Dossier

Protection réseaux grâce aux puits stationnaires et aux puits IP basés sur les évènements

Victor Oppleman 

Degré de difficulté

Rien n'est plus efficace que la présentation, même succincte, des techniques de protection des réseaux afin de mieux se défendre contre les attaques de déni de service ou attaques DoS. Nous vous présentons la technique connue sous le no sinkhole permettant d'obtenir les informations intéressantes sur les menaces auxquelles est confronté votre réseau.

La technique des puits a été déployée par les fournisseurs d'accès à Internet de manière générale afin de protéger leurs clients finaux. Comme nous allons l'expliquer dans le présent article, cette technique, connue sous le nom de puits ou sinkhole en anglais, permet également d'obtenir des informations intéressantes sur les menaces auxquelles est confronté votre réseau. En implémentant des puits, vous ajoutez une protection supplémentaire à votre réseau tout en pouvant glaner des informations sur les menaces et certaines erreurs évidentes de configuration présentes dans votre réseau.

Destiné principalement aux utilisateurs de réseaux savvy, le présent article présentera les éléments suivants :

- Contexte et fonction des puits : brève explication des puits IP et de leur installation réussie par un certain nombre d'organisations.
- Déploiement de réseaux leurres : application des techniques de puits au moyen de réseaux invisibles et de réseaux de pots de miel, afin de piéger et d'analyser des scans malveillants, des tentatives d'infiltration, ainsi que d'autres évènements liés à la surveillance de votre réseau comme la détection d'intrusions.
- Protection contre les attaque de type DoS : comment certaines organisations et leurs fournisseurs d'accès à Internet ont développé un moyen de protection contre le déni de service au moyen de déploiements extensifs et basés sur les évènements.
- Rétrodiffusion et pisteurs : brève explication de la rétrodiffusion et de l'utilisation du pistage afin d'identifier le point d'entrée des attaques DoS dans un réseau important.

Cet article explique...

- Comment utiliser les techniques de puits (sinkhole en anglais) afin de se protéger contre les attaques de type DoS.

Ce qu'il faut savoir...

- Maîtriser le fonctionnement des attaques DoS.
- Connaître les problèmes liés au trafic des réseaux du côté des Fournisseurs d'Accès à Internet (abrégés ci-après en FAI).

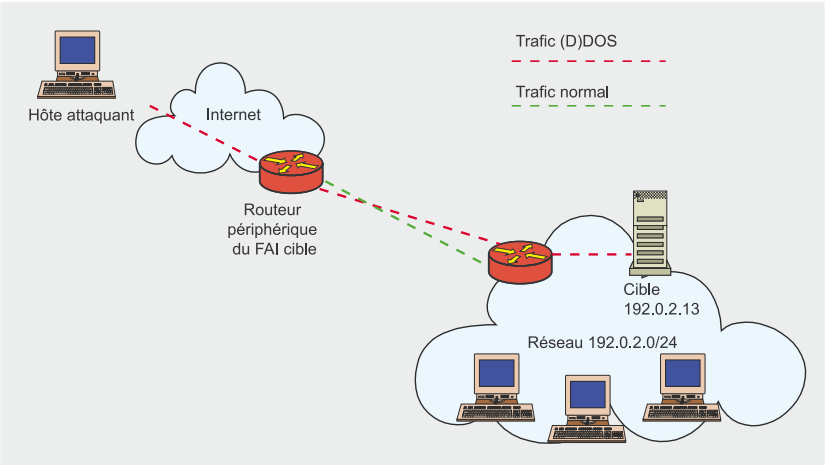

Figure 1. *Attaque sur l'adresse IP 192.0.2.13 (avant installation du puits)*

Contexte et fonction

Tout au long de cet article, le terme puits désignera un moyen généralisé de rediriger un trafic réseau IP spécifique dans différents buts sécuritaires dont l'analyse et l'expertise, la diversion des attaques, et la détection d'activités anormales. Les FAI tier-1 ont été les premiers à installer ce type de tactiques, afin de protéger leurs clients finaux contre les attaques. Depuis, les techniques ont été adaptées afin de collecter des informations intéressantes sur les menaces à des fins d'analyse sécuritaire. Afin de vous faire une idée de la forme la plus simple que peut revêtir un puits, nous prendrons l'exemple suivant.

Un trafic malveillant et dérangeant issu de divers réseaux est destiné au réseau 192.0.2.13, comme l'illustre la Figure 1. L'organisation ciblée par ce trafic utilise 192.0.2.0/24 en tant que bloc d'adresse de son réseau, lequel est acheminé par son FAI en amont. Cette attaque devient rapidement dangereuse en interrompant les activités de l'organisation ciblée et en augmentant considérablement ses coûts en raison d'une utilisation de la bande passante plus importante que de coutume. Le FAI est ainsi contraint au vu du trafic surchargé généré par l'attaque susceptible de déranger des clients adjacents sous forme de dommage collatéral.

Le FAI réagit en initiant temporairement un puits de type trou noir. Il injecte pour ce faire un chemin de cible plus spécifique (192.0.2.13/32) dans son ossature, dont l'attribut next-hop est une interface de suppression sur le routeur périphérique (également connu sous le nom de null0 ou *bit bucket*), comme l'illustre la Figure 2.

Cette tactique permet de rediriger le trafic malveillant vers le puits du FAI sans lui permettre d'atteindre sa cible originale. Ainsi, le temps que le puits entre en action, les clients adjacents du FAI ne seront probablement pas touchés par des dommages collatéraux (dans la mesure où le FAI aura prévu de concevoir ses propres puits de défense), la cible visée par l'attaque aura retrouvé sa connexion Internet et son accès local au dispositif spécifiquement ciblé. Malheureusement, une adresse (ou un dispositif) IP plus spécifique attaquée ne peut entrer en relation avec aucun système à distance sous Internet à moins de supprimer le puits (à priori une fois l'attaque éloignée). De toutes évidences, il est possible d'envoyer les services fournis originellement par le dispositif cible vers un autre dispositif sous une adresse IP différente, mais de nombreuses autres considérations doivent également être prises en compte en termes de délai d'expiration DNS TTL, et ainsi de suite.

Cet exemple décrit simplement un type de puits possible, généralement décrit comme un chemin menant vers un trou noir généré par le FAI. Vous voilà donc familiarisé avec le concept. Nous pouvons donc vous présenter divers autres usages des puits.

Utiliser les puits pour déployer des réseaux leurres

Une utilisation bien plus innovante des puits consiste à déployer diverses sortes de réseaux leurres dans le but de piéger, d'exposer ou de rassembler des informations sur les attaques.

Leurre ou Decoy en anglais \De*coy"\, n. : tout dispositif destiné à conduire dans des rets ; leurre censé tromper et induire en erreur sur le véritable danger, ou la puissance de l'ennemi ; appât.

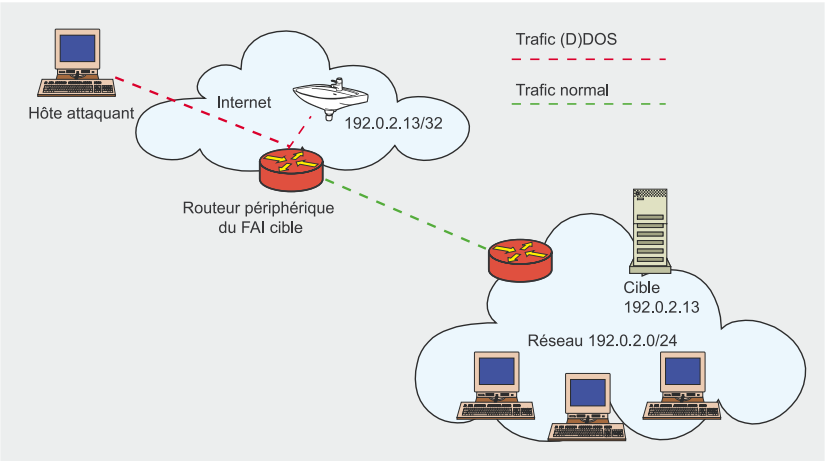

Figure 2. *Attaque de l'adresse IP 192.0.2.13 (avec mécanisme de protection du puits)*

Listing 1. *Extrait de la configuration du protocole BGP*

```
router bgp XXX
redistribute static route-map static-to-bgp
# La carte des chemins est un mécanisme stratégique
# permettant de modifier les attributs des préfixes, ou certaines
# politiques particulières de filtrage
route-map static-to-bgp permit 10
match tag 199
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export
set origin igp
```

Listing 2. *Configuration de base du côté des fournisseurs d'accès à Internet*

```
router bgp XXX
# La carte des chemins est un mécanisme stratégique permettant de
# manipuler des informations sur le routage telles que
# le paramétrage de l'attribut next-hop
neighbor < customer-ip > route-map customer-in in
# La liste des préfixes est une liste statique de préfixes clients et de
longueur de masques autorisés.
# Les clients doivent pouvoir indiquer à un seul hôte leur(s) préfixe(s)
comme
# 172.16.0.1/32, par exemple.
neighbor < customer-ip > prefix-list 10 in
# ebgp-multihop est nécessaire car il permet d'éviter
# l'annonce continuelle de préfixes ainsi que leur
# retrait.
neighbor < customer-ip > ebgp-multihop 2
# Nous définissons désormais la carte des chemins pour la correspondance
entre politiques
# et paramétrons l'attribut next-hop des trous noirs.
route-map in-customer permit 5
# Le client règle cette communauté de son côté,
# et le FAI la fait corréler de son côté.
# XXXX représentera un client ASN,
# et NNNN un nombre arbitraire approuvé par
# le FAI et le client.
match ip community XXXX:NNNN
set ip next-hop < blackhole-ip>
set community additive no-export
```

Nous allons présenter plus en détails deux types de réseaux leurres : le réseau invisible et le réseau de pots de miel. Ces deux types de réseaux peuvent être utilisés pour glaner des informations sensibles, mais l'un d'entre eux est plus particulièrement utile dans le domaine des réseaux sécurisés.

Déployer des réseaux invisibles

En règle générale, un réseau invisible désigne une partie d'espace IP acheminée et allouée, complètement dépourvue de service sensible. De tels réseaux sont considérés comme “invisibles” en raison de l'apparente *obscurité* qui y règne. Toutefois, un réseau invisible comprend en réalité un serveur, agissant comme un aspirateur de paquets. Ce serveur se charge de rassembler et d'organiser les paquets entrant dans le réseau invisible, et se révèle ainsi très utile pour des analyses en temps réel ou des expertises de réseaux post-évènements.

Il faut en effet savoir que l'intrusion de paquets dans un réseau invisible est a priori inattendue, dans la mesure où aucun paquet légitime ne doit apparaître dans un réseau invisible. Donc, les paquets qui s'y retrouvent sont arrivés soit par erreur de configuration, soit, et c'est le plus fréquent, par un scénario envoyé par malveillance. Ce programme malveillant, à la recherche de dispositifs vulnérables, va envoyer des paquets dans le réseau invisible, et s'exposer ainsi au contrôle de sécurité administrative. Assez géniale, cette approche permet de détecter des vers ainsi que d'autres programmes malveillants. Exception faite des fausses alertes, des signatures et des dispositifs d'analyses statistiques complexes, tout administrateur de la sécurité ayant correctement déployé des réseaux invisibles pourra détecter des scans malveillants (tentatives lancée par un programme malveillant dans le but de découvrir des hôtes adjacents candidats à la propagation) quelle que soit la taille du réseau. Il s'agit là d'un outil de sécurité réellement puissant. Par ailleurs, les paquets introduits dans le réseau invisible révèlent également des erreurs anodines de configuration dans le réseau dont les administrateurs réseau apprécieront de se débarrasser. Bien évidemment, les réseaux invisibles multiplient les usages dans le domaine de la sécurité. Ils peuvent ainsi être utilisés pour héberger des collecteurs de flux de données, des détecteurs de rétrodiffusion, des renifleurs de paquets, et des systèmes de détection d'intrusion. L'avantage du réseau invisible est qu'il permet de réduire considérablement le nombre de fausses alertes au moyen d'une simple diminution du trafic et ce, quel que soit le dispositif ou la technologie utilisée.

L'installation d'un réseau invisible est relativement simple. Il suffit en réalité de suivre cinq étapes fondamentales.

Commencez par sélectionner une ou plusieurs régions inutilisées dans l'espace de votre adresse IP à partir de votre réseau que vous acheminerez ensuite vers le réseau invisible. Il peut s'agir d'un préfixe /16 ou plus d'adresses, ou tous

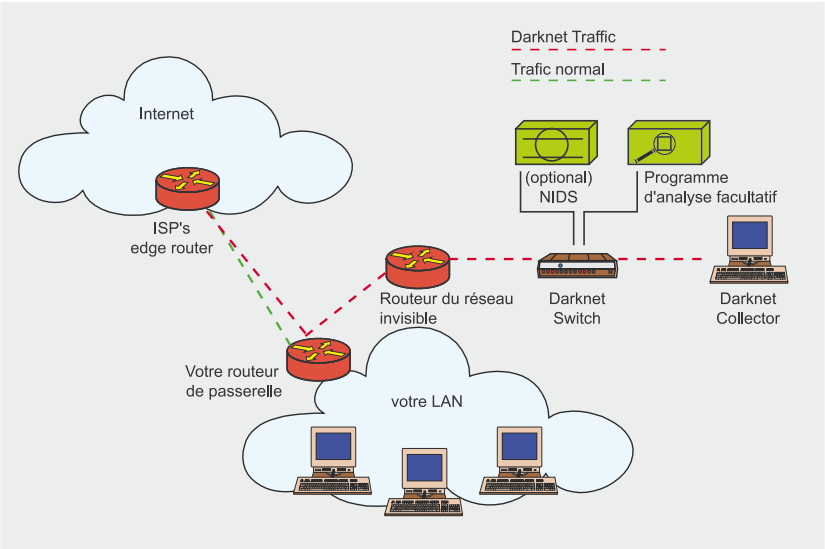

Figure 3. *Topologie physique de référence pour les réseaux invisibles*

les chemins menant à une seule adresse (/32). Plus vous sélectionnez d'adresses, plus la détection d'activités réseau non sollicitées sera pertinente d'un point de vue statistique. Il est recommandé de choisir plusieurs segments d'adresses, comme un /29 de chacun des réseaux internes à votre disposition, et un /25 de votre allocation de réseau public (externe), par exemple. Rien ne vous empêche non plus de rendre invisible une région de votre espace interne d'adresses privées (comme par exemple, l'espace RFC 1918, 10.0.0.0/8, etc.). En sélectionnant des régions de votre réseau interne pour les rendre invisibles, vous serez capable de détecter des scans internes qui vous auraient échappé si seuls des segments de votre réseau externe (public) avaient été acheminés vers votre réseau invisible. Les organisations utilisant des routages particuliers pour leurs réseaux internes peuvent envisager une autre stratégie fondée sur la règle *du chemin le plus spécifique* (généralement distribué selon certains protocoles de passerelles intérieures). Ainsi, si vous utilisez les réseaux 10.1.1.0/24 et 10.2.1.0/24 de manière interne, vous pouvez tout simplement acheminer le réseau 10.0.0.0/8 entier vers votre réseau invisible. Si votre réseau est correctement configuré, votre réseau invisible recevra tout le trafic de 10.0.0.0/8 exception faite des réseaux que vous utilisez/acheminez de manière spécifique (ces derniers sont probablement dotés d'entrées de routage statiques dans votre infrastructure de réseau).

Il faut ensuite configurer la topologie physique de votre réseau invisible. Pour ce faire, il vous faudra un routeur ou un commutateur (couche 3) chargé de transférer le trafic vers votre réseau invisible, un serveur à grande capacité de stockage pour collecter vos données, et un commutateur Ethernet afin de connecter ces composants ainsi que des composants facultatifs ultérieurement comme un capteur IDS (système de détection d'intrusion) ou un analyseur de protocole. Il est recommandé de choisir pour le routeur un dispositif de passerelle existant interne ou externe (ou les deux à la fois, bien que cette solution reste à éviter). La plupart des réseaux invisibles “entreprise” (par opposition à ceux relevant du domaine des télécommunications) sont situés dans une des zones tampon ou DMZ de l'organisation et séparés du reste du réseau. C'est la raison pour laquelle vous devez utiliser un pare feu pour réaliser cette tâche à la place de l'un de vos routeurs. Il est, toutefois, recommandé d'utiliser un routeur de passerelle externe pour vos réseaux invisibles externes, et un commutateur interne de couche 3 pour vos réseaux invisibles internes. Quel que soit votre choix, l'essentiel est de configurer ce dispositif de routage de manière à ce qu'il transfère le trafic destiné au réseau invisible reçu en dehors d'une interface Ethernet de réseau invisible (grâce au commutateur) vers le serveur collecteur configuré pour accepter de tels paquets. Le serveur collecteur doit également être doté d'une interface spécifique de réseau invisible chargée de recevoir ces paquets. Au niveau de sa gestion, le serveur collecteur nécessitera également au moins une interface Ethernet supplémentaire (à placer sur un LAN de gestion indépendant). Veillez à bien respecter les consignes de sécurité édictées pour tous les dispositifs de votre réseau, car vous pouvez être sûr que toutes sortes de programmes malveillants s'engouffreront très rapidement dans ce segment de réseau. Vous pouvez utilisez un commutateur de zone DMZ existant afin de connecter ces composants, à moins que la configuration du VLAN ne vous effraie nullement. Ainsi, aucun paquet largement diffusé n'entrera dans le réseau invisible. N'oubliez pas qu'un réseau invisible est conçu pour piéger le trafic illégitime sans prendre le risque de voir les paquets légitimes de vos autres LAN empiéter sur la zone de votre réseau invisible. Nous avons exposé dans la Figure 3 un exemple de cette configuration. Dans les exemples suivants, nous utiliserons un routeur ou un commutateur chargés de faire fonctionner Cisco IOS avec une licence logicielle de couche 3, un serveur basé sur FreeBSD, et un commutateur d'objets non gérés de couche 2 chargé de connecter les dispositifs.

Afin que votre serveur collecteur évite d'avoir recours au protocole ARP (Address Resolution Protocol) sur chaque adresse de votre espace de réseau invisible, il vous faut configurer le routeur de manière à transférer le trafic destiné au réseau invisible vers une seule adresse IP

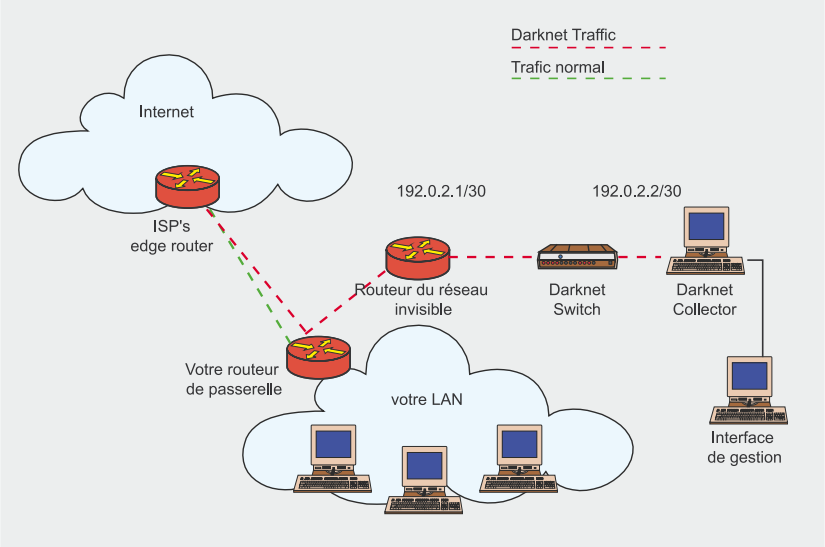

Figure 4. *Topologie logique de référence pour les réseaux invisibles*

finale sur l'interface Ethernet du réseau invisible de votre serveur. Pour ce faire, il est recommandé de consacrer un réseau /30 à ce transfert point par point entre le routeur et l'interface du réseau invisible, comme 192.0.2.0/30, par exemple. Ainsi, l'interface Ethernet de votre routeur prendra l'adresse 192.0.2.1/30 et le serveur collecteur pourra être atteint via 192.0.2.2/30. La configuration de l'interface dépend dans une large mesure des plate-formes sélectionnées. Nous supposerons donc que vous maîtrisez parfaitement ce sujet. Nous utiliserons dans les exemples Cisco IOS avec une licence logicielle de couche 3. Une fois cette tâche réalisée, il vous suffit d'entrer les déclaration de routage correctes dans le commutateur afin de transférer l'ensemble du trafic de votre réseau invisible vers 192.0.2.2 dans le serveur collecteur, et de libérer votre espace personnel, de la manière suivante :

```
router#conf t
router(config)# ip route 10.0.0.0 ←
255.0.0.0 192.0.2.2
router(config)# ^Z
router# wr
```

Vous devriez ainsi recevoir le trafic du réseau invisible. Nous avons exposé dans la Figure 4 une topologie logique de référence.

Que faire de ce trafic une fois obtenu. Le serveur doit être configuré de manière à ne pas répondre à toutes les données qu'il reçoit sur son interface de réseau invisible. Bien évidemment, le serveur utilisera le protocole ARP pour son adresse configurée (192.0.2.2/30 uniquement) afin d'établir les communications nécessaires vers le routeur. En revanche, tous les autres paquets doivent être supprimés au moyen de pares feu basés sur l'hôte. Comme nous l'avons mentionné plus haut, aucune sorte de gestion ne doit apparaître sur l'interface du réseau invisible. Vous devez configurer une autre interface Ethernet sur laquelle seront réalisées les tâches de gestion et d'administration. Le chemin par défaut menant vers le système doit être la passerelle vers l'interface de gestion. Le choix du pare feu nécessaire dépendra de la plate-forme que vous aurez sélectionnée pour votre serveur. Il est, toutefois, recommandé d'utiliser un système basé sur BSD et pf ou ipfw2 en tant que pare feu. Qu'il soit activé ou pas le journal du pare feu dépendra largement de l'utilisation que vous en ferez. Dans nos exemples, nous utilisons des outils d'analyse de fichier journal nécessitant d'être activés (de manière à pouvoir analyser les journaux et générer des alertes si nécessaire). Toutefois, selon les différents choix de matériel et de logiciel ainsi que la taille de votre réseau invisible, l'activation du journal peut diminuer considérablement la performance de votre réseau invisible. Afin de compléter vos mesures de sécurité (les pares feu ne sont pas à l'abri de panne ou de déconnexion accidentelle), il peut s'avérer judicieux de transférer le trafic de votre réseau invisible vers une destination vide dans le cas où ce trafic passerait accidentellement sans avoir été préalablement filtré. Un tel exemple sous FreeBSD ressemblerait à ceci :

```
route add -net 10.0.0.0/8 ←
127.0.0.1 -blackhole
```

Votre réseau invisible est désormais fonctionnel et votre serveur collecteur protégé. Il vous reste à stocker les données dans un format lisible par vos outils d'analyse et d'expertise. Des fichiers formatés en pcap semblent assez évidents en raison de leur quasi universalité sur la plupart des applications d'analyse réseau pouvant travailler dessus. La méthode la plus simple et la plus répandue consiste à utiliser la fonctionnalité intégrée de pivotement du programme tcpdump proposé par le Groupe de Recherches en Réseaux du Laboratoire National Lawrence Berkeley. Afin de lancer la fonctionnalité de pivotement de journal en ligne de commande tcpdump, vous pouvez par exemple taper la déclaration suivante :

```
tcpdump -i en0 -n -w darknet_dump -C125
```

Dans cet exemple, nous ordonnons au programme tcpdump d'écouter l'interface en0. La résolution nom à nombre (DNS) est désactivée, et un fichier intitulé darknet_dumpN est rédigé tous les 125 millions d'octets, où chaque augmentation de N rend le nom des fichiers uniques. Là encore, cette commande produira un fichier binaire formaté en pcap contenant le trafic du réseau invisible. Vous pouvez ensuite entrer ledit fichier dans votre logiciel d'analyse de réseau préféré, avec pour objectif de

conserver une copie des données et d'utiliser un grand nombre d'outils différents chargés de relire les fichiers ultérieurement à la recherche de caractéristiques pertinentes du trafic analysé. La règle générale veut que vous utilisiez un programme de type tcpdump combiné à une expression spécifique BPF (Berkeley Packet Filter, ou filtre de paquets de Berkeley) afin de détecter des éléments dans ces fichiers. Comme cette tâche peut être lancée au moment de l'exécution (ou de la capture), en conservant un enregistrement de l'ensemble du trafic, vous pouvez utiliser différents outils ultérieurement sans prendre le risque de perdre des informations de grande importance.

Argus (Audit Record Generation and Utilization System) pour les réseaux développé par Qosient est un autre outil très utile capable de simplifier la visualisation des flux de données relatives au trafic. Bien que nous puissions exposé ici en détail la configuration complexe de cet outil, nous utilisons Argus régulièrement afin de détecter des flux de données intéressants dans nos réseaux invisibles. Argus propose une interface de résumé des flux de données agréable censée vous aider à comprendre exactement ce qui se passe en termes de trafics malveillants.

Afin de pouvoir visualiser le volume de trafic entrant dans votre réseau invisible, des outils de compteur d'interface comme MRTG (veuillez consulter le site *http://www.mrtg.org/*) de Tobias Oetiker devraient vous aider. MRTG vous permet de produire des graphiques lisibles du trafic de votre réseau invisible relativement illisible. Il existe également une douzaine d'autres outils capables d'analyser les journaux des pares feu, pouvant remplacer rapidement et facilement les outils d'analyse plus complexes basés sur le format pcap ou Argus. Il ne faut pas ignorer les problèmes que soulèvent les journaux du filtre des paquets au format texte et l'analyse supplémentaire que de tels fichiers exigent.

Vous pouvez utiliser au bas mot des douzaines d'outils sur votre réseau invisible. Pour commencer, vous trouverez ci-après une liste de certains de nos outils :

- Capteur IDS (Bro, Snort, et al.).
- Renifleur de paquet (tcpdump tel que décrit plus haut).
- Programme d'analyse des flux de données (Argus, exportations des flux du réseau à partir du routeur, SiLK, outils de flux de données).
- Analyseur des fichiers journal de pare feu venant alimenter les bases de données RRD pour les graphiques.
- MRTG afin de représenter les compteurs de trafic sous forme de graphiques.
- p0f (par Michal Zalewski) afin de classer les plate-formes de dispositifs infectés ou servant à réaliser des scans malveillants.

Déployer des réseaux de pots de miel

À l'instar d'un réseau invisible, un réseau de pots de miel désigne en général une partie d'espace IP acheminée et allouée. Toutefois, au lieu de fournir une destination vers laquelle les paquets vont s'échouer, ici la destination imite un service réel (ou plusieurs services), afin de permettre la connexion (poignée de mains), et d'établir un dialogue à deux sens. Un pot de miel ou *honeypot* en anglais, soit le système chargé d'imiter un service réel, désigne en réalité une ressource étroitement et régulièrement contrôlée destinée à tromper les programmes malveillants afin de les infiltrer et de les examiner. Quoique de différents types, l'objectif des pots de miel reste toujours le même : apprendre les tactiques et recueillir autant d'informations que possible sur le programme malveillant.

Pots de miel physiques

Sont désignées par pots de miel physiques d'importantes machines résidant dans le réseau de pots de miel et dotées de leur propre adresse IP, de leur propre système d'exploitation et de leurs propres outils d'imitation de services.

Pots de miel virtuels

Sont désignés par pots de miel virtuels des systèmes complets de pots de miel “sur le modèle logiciel” chargés de reproduire des conditions environnementales comme le système d'exploitation, la pile du réseau et les services fournis sous forme de leurres. Un serveur physique peut proposer un réseau de milliers de pots de miel virtuels.

Pots de miel à basse interaction

Les pots de miels dits à basse interaction (type le plus répandu de pots de miel aujourd'hui) ont été conçus afin de tromper les programmes malveillants au moyen d'une ou plusieurs vulnérabilités supposées exploitables, d'établir avec ces programmes un dialogue, et de capturer les tout premiers paquets de communication avec le programme malveillant. De toutes évidences, le programme malveillant ou le logiciel malicieux autonome en conversation avec le pot de miel se rendra compte que sa cible ne peut être exploitée, mais avant de s'en apercevoir réellement, des informations de grande importance peuvent déjà être exposées, comme la tactique d'exploitation ou la signature du logiciel malveillant. De tels pots de miel à basse interaction sont de nos jours utilisés afin de modéliser les tactiques d'attaque des polluposteurs (qui tentent de dériver les heuristiques comme les caractéristiques temporelles des transactions SMTP des polluposteurs, par exemple).

Il n'existe que très peu d'installations commerciales de cette technologie liée aux pots de miel, mais la plupart des implémentations les plus utilisées sont disponibles via un projet libre intitulé honeyd, dirigé par Niels Provos. Vous trouverez plus d'amples informations sur l'obtention et la configuration d'honeyd à l'adresse suivante : *http://www.honeyd.org*.

Astuce : honeyd a été conçu sous forme de pot de miel/ réseau de pots de miel virtuel capable de simuler un certain nombre de

En vente dès mois de juillet !

www.phpsolmag.org/fr

Également disponible sur **http://buyitpress.com/fr**

systèmes d'exploitation différents ainsi que des composants logiciels permettant d'attirer les programmes malveillants.

Il faut également noter une nouvelle forme de pots de miel à basse interaction fondée sur un nouveau concept élaboré par Tom Liston intitulé LaBrea. LaBrea (ainsi désigné après la fonctionnalité tar pit) est un démon logiciel (service) capable de générer des réponses autonomes à des requêtes de connexion au travers de blocs d'adresses IP éventuellement considérable. En bref, cet outil peut créer un environnement capable d'attirer des programmes malveillants de scan et/ou de propagation, mais présente toutefois un grave inconvénient. Dès que le programme malveillant tente de se connecter, LaBrea ralentit la pile réseau de l'émetteur, de manière parfois significative. Au sens figuré, la pile réseau du système infecté par le programme malveillant se retrouve coincée dans un tar pit. De ce fait, il n'y a plus d'interaction au niveau de la couche application, mais une interaction significative au niveau de la couche 4 lors des tentatives de connexion (TCP). LaBrea est même capable d'utiliser le protocole ARP sur l'ensemble des adresses IP virtuelles dans sa configuration sans les assigner aux interfaces du système hébergeur, ce qui facilite considérablement son réglage. Vous trouverez plus d'amples informations sur LaBrea à l'adresse suivante : *http://labrea.sourceforge.net/labrea-info.html*.

Remarque : plusieurs organismes de recherche sont parvenus à la conclusion que les pots de miel à basse interaction représentent une tactique viable contre la propagation extrêmement performante de vers en les ralentissant, ce qui permet de protéger les infrastructures du réseau. Certes, la configuration requise pour pouvoir tirer parti de cet avantage est au mieux obtuse. Toutefois, LaBrea et honeyd peuvent tout deux être configurés de sorte à créer un environnement hostile aux vers.

Pots de miel à haute interaction

Quoique moins utilisés, les pots de miel à haute interaction se révèlent extrêmement utiles. Contrairement à la simple capture des toutes premières transactions dans un dialogue entre un programme malveillant et le pot de miel, le pot de miel dit à haute interaction autorise une attaque à infiltrer entièrement le système sur lequel il réside. Dans un tel cas de figure, les informations utiles capturées comprennent non seulement les techniques d'examen et le type d'exploitation utilisée, mais permettent également à l'administrateur de la sécurité de surveiller le programme malveillant une fois obtenu l'accès au système, exposant sans le vouloir ses intentions et ses outils.

Une organisation à but non lucratif connue sous le nom de Honeynet Project (veuillez consulter le site *http://www.honeynet.org/*) produit un grand nombre d'informations et d'outils faciles d'utilisation conçus pour permettre aux utilisateurs de déployer des pots de miel à haute interaction. Cette organisation propose également des outils de type expertise chargés d'analyser les données collectées lors des infiltrations dans les pots de miel.

Astuce : le projet Honeynet (*http://www.honeynet.org/*) publie un certain nombre d'outils incroyables pouvant être utilisés pour déployer vos propres réseaux de pots de miel. Les outils intitulés Honeywall, Termlog, et Sebek sont plus particulièrement intéressants. Dans le même ordre d'idée, l'équipe du projet a également développé un excellent ouvrage sur la psychologie, les tactiques et les outils utilisés par les pirates, informations recueillies grâce à la technique des réseaux de pots de miel. Ce livre intitulé *Know Your Enemy,* déjà à sa seconde édition au moment de rédiger le présent article, est disponible sur le site Web honeynet.org. L'argent récolté de sa vente sert à financer la recherche sur les réseaux de pots de miel.

Utilisation des réseaux de pots de miel

Les pots de miel ne sont d'aucune utilité aux organismes de recherche ou aux sociétés disposant de beaucoup d'argent et de temps à consacrer à la sécurité (en connaissez-vous beaucoup ?). Il est toutefois déconseillé aux entreprises de tous les jours d'avoir recours aux pots de miel. En revanche, bien qu'inadéquat dans le cadre d'un usage quotidien, il est possible d'installer un réseau de pots de miel sur demande en cas d'apparition de programme malveillant que ni des outils d'expertise ni des renifleurs ne peuvent identifier ni aider votre administrateur à résoudre les problèmes. Ce réseau de pots de miel permet ainsi d'établir une communication en imitant le comportement de la cible visée par le programme malveillant, lequel exposera malgré lui un nombre d'informations suffisant à identifier correctement le type d'attaque menée. Une autre utilisation sur demande consiste à contrôler des infiltrations suspectes. Le réseau de pots de miel constitue ainsi une autre arme à la disposition de l'administrateur de la sécurité.

Que dire enfin de cette installation concrète chez l'un des plus grands fabricants de puces ? Ce fabriquant possède dans tout son réseau des serveurs Linux exécutant VMWare, sur lequel fonctionne quatre machines virtuelles, une pour chaque version les plus répandues du système d'exploitation Windows dans le monde des entreprises, NT, 2000, 2003, et XP. Chacune de ces machines est mise à jour grâce aux niveaux standards des programmes correcteurs de la société. Le système d'exploitation Linux contrôle ces machines pour le trafic et les modifications afin de détecter de nouveaux vers (ou autres menaces) susceptibles de circuler dans la réseau de la société. Ce fabriquant utilise essentiellement cet environnement sous forme de réseau de pots de miel combiné à un système de détection des intrusions de type vers. Vous trouverez plus d'amples informations

Tableau 1. *Paquets ICMP (Internet Control Massage Protocol)*

Paquets ICMP	Signification
3.0	Réseau inatteignable
3.1	Hôte inatteignable
3.3	Port inatteignable
3.4	Fragmentation requise
3.5	Echec du chemin source
3.6	Erreur inconnue sur le réseau de destination
3.7	Erreur inconnue sur l'hôte de destination
3.10	Hôte administrativement interdit
3.11	Type de service réseau inatteignable
3.12	Type de service hôte inatteignable
3.13	Communication administrativement interdite
11.0	Expiration TTL lors du transit
11.1	Réassemblage des fragment trop long

Paquets TCP (Transmission Control Protocol)	Signification
RST bit set	Redémarrage du protocole TCP

sur cette installation à l'adresse suivante : *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*

Installer des puits pour se protéger contre les attaques DDoS

Récemment la technique des puits connaît une nouvelle application sous forme de tactique de défense contre les attaques de déni de service (distribuées). Le premier exemple exposé dans la partie intitulée *Contexte et fonction* illustrait la forme la plus simple que peut prendre cette nouvelle technique de réacheminer le trafic vers un trou noir. Une fois la cible exacte d'une attaque identifiée, l'adresse IP ciblée a été détournée vers l'interface de suppression située à la périphérie du réseau, avant de traverser le lien final vers la cible. Cette technique a permis d'éviter au réseau cible un arrêt total provoqué par la saturation du lien, sans toutefois protéger entièrement la performance de tout le réseau, notamment les clients adjacents partageant certaines parties de la topologie périphérique du transporteur sur le réseau cible. Aujourd'hui, les grands fournisseurs en télécommunications ont structuré leurs réseaux pour y inclure des versions sophistiquées de cette mesure de défense dans le cadre de leur politique de conception des réseaux. Dans de nombreux cas, ces fournisseurs sont désormais capables d'utiliser une technique de pistage afin de localiser les points d'entrée de l'attaque et rediriger vers un trou noir les paquets de données malveillants (vers leurs propres points d'entrée), sans permettre au programme malveillant d'attaquer l'ossature du réseau jusqu'au lien du réseau ciblé. Cette technique de pistage demeure toutefois inutile bien souvent dans la mesure où les chemins conduisant aux trous noirs des fournisseurs sont habituellement annoncés à l'échelle du réseau au moyen de leurs routeurs périphériques ayant recours au protocole BGP (Border Gateway Protocol). Le trafic malveillant est ainsi acheminé vers un trou noir à chaque point d'entrée, lequel peut noyer les attaques dès leur arrivée et (dans la plupart des cas) éviter une congestion de l'ossature ainsi que des périphéries du réseau. Certains fournisseurs ont même étendu le contrôle et l'automatisation de cette technique au client final au moyen des dénommés trous noirs en temps réel amorcés par le client.

Declancher un routage vers un trou noir

Comme nous venons de le mentionner plus haut, d'importants fournisseurs d'accès à Internet ont installé un système distribué et automatisé capable de *declancher* un routage vers des trous noirs sur des adresses IP ciblées. Ce déclanchement peut être provoqué par le fournisseur d'accès à Internet ou par les clients eux-mêmes, soit de manière manuelle soit automatiquement. Le routage provoqué vers un trou noir utilise la technique du simple puit évoquée plus haut dans la partie intitulée *Contexte et fonction*. Le puit peut être configuré sur tous les routeurs d'entrée (périphériques) au sein du réseau du fournisseur d'accès à Internet dans lequel celui-ci échange du trafic avec d'autres fournisseurs ou clients. Une fois la nature de l'attaque dirigée contre le réseau ciblé identifiée, le fournisseur d'accès à Internet ou le client peut indiquer le préfixe *attacked* (ou un préfixe plus spécifique) dans la table de routage BGP. Le préfixe attaqué est marqué d'un attribut next-hop acheminé de manière statistique vers l'interface de suppression sur tous les routeurs périphériques, puis propagé dans le réseau du fournisseur d'accès à Internet via un protocole BGP interne (ou iBGP). Ainsi, quelle que soit l'entrée des paquets destinés au préfixe attaqué dans le réseau du FAI (point d'entrée), ces derniers

Tableau 2. *Récapitulatif des étapes clés*

Étape	Description
Comprendre comment votre FAI peut vous aider en cas d'attaque DDoS.	Élaborer un plan d'actions à mener contre les attaques DDoS comprenant des stratégies capable d'augmenter les capacités de votre FAI dans le domaine des trous noirs en temps réel. Amorcer le dialogue entre votre organisation et votre FAI afin de pouvoir créer des trous noirs en temps réel déclanchés par les clients dans le but de vous protéger sans perdre trop de temps dans leurs procédures d'intensification.
Envisager l'installation d'un réseau invisible interne.	Un réseau invisible vous permet d'attraper des vers avant l'anti-virus de votre fournisseur. De la même manière, ce type de réseau révèle des erreurs de configuration sur votre réseau que vous serez heureux de connaître.
Envisager l'installation d'un réseau invisible externe.	Les réseaux invisibles externes peuvent vous permettre de connaître la nature du programme dirigé contre votre réseau d'un point de vue extérieur et les outils pouvant être utilisés avec ce type de réseaux vous seront certainement plus lisibles que des journaux standards de pare feu. Les messages rétro-diffusés collectés à partir de votre réseau invisible externe peut vous fournir des informations précieuses sur le moment où votre réseau est impliqué dans une attaque sur une tierce partie.
Explorer le réseau au moyen de pots de miel si vous avez le temps et les ressources nécessaires.	Bien que la plupart des organisations n'y voient que peu d'intérêt, l'installation d'un réseau de pots de miel peut se révéler fort utile pour les chercheurs en sécurité de l'information. Il peut être judicieux d'envisager cette solution au sein de votre organisation, sans oublier de tenir compte de la législation en vigueur sur l'exploration des données pouvant avoir une incidence sur votre décision.

sont immédiatement envoyés vers l'interface de suppression du routeur le plus proche en indiquant le préfixe attaqué.

Les fournisseurs d'accès à Internet doivent généralement suivre les étapes suivantes afin de pouvoir installer un mécanisme de trou noir distribué :

- sélectionner un préfixe routé de manière non globale, comme le Test-Net (RFC 3330) 192.0.2.0/24, de sorte à servir d'attribut next-hop permettant d'acheminer vers un trou noir n'importe quel préfixe d'attaque. L'utilisation d'un préfixe de longueur 24 permet d'avoir recours à plusieurs adresses IP différentes pour des types spécifique de routages vers des trous noirs. Il est en effet plus judicieux de différencier les chemins de trous noirs clients, internes ou externes.
- configurer un chemin statique sur chaque routeur d'entrée/interrogateur pour le préfixe 192.0.2.0/24, lequel pointe vers l'interface de suppression. Par exemple : `ip route 192.0.2.0 255.255.255.0 Null0`
- configurer le protocole BGP et la politique de cartes des chemins afin de mentionner les préfixes à diriger vers un trou noir, comme l'illustre le Listing 1.

Dans cet exemple de configuration, des chemins statiques sont redistribués dans le protocole BGP correspondant à la balise “tag 199” (voir ci-dessous), en paramétrant l'attribut next-hop sur une adresse IP acheminée vers l'interface de suppression, et la préférence locale sur 50 (valeur la moins préférée). Il faut enfin veiller à ne pas laisser fuir ces chemins vers un de vos pairs externes (pas d'exportation).

Une fois cette configuration élémentaire réglée, le déclencheur peut être initié par le fournisseur d'accès à Internet. Il lui suffit d'entrer un chemin statique chargé de diriger le préfixe d'attaque (ou l'hôte) vers un trou noir, de la manière suivante, par exemple :

```
ip route 172.16.0.1 255.255.255.255
192.0.2.1 Null0 tag 199
```

Le chemin statique mentionné ci-dessus agit comme *déclencheur* chargé de lancer le processus de routage vers les trous noirs. Le routeur sur lequel est configuré ce chemin indiquera le chemin au moyen d'iBGP à l'ensemble des routeurs internes, y compris les routeurs périphériques. Ainsi, tout routeur doté

d'un chemin statique vers l'interface de suppression pour 172.16.0.1/32 acheminera immédiatement le trafic local vers un trou noir.

Le fournisseur peut également créer un déclencheur automatisé grâce au protocole BGP, de manière à permettre à un client BGP de déclancher le chemin vers le trou noir indépendamment de l'intervention du FAI. Il s'agit en réalité de l'aspect le plus puissant du routage vers les trous noirs. Du côté du fournisseur d'accès à Internet, la configuration est légèrement différente dans la mesure où il va utiliser les communautés et les attributs ebgp-multihop afin de recevoir et de baliser correctement les chemins communiqués par les clients. Nous avons exposé dans le Listing 2 la configuration de base du côté des fournisseurs d'accès à Internet.

Le fournisseur d'accès à Internet a déjà acheminé de manière statique le < *blackhole-ip* > vers les interfaces de suppression dans tout le réseau. Donc, dès l'annonce du client d'un préfixe à diriger vers un trou noir, le FAI le redistribue de manière interne et le trafic vers ce préfixe est acheminé vers un trou noir à la *périphérie* du réseau du fournisseur d'accès.

Nous avons exposé dans le Listing 3 la configuration de base du côté du client.

Une fois la configuration du protocole BGP en place, il suffit au client d'installer un chemin statique pour le préfixe # visé par l'attaque. Grâce à une configuration très simple dans BGP, et l'aide de votre FAI, vous disposez désormais d'une méthode très rapide vous permettant de répondre aux attaques de type DoS menées sur un seul hôte, ou sur un préfixe entier.

Remarque : n'oubliez pas de tout contrôler avec le contact technique de votre FAI avant d'installer votre solution de déclanchement de trous noir dans la mesure où les implémentations des FAI de ce concept diffèrent légèrement de l'une à l'autre.

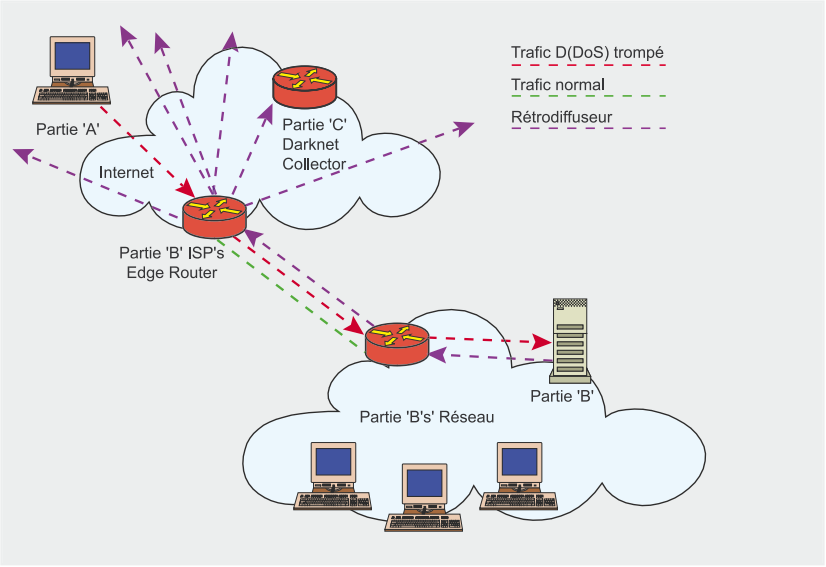

Figure 5. *Exemple d'une rétrodiffusion lors d'une attaque DdoS*

Rétrodiffusion et pisteurs

Cette partie est consacrée aux usages créatifs des réseaux leurres dans le but de détecter des attaques et des arnaques tout en pistant le pirate malveillant.

Rétrodiffusion

Il serait insensé, après avoir évoqué les réseaux leurres et les attaques de type DdoS, de ne pas évoquer la notion de rétrodiffusion. Durant tout un semestre de ma première année de lycée, j'ai écrit des lettres (oui, oui, de véritables lettres en papier) à divers amis qui devaient déménager. Étant de nature assez étourdie, j'indiquais régulièrement sur mes enveloppes une fausse adresse de retour. J'avais en effet omis d'inscrire mon numéro de chambre (je venais de découvrir la bière à cette époque). Il arrivait parfois que l'un de mes amis à qui j'avais écrit ait déménagé. La lettre m'était donc renvoyée avec la mention de la poste *retour à l'expéditeur*. Seulement, en raison de l'adresse incorrecte que j'avais indiquée, la lettre ne m'était pas directement retournée mais était renvoyée au bureau de la résidence du rez-de-chaussée qui m'appelait et m'informait de l'arrivée des lettres (en voyant mon nom bien sûr). Il ne me restait plus qu'à récupérer la lettre renvoyée. Ce *retour à l'expéditeur* n'est ni plus ni moins qu'une sorte de rétrodiffusion. Bien évidemment, le facteur indiquait au bureau de la résidence que j'avais envoyé une lettre (et à qui).

Listing 3. *Configuration de base du côté du client*

```
router bgp XXXX (customer's ASN)
# Le client va installer un chemin statique,
# redistribué dans le protocole BGP,
# lequel redistribue la carte des chemins statiques vers bgp,
# à l'instar des FAI. Le client utilise la carte des chemins pour paramétrer
et faire correspondre
# les attributs de préfixes spécifiques.
route-map static-to-bgp permit 5
# Fait correspondre la balise arbitraire,
# préalablement approuvée par le client et le FAI
match tag NNNN
set community additive XXX:NNNN
# NNNN représente la balise, approuvée par le client et le FAI
ip route 192.168.0.1 255.255.255.255 Null0 tag NNNN
```

Sur Internet, lorsqu'une partie A tente de réaliser une attaque DoS contre une partie B, en souhaitant dissimuler son identité, elle écrit en règle générale une adresse source erronée sur les paquets de son attaque (les en-têtes IP sont falsifiés de manière à donner l'impression de venir des parties A-Z, par exemple ; seul A-Z sous IPv4 correspond à des permutations 2^32). Lors de telles attaques, les routeurs et autres dispositifs du réseau ainsi que le chemin qui y mène renvoient inévitablement une variété de messages allant du redémarrage de la connexion à des requêtes quench sur des notifications inatteignables. Dans la mesure où ces messages sont *retournés à l'expéditeur*, lequel est falsifié, l'ensemble des parties A-Z recevront ces messages qui les informera d'une attaque dirigée contre la partie B, à l'instar du bureau de ma résidence informé des lettres que j'envoyais. La Figure 5 illustre le mécanisme.

Dans le filtrage de paquets désormais pratiqué, la plupart de ces messages renvoyés sont ignorés de manière silencieuse par les pares feu. En effet, ces messages sont considérés comme des réponses à des messages que nous n'avons pas envoyés. Toutefois, grâce à l'installation d'un réseau invisible externe expliquée plus haut, il est possible de retrouver ces paquets renvoyés afin de déterminer le moment où notre espace d'adresse est impliqué dans une attaque sur une autre partie. Les types suivants de paquets susceptibles d'apparaître dans un réseau invisible peuvent être définis comme rétrodiffuseurs et vous informent généralement de l'implication de votre espace d'adresse (ou de réseau invisible) dans une attaque :

Pistage

Vous connaissez désormais la technique de rétrodiffusion, mais comment l'utiliser à bon escient ? Dans un réseau à plusieurs passerelles de transit Internet, il peut s'avérer utile de localiser le point d'entrée de ces *mauvais paquets* en cas d'attaque particulièrement virulente. Cette technique connue sous le nom de pistage, ou *traceback* en anglais, est d'autant plus pratique qu'une fois le point d'entrée spécifique sur le réseau (ou le réseau du FAI) identifié, il est possible de lâcher le trafic à cet endroit et de réduire la charge sur les liens, en permettant éventuellement au *bon* trafic de passer (via des passerelles alternatives), contrairement à la tactique plus simple du trou noir DdoS, évoquée plus haut. Cette technique du pistage permet d'utiliser les rétrodiffuseurs collectés dans le(s) réseau(x) invisible(s) comme moyen de recherche du point d'entrée de l'attaque dans le réseau. Malheureusement, cette technique n'est véritablement viable que du côté des FAI ou sur les réseaux de données éloignés dotés de nombreuses passerelles Internet. Il faut en effet comprendre en plus de la présente description certaines dépendances supplémentaires parmi lesquelles l'utilisation du mécanisme de défense des trous noirs à *chaque* passerelle Internet. Dans la mesure où les FAI les plus importants procèdent de cette manière ainsi qu'une poignée de réseaux entreprise mondiaux, nous allons tout de même expliquer en quoi consiste ce processus.

Supposons que vous disposiez d'un réseau configuré comme décrit plus haut, vous pouvez alors réaliser un pistage au beau milieu d'une attaque DoS. Il vous suffit de suivre les trois étapes suivantes :

- identifier la cible et contrôler que le trafic de l'attaque est bien falsifié (si tel n'était pas le cas, cette tactique de pistage deviendrait inutile).
- diriger vers un trou noir le chemin des hôtes spécifiques (vraisem-

Sur Internet

- *Extreme Exploits : Advanced Defenses against Hardcore Hacks*, publié par McGraw-Hill/Osborne, tous droits réservés 2005, http://www.amazon.com/gp/product/0072259558/
- RFC 3330 (adresses Ipv4 d'utilisation spéciale) et 3882 (configuration du protocole BGP afin de bloquer les attaques DoS) Internet
- Projet sur les réseaux invisibles de l'équipe Cymru, http://www.cymru.com/Darknet/
- Page d'accueil des outils tcpdump et libpcap, http://www.tcpdump.org/
- Page d'accueil de l'outil ARGUS, http://www.qosient.com/argus/flow.htm
- Page d'accueil de Honeyd, http://www.honeyd.org
- Page d'accueil du projet HoneyNet, http://www.honeynet.org
- Page d'accueil de l'outil p0f, http://lcamtuf.coredump.cx/p0f.shtml
- Article de Chris Morrow et de Brian Gemberling sur les trous noirs des FAI et l'analyse de la rétrodiffusion, http://www.secsup.org/Tracking/
- Présentation de Dan Hawrylkiw sur les réseaux de pots de miel, http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf
- Questions les plus fréquentes sur le filtre de paquets OpenBSD, http://www.openbsd.org/faq/pf/

À propos de l'auteur

Auteur et orateur reconnu, M. Oppleman enseigne dans le domaine de la sécurité des réseaux tout en travaillant comme consultant auprès de sociétés parmi les plus prestigieuses au monde. Le logiciel libre élaboré par M. Oppleman a été distribué sur des centaines de milliers d'ordinateurs dans le monde entier. M. Oppleman détient par ailleurs la propriété intellectuelle de certaines applications client sans fil et de routage adaptable distribué. Une grande partie du contenu du présent article est tiré du livre de M. Oppleman intitulé *Extreme Exploits : Advanced Defenses Against Hardcore Hacks*, publié par McGraw-Hill/Osborne (tous droits réservés 2005) et disponible en librairie.

blablement de type /32) ciblés par l'attaque pour chacune de vos passerelles. La plus grande attention est requise en termes de transfert vers l'interface de suppression venant remplacer l'utilisation d'un filtre à paquets censé stopper les paquets de l'attaque. Cette opération de trou noir obligera le routeur de la passerelle concernée à générer des messages ICMP inatteignables, retournés (ou tentés d'être retournés) vers les sources falsifiées des paquets de l'attaque.

- utiliser dans les réseaux invisibles des outils chargés de détecter le trafic de rétrodiffusion (vraisemblablement sous la forme de messages ICMP inatteignables) à l'aide de l'adresse IP des routeurs de passerelles. Toutes les adresses IP des passerelles considérées comme sources des paquets rétrodiffuseurs valident le fait que ces passerelles sont en réalité des points d'entrée pour le trafic de l'attaque. Voilà ! Vous venez de trouver le point d'entrée de l'attaque dans votre réseau. Même si vous ne disposez pas d'outils de réseau invisibles sophistiqués, une simple liste d'accès appliquée à l'interface du routeur de votre réseau invisible suffira à faire le travail à votre place, de la manière suivante :

```
access-list 105 permit icmp any any unreachables log; access-list 105 permit ip any any
```

Enfin, si vous entrez en mode contrôle terminal dans cette liste d'accès (ou tout simplement si vous suivez le journal), vous obtiendrez un modeste rapport sur les rétrodiffuseurs dans lequel vous pouvez cherchez les adresses IP de vos passerelles.

Cette tactique de pistage combinée à une défense de type trou noir contre les attaques DDoS se révèle utiles dans des situations où les flux de trafics malveillants ont falsifié les en-têtes. Il s'agissait jusqu'à très récemment de la forme la plus répandue pour lancer ce type d'attaques. Toutefois, avec la prolifération des machines zombies et des réseaux de zombies, de nombreux pirates ont désormais cessé la falsification des paquets DdoS. En effet, nul besoin de falsifier les en-têtes si votre armée de systèmes d'attaque se trouve partout. C'est la raison pour laquelle les administrateurs réseau observent une chute considérable des attaques DdoS falsifiées au profit du large déploiement des uRPF et du filtrage de points d'entrée. ●