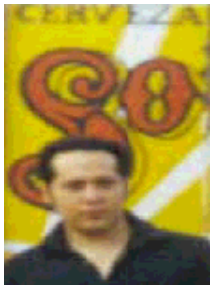
LinuxFocus article number 274
http://linuxfocus.org



par José Salvador González Rivera
<jsgr(at)tec.com.mx>

L´auteur:

José Salvador González Rivera est un membre actif du Groupe d'Utilisateurs de Linux de Puebla (Mexique). Il participe souvent à des manifestations pour la promotion du Logiciel Libre, et particulièrement de Linux. Il vient d'obtenir une licence en Informatique et Systèmes. Vous pouvez le joindre à jsgr(at)tec.com.mx ou à jsgr(at)linuxpuebla.org.

Détection d'Intrusion sous Debian GNU/Linux

Résumé:

Aujourd'hui, une grande partie de l'information est stockée numériquement sur des supports électroniques et par conséquent, elle devient plus facile d'accès par l'intermédiaire de réseaux d'ordinateurs. Ces derniers nous permettent d'obtenir des données distantes qu'elles soient financières, administratives, militaires, industrielles ou commerciales. Malheureusement, ces données sont une cible facile pour des gens mal intentionnés désirant se les procurer ou les détruire, le mot "éthique" ne faisant pas partie de leur vocabulaire.

Contre l'absence de conscience, il n'y a pas grand chose à faire. Dans ce court article je ferai un tour d'horizon de la technique et des outils de détection d'intrusion sous Debian GNU/Linux. Je ne reproduirai pas le contenu des manuels puisque je me concentrerai sur ce qui se passe dans la réalité.

Traduit en Français par:
Georges Tarbouriech
<gt(at)linuxfocus.org>

Introduction

Lors du choix d'un système d'exploitation Linux, de nombreuses distributions sont à prendre en considération. Nombre d'entre elles sont basées sur RedHat, par exemple Conectiva (Brésil), Hispa source (Espagne), Mandrake (France), SuSE (Allemagne), Caldera et beaucoup d'autres utilisant le système de paquetages RPM. Il existe aussi Slackware qui essaie d'être plus proche de l'Unix traditionnel en n'utilisant que des archives .tgz. "Presque" toutes sont développées par des sociétés

commerciales, mais ce n’est pas le cas de Debian. Debian propose un gestionnaire de paquetages (DPKG) qui nous permet des mises à jour automatiques par Internet; il vérifie également les dépendances, rendant l’administration du système plus facile tout en restant à jour pour ce qui concerne les correctifs de sécurité.

Pourquoi Debian GNU/Linux ?

Debian dispose de caractéristiques intéressantes :

1) Il n’a aucun but commercial et ne subit pas la loi du marché.
2) Il possède un très bon système de suivi d’erreurs et les problèmes sont résolus en moins de 48 heures.
3) Depuis le début, sa priorité consiste à développer un système d’exploitation complet et fiable.
4) Il est développé par des volontaires tout autour du monde.

Chaque nouvelle version offre un nouveau support matériel; pour l’instant, les architectures supportées sont les suivantes : Alpha, ARM, HP PA-RISC, Intel x86, Intel IA-64, Motorola 680x0, MIPS, MIPS (DEC), Power PC, IBM S/390, Sparc et ils sont en train de travailler sur les processeurs Sun UltraSparc et Hitachi SuperH. C’est le système Linux fonctionnant sur le plus grand nombre de plates-formes.

Parmi les paquetages Debian existants, plusieurs outils de détection d’intrusion en temps réel sont capables de découvrir un comportement hostile envers une connexion. Il en existe deux catégories : ceux qui surveillent les tentatives d’attaques sur un réseau et ceux qui contrôlent l’activité sur un hôte spécifique.

Outils d’hôtes

Nous utilisons PortSentry pour détecter les scans de ports, TripWire pour contrôler les changements dans le système et LogSentry pour l’analyse des "logs". Le premier et le dernier font partie de la suite TriSentry de Psionic Technologies.

Détection de scans de ports

PortSentry surveille les ports de notre système et il effectue une action (généralement un blocage) s’il détecte une tentative de connexion sur un port dont nous ne souhaitons pas qu’il soit écouté.

Le site web se trouve à http://www.psionic.com/products/portsentry.html et PortSentry est disponible pour Solaris, BSD, AIX, SCO, Digital Unix, HP-UX, et Linux.

Sur Debian il peut s’installer par la commande :

apt-get install portsentry

Différents niveaux d'activité peuvent être choisis : le mode classique, le mode "stealth" (furtif) et le mode avancé. La configuration repose sur le fichier /usr/local/psionic/portsentry/portsentry.conf.

J'ai trouvé les options principales dans un article de José Torres Luque dans ES Linux Magazine et ce sont les suivantes :

TCP_PORTS, vous définissez ici les ports à contrôler soit en mode classique soit en mode stealth. L'auteur du programme propose trois listes de ports selon le degré de réactivité que vous souhaitez appliquer. Le nombre maximum de ports s'élève à 64.

UDP_PORTS, comme le précédent mais pour les ports UDP.

ADVANCED_PORTS_TCP, ADVANCED_PORTS_UDP, indique le numéro de port le plus élevé à utiliser en mode avancé. Chaque port au-dessous de celui-ci sera surveillé sauf ceux déjà exclus. Le port le plus élevé peut être défini jusqu'à 65535. Toutefois il est déconseillé de dépasser 1024 afin d'éviter les fausses alertes.

ADVANCED_EXCLUDE_TCP, ADVANCED_EXCLUDE_UDP, propose une liste des ports à exclure. Les ports présents dans cette section ne seront pas surveillés en mode avancé. Vous pouvez y inscrire les ports habituellement dédiés aux clients distants et ceux n'offrant pas un véritable service. ident, par exemple.

IGNORE_FILE, nous y inscrivons le chemin du fichier dans lequel nous définissons les adresses IP à ignorer. L'interface locale, lo comprise, doivent également se trouver dans ce fichier. Vous pouvez aussi y ajouter les adresses IP locales.

KILL_ROUTE, nous pouvons ajouter ici la commande à exécuter pour bloquer l'hôte attaquant. Par exemple : iptables -I INPUT -s $TARGET$ -j DROP où $TARGET$ correspond à l'hôte attaquant.

KILL_RUN_CMD, nous indiquons une commande à exécuter avant de bloquer l'accès de l'hôte attaquant.

SCAN_TRIGGER, détermine le nombre de tentatives avant de déclencher l'alarme.

PORT_BANNER, affiche un message sur les ports ouverts en mode connexion.

Une fois configuré, il doit être exécuté dans l'un des trois modes grâce aux options suivantes : pour TCP vous disposez de -tcp (mode de base), -stcp (mode stealth) et -atcp (mode avancé); pour UDP ce peut être -udp, -sudp, -audp.

Analyse d'intégrité

TripWire permet de vérifier l'intégrité des fichiers du système; le site web se trouve à http://www.tripwire.org et il est libre pour Linux et commercial pour Windows NT, Solaris, AIX et HP-UX.

Sur Debian il peut être installé par la commande :

apt-get install tripwire

Pour stocker l'information deux clés sont nécessaires : la première, la clé du site ("site key") est utilisée pour chiffrer les règles et les fichiers de configuration, et la seconde, la clé locale ("local key") sert à chiffrer l'information sur l'état des fichiers contrôlés.

La configuration se fait simplement dans le fichier /etc/tripwrie/twpol.txt et une fois qu'elle a été adaptée, vous pouvez l'installer en tapant :

twadmin -m P /etc/tripwire/twpol.txt

Pour créer la base de données initiale contenant l'état actuel des fichiers, nous exécutons la commande :

tripwire -m i 2

Pour vérifier l'intégrité du système de fichiers, nous tapons :

tripwire -m c

Le fichier de configuration peut être effacé afin d'empêcher un intrus de savoir quels fichiers ont été modifiés en tapant :

rm /etc/tripwire/twcfg.txt /etc/tripwire/twpol.txt

Pour les créer si besoin est, tapez :

twadmin -m p > /etc/tripwire/twpol1.txt twadmin -m f > /etc/tripwire/twcfg.txt

Analyse des logs

LogCheck fait partie de LogSentry et permet une analyse efficace des logs puisqu'il les classifie et établit des rapports sur l'activité et les erreurs qui réclament une lecture. Il propose quatre niveaux d'analyse différents : ignorer, activité inhabituelle, violation de sécurité et attaque.

Le site web est à http://www.psionic.com/products/logsentry.html. LogSentry est disponible pour Solaris, BSD, HP-UX et Linux.

Sur Debian il peut être installé par la commande :

apt-get install logcheck

Ceci installe le programme logtail dans /usr/local/bin pour maintenir une liste des analyses déjà effectuées. Les fichiers suivants sont également installés :

Logcheck.sh,
Un script contenant la configuration de base.

Logcheck.hacking,
Contient les règles définissant les niveaux d'activité.

Logcheck.ignore,
Contient les expressions à ignorer.

Logcheck.violations,
Contient les expressions pouvant être considérées comme des violations de sécurité.

Logcheck.violations.ignore,
Les expressions présentes dans ce fichier sont destinées à être ignorées.

Vous pouvez utiliser cron pour lancer logcheck toutes les heures : 0 * * * * /bin/sh /usr/local/etc/logcheck.sh

Outils réseau

Nous utilisons Snort pour détecter les tentatives d'attaque réseau. Le site web se trouve à http://www.snort.org et snort est disponible pour BSD, Solaris, AIX, Irix, Windows, MacOS X et Linux.

Sur Debian il peut être installé par la commande :

apt-get install snort

Il fonctionne en trois modes : sniffer, packet logger et détecteur d'intrusion

Il utilise les paramètres suivants :

-l répertoire
indique le répertoire où stocker les fichiers.

-h IP
définit l'adresse IP du réseau que nous voulons surveiller.

-b
capture les paquets sous forme binaire.

-r fichier
examine un fichier binaire.

Les modes Sniffer et Packet Logger de snort

En mode sniffer, il lit tous les paquets circulant à travers le réseau et les affiche sur la console alors qu'en mode packet logger il envoie les données dans un fichier.

Snort -v

Montre IP et en-têtes.

Snort -dv

Montre également les données qui circulent.

Snort -dev

Propose une information plus détaillée.

Mode de Détection d'Intrusion de snort

Dans ce mode, snort nous informe sur les scans de ports, les attaques DoS (Déni de Service), les exploitations de vulnérabilités (exploits), etc. Il s'appuie sur des règles se trouvant dans /usr/local/share/snort, que vous pouvez télécharger sur le site, et le serveur les remet à jour toutes les heures.

Sa configuration est très simple puisqu'elle consiste à modifier le fichier snort.conf, dans lequel nous indiquons les caractéristiques de notre réseau et les répertoires de travail. Modifiez seulement l'IP :

var HOME_NET IP

Pour exécuter snort, tapez :

snort -c snort.conf

Les fichiers de "logs" sont enregistrés dans /var/log/snort et nous pouvons y voir les adresses IP des attaquants. Ceci n'est bien sûr qu'un très bref résumé des possibilités de snort et je recommande une lecture plus approfondie sur le sujet. La plupart des organisations, des magazines, des groupes de sécurité considèrent cet excellent outil comme le meilleur système de détection d'intrusion pour Unix ou Windows et n'hésitent pas à le recommander. Il existe un support commercial proposé par des sociétés comme Silicon Defense et Source Fire et des interfaces graphique commencent à apparaître pour offrir une présentation des résultats plus esthétique.

Parfois des situations d'urgence se présentent réclamant une analyse plus détaillée puisque certains problèmes ont pu ne pas être pris en compte et doivent être résolus immédiatement.

Ces problèmes sont habituellement causés par des gens mal intentionnés ou des intrus essayant d'accèder à nos serveurs pour différentes raisons, qu'il s'agisse de voler ou d'altérer nos données ou

d’attaquer d’autres machines à partir de la notre, soit en installant un sniffer ou un rootkit qui sont des ensembles logiciel permettant d’obtenir un maximum de privilèges sur un système.

Autres outils utiles

Détection de sniffer

Un sniffer est un outil qui passe notre interface réseau en mode "promiscuous" dans le but d’écouter le trafic du réseau. La commande ifconfig nous fournit la totalité des informations concernant l’interface réseau :

```
eth0 Link encap:Ethernet HWaddr 00:50:BF:1C:41:59
inet addr:10.45.202.145 Bcast:255.255.255.255 Mask:255.255.128.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7180 errors:0 dropped:0 overruns:0 frame:0
TX packets:4774 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:8122437 (7.7 MiB) TX bytes:294607 (287.7 KiB)
Interrupt:10 Base address:0xc000
```

Toutefois, si la commande ifconfig a été remplacée ou si le sniffer fonctionne à partir d’une autre machine, vous devez vérifier les connexions externes, par exemple, en envoyant un courrier à un compte "bidon" ou en essayant de détecter les logs du sniffer.

Il existe un outil nommé neped, conçu par un groupe Espagnol, qui nous informe sur les interfaces de notre réseau fonctionnant en mode "promiscuous". Il ne fait pas partie de Debian mais peut être téléchargé depuis ftp://apostols.org/AposTools/snapshots/neped/neped.c
Note : ce serveur semble ne plus répondre depuis quelques semaines.

Exécuter ce programme donnera une réponse du genre :

```
neped eth0
-----------------------------------------------------
> My HW Addr: 00:80:F6:C2:0E:2A
> My IP Addr: 192.168.0.1
> My NETMASK: 255.255.255.0
> My BROADCAST: 192.168.1.255
-----------------------------------------------------
Scanning ....
* Host 192.168.0.2, 00:C2:0F:64:08:FF **** Promiscuous mode detected !!!
End.
```

Lorsque nous envoyons un paquet IP de 191.168.0.1 à 192.168.0.2 nous devons connaître l’adresse

MAC. Ceci s’accomplit en envoyant un paquet "broadcast" au réseau réclamant l’adresse MAC de l’IP spécifiée : toutes les machines recoivent la demande mais seul l’hôte concerné répond.

Dans ce cas, neped pose la question à toutes les adresses IP du réseau, toutefois, il n’envoie pas un "broadcast" mais à la place utilise une adresse IP inexistante. Seuls les hôtes ayant leur interface en mode "promiscuous" répondront puisque les autres sont incapables de voir ces paquets.

J’ai découvert ce programme dans un article sur Internet concernant la détection d’espion. Il proposait un exemple similaire. Si vous connaissez l’URL de cet article, n’hésitez pas à m’envoyer un courrier électronique, parce que je l’ai perdu :-)

Détection de rootkits

Les rootkits "offrent" un moyen d’obtenir des privilèges supérieurs à ceux d’un utilisateur normal. Généralement, ils remplacent les fichiers binaires de notre machine par des versions susceptibles de leur fournir un accès ultérieur au système. C’est pourquoi nous devons vérifier si nous possédons toujours les originaux en utilisant chkrootkit. Il peut être installé comme suit :

apt-get install chkrootkit

Le site est à www.chkrootkit.org et il contrôle les fichiers suivants :

aliens, asp, bindshell, lkm, rexedcs, sniffer, wted, z2, amd, basename, biff, chfn, chsh, cron, date, du, dirname, echo, egrep, env, find, fingerd, gpm, grep, hdparm, su, ifconfig, inetd, inetdconf, identd, killall, ldsopreload, login, ls, lsof, mail, mingetty, netstat, named, passwd, pidof, pop2, pop3, ps, pstree, rpcinfo, rlogind, rshd, slogin, sendmail, sshd, syslogd, tar, tcpd, top, telnetd, timed, traceroute, w, write

Pour l’utiliser, tapez :

chkrootkit

Il vérifie les fichiers, recherche les sniffers et les rootkits connus. D’autres outils permettent de vérifier une éventuelle altération des "logs" (chkwtmp and chklastlog) et ifpromisc nous indique si notre interface réseau est en mode "promiscuous".

Références

Lire les pages de manuel de ces programmes est fortement recommandé. Je vous propose quelques références que j’ai utilisées. N’hésitez pas à m’envoyer vos suggestions et vos commentaires à mon adresse de courrier électronique.

- Alexander Reelsen, Securing Debian How To, version 1.4, 18 Février 2001

- Anónimo, Linux Máxima Seguridad, Pearson Educación, Madrid 2000
- Brian Hatch, Hackers in Linux, Mc Graw Hill 2001
- Jim Mellander, A Stealthy Sniffer Detector, Network Security
- Antonio Villalón Huerta, Seguridad en Unix y redes, Open Publication License, Octobre 2000
- CSI FBI Computer Crime and Security Survey, CSI Issues&Trends, Vol.7
- Who's Sniffing Your Network?, www.linuxsecurity.com/articles/intrusion_detection_article-798.html
- Root-kits et intégrité: Article de Linuxfocus

Site Web maintenu par l´équipe d´édition LinuxFocus © José Salvador González Rivera "some rights reserved" see linuxfocus.org/license/ http://www.LinuxFocus.org	Translation information: es --> -- : José Salvador González Rivera <jsgr(at)tec.com.mx> es --> en: Georges Tarbouriech <gt(at)linuxfocus.org> en --> fr: Georges Tarbouriech <gt(at)linuxfocus.org>

2005-01-14, generated by lfparser_pdf version 2.51