht a recours aux attaques ICMP, UDP, SYN et Smurf. Pour établir une communication entre le client et le serveur, il utilise une combinaison de paquets TCP et ICMP (réponse ECHO).

Le mode de chiffrement appliqué entre le client et le serveur exploite un algorithme de chiffrement symétrique. Une protection par mot de passe par défaut est également proposée par cet outil. Il convient de mentionner la possibilité de mettre à niveau la composante serveur sur demande au moyen de la commande rcp.

Pour plus de détails concernant Stacheldraht, consultez l'analyse proposée par Dave Dittrich et disponible sur http://staff.washington.edu/dittrich/misc/ddos/.

Parades à Stacheldraht

Détection – Un certain nombre de mécanismes de détection de Stacheldraht sont à votre disposition, notamment DDOSPing de Foundstone (http://www.foundstone.com), Zombie Zapper de l'équipe Razor de Bindview (http://razor.bindview.com) et find_ddos (http://www.nipc.gov) du NIPC (National Infrastructure Protection Center).

Prévention – Comme pour les outils de déni de service distribué présentés précédemment, la meilleure défense contre Stacheldraht est d'empêcher vos systèmes de devenir des zombies. Pour cela, il suffit de mettre en œuvre toutes les mesures décrites dans le chapitre consacré à UNIX (chapitre 7), c'est-à-dire limiter les services, appliquer les correctifs destinés aux applications et aux systèmes d'exploitation et définir des autorisations d'accès aux fichiers/répertoires (entre autres recommandations). En outre, vous disposez d'une mesure préventive supplémentaire contre Stacheldraht : la désactivation de tout le trafic ICMP entrant sur votre réseau, puisque la communication TFN passe par ICMP.

Pour protéger vos systèmes contre les attaques Stacheldraht, vous pouvez appliquer une forme de filtrage de débit à vos routeurs de frontière (par exemple, le filtrage de débit ICMP pour limiter les attaques ICMP et Smurf), c'est-à-dire le filtrage disponible sur le système d'exploitation Cisco IOS 12.0, puis configurer l'option CBAC (Context Based Access Control) dans Cisco IOS 12.0 afin de limiter le risque d'attaques SYN.

TFN2K

Popularité :	*8*
Simplicité :	*5*
Impact :	*9*
Niveau de risque :	***7***

L'outil TFN2K, c'est-à-dire TFN 2000, succède à TFN. Cet outil de déni de service distribué est bien meilleur que son prédécesseur. Il permet d'organiser de façon aléatoire les communications sur les ports (pour contrer la parade du blocage de port aux routeurs de frontière) et de chiffrer les communications (pour contrer la parade IDS de réseau comme moyen de détection). Comme son prédécesseur, TFN2K peut lancer des attaques SYN, UDP, ICMP et Smurf. Il peut également passer de manière aléatoire d'un mode d'attaque à un autre. Toutefois, à la différence de Stracheldraht, TFN2K utilise un mode de chiffrement plus faible portant le nom de codage Base-64.

Jason Barlow et Woody Thrower d'AXENT Security Team ont analysé TFN2K de manière approfondie ; leur étude est disponible sur http://www.packetstormsecurity.net.

Parades à TFN2K

Détection – Un certain nombre de mécanismes de détection de TFN2K sont à votre disposition, notamment Zombie Zapper de l'équipe Razor de Bindview (http://razor.bindview.com) et find_ddos (http://www.nipc.gov) du NIPC (National Infrastructure Protection Center).

Prévention – Comme pour les outils de déni de service distribué présentés précédemment, la meilleure défense contre TFN2K est d'empêcher vos systèmes de devenir des zombies. Pour cela, vous devez mettre en oeuvre toutes les mesures décrites dans le chapitre consacré à UNIX (chapitre 7), c'est-à-dire limiter les services, appliquer les correctifs destinés aux applications et aux systèmes d'exploitation et définir des autorisations d'accès aux fichiers/répertoires (entre autres recommandations).

Pour protéger vos systèmes contre des attaques TFN2K, vous pouvez appliquer une forme de filtrage de débit sur vos routeurs de frontière (par exemple, le filtrage de débit ICMP pour limiter les attaques ICMP et Smurf), c'est-à-dire le filtrage disponible sur le système d'exploitation Cisco IOS 12.0, puis configurer l'option Context Based Access Control (CBAC) dans Cisco IOS 12.0 afin de limiter le risque d'attaques SYN.

WinTrinoo

Popularité :	*5*
Simplicité :	*5*
Impact :	*9*
Niveau de risque :	***6***

WinTrinoo a été présenté au grand public pour la première fois par l'équipe Razor de Bindview. Il s'agit de la version Windows de Trinoo qui a pratiquement toutes les capacités de son aîné. Cet outil est un cheval de Troie généralement appelé service.exe (s'il n'a pas été renommé) ; il pèse 23 145 octets. Une fois le fichier exécutable lancé, il ajoute une valeur à la clé Run du registreWindows pour autoriser son redémarrage chaque fois que l'ordinateur est relancé :

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
System Services: REG_SZ: service.exe
```

INFO Ne confondez pas le fichier service.exe de WinTrinoo et le fichier services.exe (au pluriel).

Bien entendu, cette valeur est exécutée uniquement si le fichier service.exe se trouve sur le chemin d'accès de commandes externes de la cible. WinTrinoo écoute à la fois les ports TCP et UDP 34555.

Parades à WinTrinoo

Pour détecter WinTrinoo, vous pouvez rechercher sur le réseau le port TCP ou UDP 34555 ouvert ou un fichier nommé service.exe (en sachant qu'il a pu être renommé) dont la taille est de 23 145 octets. Outre cette technique manuelle, vous pouvez installer un programme antivirus tel que Norton Antivirus de Symantec qui mettra automatiquement en quarantaine ce fichier avant son exécution.

Attaques par déni de service locales

Bien que seules les attaques par déni de service à distance aient le droit aux gros titres, les attaques locales sont tout aussi destructrices. De nombreux systèmes multiutilisateurs sont victimes du lancement d'une attaque par déni de service non autorisée effectué par un utilisateur autorisé. La plupart de ces attaques utilisent les ressources système ou exploitent les défauts des programmes existants pour refuser l'accès à des utilisateurs légitimes. Bien qu'il existe des centaines d'attaques locales par déni de service pour les systèmes UNIX et Windows, nous allons nous concentrer uniquement sur les attaques par épuisement des ressources et les erreurs de programmation, respectivement sous Windows et UNIX.

Terminal Server de Windows NT 4.0 et proquota.exe

Popularité :	*2*
Simplicité :	*4*
Impact :	*7*
Niveau de risque :	***4***

L'utilisation de l'espace disque disponible par dépassement des quotas imposés est un exemple classique d'attaque par épuisement des ressources. Bien que la fonction de quota de disque soit utilisée depuis un certain temps déjà dans le monde UNIX, elle est relativement nouvelle dans le monde Windows NT. Sur Terminal Server Edition SP4 de Windows NT, un utilisateur ordinaire peut tirer parti de la fonctionnalité de quota de disque Windows NT pour saturer %systemdrive%. Cette opération permet de refuser l'accès au système à tous les utilisateurs ne possédant pas des copies locales de leur profil. Dans ce type d'attaque, les utilisateurs ne devraient pas être autorisés à se déconnecter du système s'ils ont dépassé leur quota. Toutefois, ils peuvent tuer le processus proquota.exe pour contourner cette interdiction et se déconnecter ensuite. Il est possible de tuer proquota.exe parce que ce processus appartient à l'utilisateur et non au compte système.

Parade à Terminal Server de Windows NT 4.0 et proquota.exe

En matière de sécurité, il est fortement conseillé de placer les fichiers système et les données utilisateurs sur deux partitions différentes. Ce principe vaut également dans le cas présent. Le fichier %systemdrive% doit en principe se trouver sur une partition distincte de celle où se trouvent les fichiers accessibles par l'utilisateur. Nous vous conseillons en outre de placer les

profils sur une partition non amorçable (non bootable) du système et de les utiliser uniquement en cas de besoin.

Panique noyau

Popularité :	*2*
Simplicité :	*1*
Impact :	*7*
Niveau de risque :	***3***

La version noyau 2.2.0 de Linux contient une condition de déni de service potentielle lorsque ldd, un programme permettant d'afficher les bibliothèques utilisées d'une liste donnée de fichiers, est employé pour certains fichiers centraux. Cette vulnérabilité est liée à l'appel de fonction munmap() auquel ldd a recours et qui établit ou supprime des projections mémoire des fichiers ou périphériques. Dans des situations données, munmap() écrase les zones critiques de la mémoire noyau et provoque la panique dans le système, puis un redémarrage. Si cette vulnérabilité n'a rien d'extraordinaire en tant que tel, elle illustre parfaitement le concept d' attaque par déni de service contre le noyau. Dans la plupart des cas, un utilisateur non autorisé peut exploiter un défaut de programmation pour corrompre une zone critique de la mémoire utilisée par le noyau. Ce qui entraîne presque toujours une panique au niveau du noyau.

Parade à la panique noyau

Un correctif de noyau permettant de résoudre ce problème a été intégré à la version 2.2.1. Si le code source est fermé et propriétaire, vous êtes relativement démuni pour vous assurer que le système d'exploitation et ses composants, tels que le noyau, sont exempts de toute erreur de programmation. En revanche, pour les nombreuses versions libres d'UNIX, il est possible de chercher dans le code source les défauts de programmation et les vulnérabilités liées à la sécurité.

En résumé…

Comme nous venons de le voir, les utilisateurs malveillants ont à leur disposition un large éventail d'attaques par déni de service susceptibles d'interrompre les services. Les attaques par saturation de bande passante sont très en vogue car elles permettent d'amplifier de petites quantités de trafic jusqu'à des niveaux dommageables. Les attaques par épuisement de ressources font rage depuis de nombreuses années et certains pirates continuent à les utiliser avec beaucoup de succès. Les défauts de programmation sont l'une des armes privilégiées des pirates dans la mesure où la complexité d'implémentation des piles IP et des programmes associés ne cesse de croître. Enfin, les attaques par routage et DNS sont extrêmement efficaces pour exploiter des vulnérabilités inhérentes aux services critiques à la base d'une grande partie d'Internet. En fait, certains experts en sécurité estiment qu'il est possible de lancer une attaque par déni de service contre le réseau Internet lui-même en manipulant des informations

de routage via le protocole BGP (Border Gateway Protocol) qui est largement utilisé par la plupart des fournisseurs de réseau fédérateur Internet.

Les attaques par déni de service distribué progressent également : les assaillants peuvent se procurer les outils aisément et n'ont pas besoin de grandes connaissances techniques pour les exécuter. Ces attaques comptent parmi les plus dévastatrices dans la mesure où elles peuvent rapidement consommer les ressources des hôtes les plus importants d'Internet et les rendre inopérants.

Avec la progression du commerce électronique, les attaques par déni de service ont un impact croissant sur l'activité économique des entreprises. L'aspect furtif de la plupart de ces attaques est encore plus inquiétant car il leur permet de passer totalement inaperçues. N'oublions pas, enfin, les conséquences des attaques par déni de service utilisées à des fins militaires. De nombreux gouvernements possèdent ou sont en train de mettre en place des dispositifs de guerre électronique qui exploiteront les attaques par déni de service à la place des missiles conventionnels. Bienvenue dans l'ère du cyberterrorisme.