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

About the author:

José Salvador González Rivera ist ein aktives Mitglied der Linux Users Group von Puebla (Mexico). Er nimmt oft an Veranstaltungen teil, die Freie Software, insbesonders Linux, fördern. Er hat gerade einen Abschluß in Informatik erhalten. Sie können ihn unter sgr(at)tec.com.mx oder jsgr(at)linuxpuebla.org erreichen.

Entdeckung von Einbrüchen mit Debian GNU/Linux

Abstract:

Heutzutage werden viele Informationen digital mit elektronischer Unterstützung gespeichert und dementsprechend ist es viel leichter, über Computernetzwerke darauf zuzugreifen. Diese erlauben uns den Zugriff auf entfernte Daten, seien sie finanzieller, administrativer, militärischer, industrieller oder kommerzieller Art. Leider sind diese Daten auch ein leichtes Ziel für böswillige Menschen, die diese Daten abrufen oder zerstören wollen, weil sie noch nie etwas über moralisches Verhalten gehört haben.

Gegen das fehlende Bewußtsein können wir nicht viel tun. In diesem kurzen Artikel werde ich die Techniken und Hilfsprogramme besprechen, die wir unter Debian GNU/Linux nutzen können, um Einbrecher zu entdecken und zu verfolgen. Ich werde nicht den Inhalt der Handbücher wiederholen, sondern mich darauf konzentrieren, was im wirklichen Leben passieren kann.

Translated to English by:
Georges Tarbouriech
<gt(at)linuxfocus.org>

Einführung

Bei der Auswahl eines Linux−Betriebssystems müssen wir die verschiedenen verfügbaren Distributionen betrachten. Viele basieren auf RedHat, z. B. Conectiva (Brasilien), Hispa source (Spanien), Mandrake (Frankreich), SuSE (Deutschland), Caldera und viele andere, die den RPM−Paketverwalter benutzen. Es gibt auch Slackware, die sich mehr am traditionellen Unix orientieren und nur .tgz−Archive nutzen. "Fast" alle werden von kommerziellen Firmen entwickelt, dies gilt allerdings nicht für Debian. Debian bietet einen Paket−Verwalter (DPKG), der bei der Systemaktualisierung hilft, weil er automatisch nach Aktualisierungen aus dem Internet sucht; er prüft ferner Abhängigkeiten und macht daher die Systemadministration wesentlich einfacher und ermöglicht es, ein System in Bezug auf Sicherheitsaspekte aktuell zu halten.

Warum Debian GNU/Linux ?

Debian bietet einige wichtige Eigenschaften:

1) Es dient keinem kommerziellem Zweck und muss nicht dem Diktat von Markt−Notwendigkeiten folgen.
2) Es bietet ein gutes Fehler−Verfolgungssystem und Probleme werden in weniger als 48 Stunden behoben.
3) Von Anfang an lag die Haupt−Priorität darauf, ein vollständiges und verläßliches Betriebssystem zu entwickeln.
4) Es wird von Freiwilligen in der ganzen Welt entwickelt.

Jede neue Version bietet Unterstützung für neue Hardware−Architekturen; derzeit gibt es Unterstützung für: Alpha, ARM, HP PA−RISC, Intel x86, Intel IA−64, Motorola 680x0, MIPS, MIPS (DEC), Power PC, IBM S/390, Sparc und man arbeitet an Sun UltraSparc und Hitachi SuperH. Es ist das Linuxsystem, das die meisten Plattformen unterstützt.

Unter den existierenden Debian−Paketen gibt es verschiedene Echtzeit−Einbruchsentdeckungs−Programme, die in der Lage sind, feindliches Verhalten gegenüber einer Verbindung zu entdecken. Es gibt zwei verschiedene Typen: diejenigen, die einen Netzwerk−Angriffsversuch beobachten und diejenigen, die eine spezielle Rechneraktivität beobachten.

Host−Programme

Wir benutzen PortSentry zum Entdecken von Portscans, TripWire zum Aufdecken von Systemänderungen und LogSentry zur Logdatei−Analyse. Das erste und das letzte Programm sind Teil der TriSentry−Suite von Psionic Technologies.

Portscan−Erkennung

PortSentry beobachtet die Ports unseres Systems und führt eine Aktion (normalerweise Blockade) aus, wenn es einen Verbindungsversuch zu einem Port entdeckt, der nicht aktiviert sein soll.

Die Webpräsenz dazu findet sich unter http://www.psionic.com/products/portsentry.html und PortSentry ist verfügbar für Solaris, BSD, AIX, SCO, Digital Unix, HP−UX und Linux.

Unter Debian kann es mit dem folgenden Befehl installiert werden:

apt−get install portsentry

Es können verschiedene Aktivitätsebenen gewählt werden: der klassische Modus, der heimliche und der erweiterte Modus. Die Konfiguration wird in der Datei /usr/local/psionic/portsentry/portsentry.conf vorgenommen.

Die Hauptoptionen fand ich in einem Artikel von José Torres Luque im ES Linux Magazine und es sind die folgenden:

TCP_PORTS, hier definieren Sie die Ports, die entweder im klassischen oder im heimlichen Modus kontrolliert werden. Der Autor bietet drei Port−Listen entsprechend dem von Ihnen gewünschten

Empfindlichkeits−Level. Die Maximal−Anzahl an Ports ist 64.

UDP_PORTS, wie vorher, jedoch für UDP−Ports.

ADVANCED_PORTS_TCP, ADVANCED_PORTS_UDP, zeigen die höchste Port−Nummer an, die im erweiterten Modus benutzt werden soll. Jeder Port unter dem ausgewählten (abgesehen von den bereits ausgeschlossenen) wird überprüft. Der höchste Port kann bis zu 65535 definiert werden. Es wird jedoch empfohlen, 1024 nicht zu überschreiten, um falsche Alarme zu vermeiden.

ADVANCED_EXCLUDE_TCP, ADVANCED_EXCLUDE_UDP, enthalten eine Liste ausgenommener Ports. Die hier definierten Ports werden im erweiterten Modus nicht beobachtet. Hier definieren Sie die Ports, die normalerweise für entfernte Clients reserviert sind, und diejenigen, die keinen echten Dienst bereitstellen, z. B. ident.

IGNORE_FILE, hier geben wir den Pfad zu der Datei an, die die IP−Adressen enthält, welche zur Beobachtungszeit ignoriert werden sollen. Die lokalen Schnittstellen, einschließlich lo, sollten sich hier auch finden. Sie können auch die lokalen IP−Adressen hinzufügen.

KILL_ROUTE, hier können wir den Befehl hinzufügen, der zur Blockade des angreifenden Rechners ausgeführt werden soll. Z. B.: iptables −I INPUT −s $TARGET$ −j DROP, wobei $TARGET$ sich auf den angreifenden Rechner bezieht.

KILL_RUN_CMD, gibt einen Befehl an, der vor der Blockade des Zugriffs vom angreifenden Rechner ausgeführt wird.

SCAN_TRIGGER, definiert die Anzahl der Versuche, bevor der Alarm aktiviert wird.

PORT_BANNER, zeigt im Verbindungsmodus eine Nachricht auf den offenen Ports an.

Nach der Konfiguration muss es in einem der drei Modi mittels der folgenden Optionen ausgeführt werden: für TCP gibt es −tcp (Basis−Modus), −stcp (heimlicher Modus) und −atcp (erweiterter Modus); für UDP kann es −udp, −sudp oder −audp sein.

Integritäts−Analyse

TripWire erlaubt die Überprüfung der Integrität des Dateisystems; die Webpräsenz findet sich unter http://www.tripwire.org; TripWire ist frei erhältlich für Linux und kommerziell für Windows NT, Solaris, AIX und HP−UX.

Unter Debian kann es mit der folgenden Anweisung installiert werden:

apt−get install tripwire

Zum Speichern der Information werden zwei Schlüssel benötigt: der erste, "Unternehmens−Schlüssel", wird benutzt, um die Regeln und die Konfigurationsdateien zu verschlüsseln, und der zweite, "lokale Schlüssel", dient zur Verschlüsselung der Informationen über den Status der beobachteten Dateien.

Die Konfiguration wird einfach über die Datei /etc/tripwrie/twpol.txt vorgenommen und nach deren Anpassung können Sie TripWire wie folgt "installieren":

twadmin −m P /etc/tripwire/twpol.txt

Zum Erstellen der anfänglichen Datenbank, die den aktuellen Status der Dateien enthält, führen wir folgenden Befehl aus:

tripwire −m i 2

Um die Integrität des Dateisystems zu prüfen, geben wir diese Anweisung ein:

tripwire −m c

Die Konfigurationsdatei kann gelöscht werden, um einen Eindringling davon abzuhalten, zu erfahren, welche Dateien geändert wurden:

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

Um sie zu erstellen, falls sie benötigt werden, geben Sie folgendes ein:

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

Logdatei−Analyse

LogCheck ist Bestandteil von LogSentry und erlaubt eine sehr effiziente Log−Analyse, da es die Aktivitäten klassifiziert und Berichte darüber erstellt. Es enthält vier verschiedene Logging−Ebenen: ignorieren, ungewöhnliche Aktivitäten, Sicherheitsverletzungen und Attacken.

Die Webpräsenz findet sich unter http://www.psionic.com/products/logsentry.html. Es ist für Solaris, BSD, HP−UX und Linux verfügbar.

Unter Debian kann es mit der folgenden Anweisung installiert werden:

apt−get install logcheck

Dies installiert in /usr/local/bin das Programm logtail, um eine Liste aller bisher analysierten Logdateien zu erhalten. Außerdem werden folgende Dateien installiert:

Logcheck.sh,
Ein Skript, das die Basis−Konfiguration enthält.

Logcheck.hacking,
Enthält die Regeln, die die Aktivitätsebenen definieren.

Logcheck.ignore,
Enthält zu ignorierende Ausdrücke.

Logcheck.violations,
Enthält Ausdrücke, die als Sicherheitsverletzungen betrachtet werden.

Logcheck.violations.ignore,
Die in dieser Datei enthaltenen Ausdrücke werden ignoriert.

Sie können cron benutzen, um logcheck jede Stunde zu aktivieren: 0 * * * * /bin/sh /usr/local/etc/logcheck.sh

Netzwerk−Hilfsprogramme

Wir benutzen Snort zum Entdecken von Netzwerk−Angriffsversuchen. Die Webpräsenz findet sich unter http://www.snort.org und es ist verfügbar für BSD, Solaris, AIX, Irix, Windows, MacOS X und Linux. Unter Debian kann es wie folgt installiert werden:

apt−get install snort

Snort arbeitet in drei verschiedenen Modi: sniffer, Paket−Logger und Einbruchsdetektor.

Es kann folgende Parameter benutzen:

−l Verzeichnis
gibt das Verzeichnis an, in dem die Dateien gespeichert werden.

−h IP
definiert die Netzwerk−IP−Adresse, die wir kontrollieren möchten.

−b
zeichnet jedes Paket im Binärformat auf.

−r file
verarbeitet eine Binärdatei.

Snort Sniffer− und Paket−Logger−Modi

Im Sniffer−Modus liest es jedes durch das Netzwerk zirkulierende Paket und zeigt es auf der Konsole an, während im Paket−Logger−Modus die Daten an eine Datei in einem Verzeichnis geschickt werden.

Snort −v

Zeigt IP und Header an.

Snort −dv

Zeigt ferner die umlaufenden Daten an.

Snort −dev

Eine ausführlichere Anzeige.

Snort Einbruchs−Entdeckungs−Modus

In diesem Modus informiert uns snort über Portscans, DoS−(Denial of Service−)Attacken, Ausnutzen von Sicherheitslücken, usw. Es verläßt sich dabei auf Regeln, die es in /usr/local/share/snort findet und die Sie von der Webpräsenz abrufen können. Der Server aktualisiert diese Regeln ungefähr stündlich.

Seine Konfiguration ist sehr einfach, da sie nur aus Änderungen in der snort.conf−Datei besteht, in der wir unsere Netzwerk−Angaben und die Arbeitsverzeichnisse angeben. Ändern Sie einfach die IP:

var HOME_NET IP

Um snort auszuführen, geben Sie ein:

snort −c snort.conf

Die Log−Dateien werden in /var/log/snort gespeichert, und darin können wir die IP−Adressen der Angreifer sehen. Dies ist natürlich ein sehr kurzer Überblick über das, was Sie mit snort tun können und ich empfehle, mehr darüber zu lesen. Viele Organisationen, Magazine und Sicherheitsgruppen betrachten dieses großartige Programm als das beste Einbruchs−Entdeckungs−System für jede Unix− oder Windows−Plattform und empfehlen es. Es gibt kommerzielle Unterstützung von Firmen wie Silicon Defense und Source Fire und mittlerweile gibt es auch grafische Oberflächen, die eine ansprechendere Darstellung der Ergebnisse erlauben.

Manchmal gibt es Notfall−Situationen, die eine tiefere Analyse erfordern, da es Probleme gibt, die noch nicht in Betracht gezogen wurden und sofort gelöst werden müssen.

Diese Probleme werden üblicherweise von böswilligen Menschen oder Eindringlingen verursacht, die versuchen aus irgendwelchen Gründen auf unsere Server zuzugreifen, entweder um unsere Daten zu stehlen oder zu verändern oder um andere Maschinen von unseren Rechnern aus zu attackieren oder selbst einen Sniffer oder ein Rootkit zu installieren, die es erlauben, größere Privilegien auf jedem System zu erhalten.

Andere nützliche Programme

Sniffer−Entdeckung

Ein Sniffer ist ein Programm, das unsere Netzwerk−Schnittstelle in den unterschiedslosen Modus versetzt mit dem Ziel, den gesamten Netzwerkverkehr abzuhören. Das ifconfig−Programm versorgt uns mit der vollständigen Information über die Netzwerk−Schnittstelle:

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

Wenn das ifconfig−Programm jedoch ersetzt wurde, oder der Sniffer von einer anderen Maschine im Netzwerk arbeitet, müssen Sie die Verbindungen nach außerhalb prüfen, z. B. ob Email zu "seltsamen" Konten versandt wird oder die Logdateien des Sniffers finden.

Es gibt ein von einer spanischen Hackergruppe entwickeltes Programm namens neped, das uns Informationen über die im unterschiedslosen Modus arbeitenden Schnittstellen im Netzwerk liefert. Es ist nicht Bestandteil von Debian, kann aber von der folgenden Adresse abgerufen werden:
ftp://apostols.org/AposTools/snapshots/neped/neped.c
Hinweis: Dieser Server scheint für einige Wochen nicht verfügbar gewesen zu sein.

Die Ausführung dieses Programms gibt ungefähr folgendes Ergebnis:

```
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.
```

Wenn wir ein IP−Paket von 191.168.0.1 nach 192.168.0.2 senden möchten, müssen wir dessen MAC−Adresse wissen. Dies geschieht, indem ein Broadcast−Paket ins Netzwerk geschickt und nach der MAC−Adresse der angegebenen IP−Adresse gefragt wird; alle Maschinen erhalten die Anfrage, aber nur der richtige Host wird antworten.

In diesem Fall fragt neped jede Netzwerk−IP−Adresse, es sendet jedoch kein Broadcast−Paket, sondern benutzt stattdessen eine nicht existierende IP−Adresse. Nur die Rechner, deren Netzwerkschnittstelle im unterschiedslosen Modus arbeitet, werden antworten, weil sie die einzigen sind, die diese Pakete sehen können.

Ich fand dieses Programm in einem Artikel über Spion−Entdeckung im Netz, er enthielt ein ähnliches Beispiel. Wenn Sie die URL dieses Artikels kennen, senden Sie mir diese bitte per Email, da ich sie verloren habe :−)

Entdeckung von Rootkits

Rootkits bieten eine Möglichkeit, höhere Privilegien zu erhalten, als sie einem normalen Benutzer zustehen. Allgemein ersetzen sie unsere System−Binärprogramme mit unterschiedlichen Versionen, um später Zugang zum System zu bekommen. Darum müssen wir mittels chkrootkit überprüfen, ob wir noch über die Originale verfügen. Es kann wie folgt installiert werden:

```
apt−get install chkrootkit
```

Die Webpräsenz findet sich unter www.chkrootkit.org und es werden folgende Dateien überprüft:

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

Zur Benutzung geben Sie einfach ein:

chkrootkit

Es überprüft die Dateien und sucht nach bekannten Sniffern und Rootkits. Es gibt weitere Programme zur Überprüfung, ob Logdateien geändert wurden (chkwtmp und chklastlog) und auch ifpromisc, um herauszufinden, ob sich unsere Netzwerk−Schnittstelle im unterschiedslosen Modus befindet.

Referenzen

Ich empfehle, die Handbuchseiten dieser Programme zu lesen. Ich nenne Ihnen einige Referenzen, die ich benutzt habe. Bitte fühlen Sie sich frei, mir Vorschläge und Kommentare an meine Email−Adresse zu senden.

- Alexander Reelsen, Securing Debian How To, version 1.4, 18 February 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, octubre 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 and integrity: November 2002 Linuxfocus article

Webpages maintained by the LinuxFocus Editor team © 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 −−> de: Hermann−Josef Beckers <beckerst/at/lst−oneline.de>

2005−01−11, generated by lfparser_pdf version 2.51