Empêcher les attaques par déni de service distribué (DDoS)

Gazette Linux n°126 — Mai 2006

Blessen Cherian

Ben Okopnik

Article paru dans le n°126 de la Gazette Linux de mai 2006.
Traduction française par Deny `<deny CHEZ monaco POINT net>`.
Relecture de la traduction française par Joëlle Cornavin `<jcornavi CHEZ club TIRET internet POINT fr>`.

Table des matières

1. Introduction

Dans cet article, j'essaierai de décrire ce qu'est une attaque par DDoS (*Distributed Denial of Service*, déni de service distribué), comment l'empêcher ou la limiter. Nombre des serveurs, dans les centres de traitement de l'information, fonctionnent sous Linux ; je vais par conséquent aborder la prévention et la limitation des d'attaques par DDoS contre les serveurs Linux.

Les attaques par DDoS surviennent en raison d'un manque de prise de conscience, d'applications ou de compétence en matière de sécurité de la part des propriétaires ou des administrateurs de réseaux ou de serveurs. Nous entendons souvent qu'une machine en particulier subit une attaque par DDoS ou que le NOC (*Netswork Operation Center*, centre d'exploitation du réseau) a déconnecté une machine donnée en raison de son implication dans une attaque par DDoS. Le DDoS est devenu un des problèmes courants de notre monde. Par certains côtés, DDoS est comme une maladie contre laquelle nous n'avons pas de remède efficace, et requiert beaucoup de prudence lorsqu'on y est confronté. Ne le prenez jamais à la légère. Dans cet article, j'essaierai de faire un compte rendu des étapes et des mesures qui nous aideront à défendre nos machines contre une attaque par DDoS — au moins jusqu'à un certain point.

2. Qu'est-ce qu'une attaque par DDoS ?

Pour résumer, le DDoS (*Distributed Denial of Service*, déni de service distribué) est une version avancée de l'attaque par DoS (*Denial of Service*, déni de dervice). Tout comme le DoS, le DDoS tente également de bloquer des services importants s'exécutant sur un serveur en inondant de paquets le serveur de destination. La spécialité du DDoS est que les attaques ne proviennent pas d'un seul réseau ou hôte, mais d'un certain nombre d'hôtes ou de réseaux différents qui ont été précédemment compromis.

On peut considérer que le DDoS, comme nombre d'autres stratégies d'attaque, est constitué de trois participants ; nous pouvons y faire référence sous les termes du Maître, de l'Esclave et de la Victime. Le Maître est la source initiale de l'attaque — c'est-à-dire la personne ou la machine responsable. L'Esclave est l'hôte ou le réseau qui a été précédemment compromis par le Maître, et la Victime est le site ou le serveur cible attaqué. Le Maître ordonne à l'Esclave (ou aux Esclaves) de lancer une attaque sur le site ou la machine de la Victime ; puisque l'attaque provient de sources multiples simultanément (notez que le Maître n'est habituellement pas impliqué dans cette phase), elle est qualifiée d'attaque distribuée (ou coordonnée).

3. Comment fonctionne-t-elle ?

Une attaque par DDoS se déroule en deux phases. Dans la première, le propriétaire de l'hôte Maître compromet des machines vulnérables dans différents réseaux à travers le monde et installe des outils de DDoS (c'est-à-dire des programmes qui effectueront l'attaque dés lors qu'ils seront déclenchés) : c'est la phase d'intrusion. Dans la phase suivante, le Maître expédie les informations de déclenchement à ces hôtes compromis, ce qui comprend d'ordinaire l'IP à attaquer (inversement, cette IP pourrait avoir été préprogrammée dans les outils et l'attaque elle-même pourrait être à déclenchement programmé — comme par exemple le DDoS du virus *Code Red* contre les serveurs de la Maison Blanche : c'est la phase d'attaque.

4. Que vous permet-elle de faire ?

Le succès de la phase d'intrusion repose sur la présence de machines vulnérables sur un réseau arbitraire.

Malheureusement, il y a un très grand nombre de propriétaires d'ordinateurs naïfs et d'administrateurs système dont les machines manquent cruellement de protection et, de ce fait, cette phase sera facilement accomplie par l'attaquant dans presque tous les cas.

Voici quelques-uns des facteurs qui rendent des machines Esclaves vulnérables :

1. Des logiciels ou les applications vulnérables fonctionnant sur une machine ou un réseau ;
2. Une configuration réseau ouverte ou non protégée ;
3. Des hôtes configurés sans prise en compte de la sécurité ;
4. Une absence de surveillance ou d'analyse de données ;
5. Une absence de conduite de mises à niveau ou d'audit réguliers.

5. Que devrions-nous faire en cas d'attaque ?

Si votre hôte est un des Esclaves lors d'une attaque par DDoS, vous n'en serez probablement jamais conscient — à moins que vous n'examiniez soigneusement vos fichiers journaux et surveilliez une activité indésirable du réseau. Si, par ailleurs, vous êtes la Victime, les conséquences seront spectaculaires et évidents.

5.1. Symptômes de la Victime

1. Les programmes s'exécutent très lentement.
2. Les services (par exemple, HTTP) échouent à un taux élevé.
3. On observe un grand nombre de requêtes de connexion provenant de différents distincts.
4. L'utilisateur se plaint de l'accès aux sites ralenti (ou aucun accès).
5. La machine affiche une charge du processeur élevée.

5.2. Si vous découvrez que vous êtes attaqué

Suivez ces étapes :

- Vérifiez si la charge de votre processeur est élevée et si vous avez un grand nombre de processus HTTP actifs.

  Vérifiez la charge à l'aide des commandes **w** ou **uptime** :

  Comptez le nombre de processus HTTP (cela vous pemet de savoir quel est votre compte normal pour comparer) :

- Déterminez le réseau attaquant.

Pour un serveur à forte charge, le nombre de connexions peut s'élever à plus de 100 — mais pendant une attaque par DDoS, ce nombre peut encore augmenter. C'est à ce stade que nous devons découvrir, aussi rapidement que possible, quels réseaux lancent ces attaques. Dans une attaque par DDoS, la machine esclave individuelle n'a pas beaucoup d'importance ; c'est le réseau qui importe le plus, puisqu'un attaquant pourrait utiliser n'importe laquelle, voire toutes les machines sur un réseau compromis. En conséquence, l'adresse du réseau est d'une importance cruciale.

L'exécution de la commande suivante affichera les IP dans l'ordre des connexions établies :

Pour un hôte moyen, si vous avez plus de 30 connexions provenant d'une seule IP, il est probable que vous êtes « en pleine attaque ». En fonctionnement normal, il y a très rarement une raison pour un grand nombre de requêtes depuis une seule IP. Identifiez ces réseaux pour faire un rapport ultérieur, éventuellement à l'aide de la commande **whois**.

Si plus de 5 de tels hôtes ou IP se connectent depuis le même réseau, c'est un signe très clair de DDoS.

- Bloquez le réseau attaquant.

Pour ce faire, utilisez iptables ou apf :

Si vous lancez apf, ajoutez simplement ces IP au fichier `/etc/apf/deny_hosts.rules` . Poursuivez ce processus d'élimination jusqu'à ce que l'attaque sur la machine soit réduite (et, si tout se passe bien, arrêtée tout à fait). À titre de mesure complémentaire, contactez le responsable du centre de traitement ou du NOC de ce réseau pour l'informer que les systèmes sont compromis.

Comme stratégie à long terme, une fois que l'attaque immédiate est terminée (ou, si vous êtes rusé, vous pouvez le faire dés à présent), installez Portsentry (reportez-vous la liste des logiciels à la fin de cet article).

6. Comment pouvons-nous empêcher ces attaques ou nous en défendre ?

Il n'existe aucune solution complète ou parfaite au DDoS. La logique est simple : AUCUN logiciel ou contre-mesure ne peut bloquer les attaques de, par exemple, 100 serveurs à la fois. On ne peut que prendre des mesures préventives, et répondre rapidement et efficacement lorsque l'attaque a lieu.

Comme on le dit souvent, mieux vaut prévenir que guérir — et c'est particulièrement vrai dans le cas du DDoS. Dans l'introduction, j'avais mentionné que le DDoS se produit souvent à cause de logiciels ou d'applications vulnérables fonctionnant sur une machine dans un réseau particulier. Les attaquants utilisent ces trous de sécurité pour compromettre les hôtes et les serveurs, et installer des outils de DDoS tels que trin00.

Pour empêcher ou limiter de futures attaques par DDoS, suivez ces étapes :

1. Créez et mettez en œuvre une bonne politique de sécurité.
2. Installez un pare-feu qui filtre à l'entrée et à la sortie de la passerelle (par exemple, APF de http://www.rfxnetworks.com/apf.php).

3. Employez un outil de détection d'intrusion sur votre passerelle ou votre machine pour vous avertir des balayages de port et des tentatives d'intrusion (par exemple, AIDE de http://freshmeat.net/projects/aide/).

Pour empêcher que votre réseau soit utilisé comme esclave, suivez ces étapes :

1. Menez des audits réguliers sur chaque hôte du réseau pour trouver les outils de DDoS installés et les applications vulnérables.
2. Faites appel à des outils comme Rkdet (http://vancouver-webpages.com/rkdet/Rkdet), Rootkit Hunter (http://www.rootkit.nl/projects/rootkit_hunter.html) ou Chkrootkit (http://www.chkrootkit.org) pour savoir si un *rootkit* a été installé sur votre système.
3. Procédez à un audit général de sécurité sur vos systèmes de façon régulière :
   - Maintenez votre système à jour pour minimiser les vulnérabilités des logiciels (mise à niveau du noyau et des applications).
   - Recherchez la présence de *rootkits.*.
   - Contrôlez les fichiers journaux pour rechercher des preuves de reniflages de port, etc.
   - Contrôlez les processus cachés en comparant la sortie de **ps** et **lsof**.
   - Employez des outils d'audit (c'est-à-dire Nessus (http://www.nessus.org/), SAINT (http://www.saintcorporation.com/products/vulnerability_scan/saint/saint_scanner.html) ou SARA (http://www-arc.com/sara/sara.html)).
   - Contrôlez les binaires du système avec, par exemple, Tripwire pour voir s'ils ont été changés depuis votre dernier instantané.
   - Recherchez la présence de relais de messagerie électronique ouverts.
   - Recherchez la présence de lignes cron malveillantes.
   - Recherchez dans les répertoires `/dev`, `/tmp`, `/var` la présence de fichiers inhabituels (c'est-à-dire, `...`, des permissions/appartenances incorrectes sur les fichiers de périphériques, etc.).
   - Examinez si les sauvegardes sont maintenues.
   - Recherchez la présence d'utilisateurs ou de groupes indésirables (examinez `/etc/passwd`).
   - Recherchez et désactivez tout service inutile.
   - Rechercher les fichiers SUID, SGID et *nouser* dans votre système avec la commande **find**.
   - Notez les performances du système (mémoire et utilisation du processeur) ; notez les niveaux moyens.
4. Créez une équipe de DSE (*Dedicated Security Expert*, expert en sécurité) pour votre entreprise.
5. Imposez et mettez en œuvre des mesures de sécurité pour tous les hôtes du réseau. Les seuls hôtes qui devraient être autorisés sur votre réseau sont ceux qui contrôlés par votre administrateur en sécurité ou votre DSE. Tous les hôtes présents sur le réseau devraient être contrôlés régulièrement par votre équipe de DSE.
6. Collectez les données de votre réseau et de votre hôte, et analysez-les pour savoir quels sont les types d'attaques lancés à l'encontre de vos réseaux.

7. Mettez en œuvre une protection reposant sur Sysctl. Activez les lignes suivantes dans votre `/etc/sysctl.conf` :

   Inversement, vous pourriez ajouter ce code dans votre `/etc/rc.local` :

8. Installez PortSentry (http://linux.cudeso.be/linuxdoc/portsentry.php#config) pour bloquer le balayage des hôtes.
9. Ajoutez Mod_dosevasive à votre installation Apache. C'est un module Apache qui effectue une action `evasive` dans l'éventualité d'une attaque par DDoS via HTTP ou une attaque en force brute.
10. Installez le module Mod_security. Puisque souvent le DDoS cible HTTP (port 80), il est judicieux d'avoir un système de filtrage pour Apache ; Mod_security analysera les requêtes avant de les transmettre au serveur *web*.
11. Installez un équilibrage de charge pour vos services. Par certains côtés, c'est la défense à commande réseau la plus puissante contre le DDoS.
12. Créez une prise de conscience des problèmes de sécurité.

7. Conclusion

Les attaques par DDoS peuvent être limitées sur la machine cible et empêchées sur le réseau esclave en mettant en œuvre une sécurité correcte. Je conseille à chaque propriétaire de serveur et de réseau d'appliquer des mesures de sécurité efficaces ; puisque le DDoS est un problème à l'échelle du réseau, sa prévention va nécessiter les efforts de chacun.

> Mon nom est Blessen et je préfère que l'on m'appelle Bless. Je me suis intéressé à Linux quand j'ai rejoint la SSII Poornam Info Vision Pvt Ltd (http://poornam.com/), également connue sous le nom de Bobcares (http://bobcares.com/). Elle m'a fait découvrir Linux.
>
> Je suis titulaire d'un *B-Tech* du *College of Engineering* de Chengannur. J'ai terminé mes études en 2001 et suis entré dans l'entreprise la même année. Durant mon travail, j'étais passionné par la sécurité sous Linux et j'envisage de m'améliorer dans ce domaine.
>
> Mes centres d'intérêt consistent à naviguer sur le Net, apprendre de nouvelles technologies et aider les autres. Pendant mes loisirs, je développe également des logiciels *opens source*, dont l'un d'entre eux est une version réduite de formmail. Le projet, appelé Smart Mail, est plus sécurisé que formmail.
>
> —Blessen Cherian

> Ben est le rédacteur en chef de la *Linux Gazette* et il est membre de l'*Answer Gang*.
>
> Ben est né à Moscou (Russie) en 1962. Il a commencé à s'intéresser à l'électricité dès l'âge de 6 ans, ce qu'il a rapidement démontré en enfonçant une fourchette dans une prise et en déclenchant un incendie, et depuis il n'a jamais cessé de s'intéresser à la technologie. Il travaille avec les ordinateurs depuis les Temps Anciens, lorsqu'il fallait souder soi-même des composants sur des cartes à circuits imprimés et que les programmes devaient tenir dans 4 ko de mémoire. Il serait heureux de payer un bon prix tout psychologue capable de le guérir des cauchemars récurrents qu'il a gardés de cette époque.
>
> Ses expériences suivantes comprennent la création de programmes dans près d'une douzaine de langages, la maintenance de réseaux et de bases de données pendant l'approche d'un ouragan, sans oublier l'écriture d'articles pour des publications allant des magazines de voile aux journaux technologiques. Après une croisière de 7 ans dans l'Atlantique et les Caraïbes ainsi que des passages sur la côte Est des États-Unis, il a désormais jeté l'ancre à St-Augustine (Floride). Instructeur technique chez Sun Microsystems, il travaille également à titre privé comme consultant *open source* et développeur web. Ses passe-temps actuels sont notamment

l'aviation, le yoga, les arts martiaux, la moto, l'écriture et l'histoire romaine. Son Palm Pilot© est truffé d'alarmes dont la plupart contiennent des points d'exclamation.

Il travaille avec Linux depuis 1997 et lui doit d'avoir perdu tout intérêt sur les retombées d'une guerre nucléaire dans le nord-est du Pacifique.

—Ben Okopnik