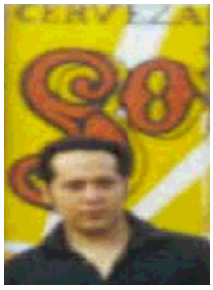
LinuxFocus article number 274
http://linuxfocus.org



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

About the author:

José Salvador González Rivera is an active member of the Linux Users Group of Puebla (Mexico). He often participates in events promoting Free Software use, particularly Linux. He just got a degree in Computers System. You can contact him at jsgr(at)tec.com.mx or at jsgr(at)linuxpuebla.org.

Intrusion detection with Debian GNU/Linux

Abstract:

Today, most of the information is digitally stored on electronic supports, and accordingly, it is much easier to access through computer networks. These last allow us to get remote data, whether it is financial, administrative, military, industrial or commercial. Unfortunately this data is an easy target for ill-intentioned people wishing to get it or to destroy it, since they have never heard about moral codes.

Against the lack of conscience there is not much we can do. In this short article I will review the technique and the tools we can use under Debian GNU/Linux to detect and track the intruders. I will not reproduce the content of users manuals since I will focus on what can happen in real life.

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

Introduction

When selecting a Linux Operating Sytem, we must consider the numerous available distributions. Most of them are based on RedHat, for instance Conectiva (Brazil), Hispa source (Spain), Mandrake (France), SuSE (Germany), Caldera and many others using the RPM package manager. There is also Slackware, trying to be closer to traditional Unix only using .tgz archives. "Almost" all of them are developed by commercial companies, but this is not true for Debian. Debian provides a package manager (DPKG) helping us in updating since it automatically looks for updates from Internet; it also checks dependencies, thus making system administration easier and allows a system to be up-to-date as far as

security patches are concerned.

Why Debian GNU/Linux ?

Debian also provides a few important features:

1) It does not have a commercial purpose and does not follow the dictates of market emergencies.
2) It does have a good bug tracking system, and problems are solved in less than 48 hours.
3) From the beginning its main priority is to develop a complete and reliable operating system.
4) It is developed by volunteers all around the world.

Every new version provides new hardware architecture support; at the moment, there is support for: Alpha, ARM, HP PA-RISC, Intel x86, Intel IA-64, Motorola 680x0, MIPS, MIPS (DEC), Power PC, IBM S/390, Sparc and they are working on Sun UltraSparc and Hitachi SuperH. It is the Linux system supporting the highest number of platforms.

Among the existing Debian packages, there are various real time intrusion detection tools able to detect hostile behavior towards a connection. There are two types of tools: the ones monitoring a network attack attempt and the ones monitoring a specific host activity.

Host tools

We use PortSentry to detect portscans, TripWire to detect system changes and LogSentry for log analysis. The first one and the last one are part of the TriSentry suite by Psionic Technologies.

Portscan detection

PortSentry monitors the ports of our system and executes an action (usually blocking) if it detects a connection attempt to a port we do not want to be listened to.

Its home page is at http://www.psionic.com/products/portsentry.html and PortSentry is available for Solaris, BSD, AIX, SCO, Digital Unix, HP-UX, and Linux.

On Debian it can be installed typing the following instruction:

apt-get install portsentry

Different activity levels can be selected: the classic mode, the stealth mode and the advanced mode. The configuration relies on the /usr/local/psionic/portsentry/portsentry.conf file

I found the main options in an article from José Torres Luque in ES Linux Magazine and they are as

follows:

TCP_PORTS, here you define the ports to be controlled either in classic mode or in stealth mode. The program's author provides three ports lists according to the sensitivity level you want to apply. The maximum number of ports is 64.

UDP_PORTS, is like the previous one but for UDP ports.

ADVANCED_PORTS_TCP, ADVANCED_PORTS_UDP, indicate the highest port number to use in advanced mode. Every port under the one selected will be checked except the ones already excluded. The highest can be defined till the 65535. However, it is recommended not to exceed 1024 to avoid false alarms.

ADVANCED_EXCLUDE_TCP, ADVANCED_EXCLUDE_UDP, provide a list of excluded ports. The ports found in this section will not be monitored in advanced mode. Here you write the connection ports usually dedicated to remote clients and the ones not providing a real service. For instance: ident

IGNORE_FILE, here we give the path of the file where we write the IP addresses to be ignored at monitoring time. The local interface, including lo, should be found there too. You can also add the local IP addresses.

KILL_ROUTE, here we can add the command to be executed to block the attacker host. For instance: iptables -I INPUT -s $TARGET$ -j DROP where $TARGET$ refers to the attacker host.

KILL_RUN_CMD, we indicate a command to be executed before blocking the access to the attacker host.

SCAN_TRIGGER, defines the number of attempts before activating the alarm.

PORT_BANNER, displays a message on the open ports in connect mode.

Once configured, it must be executed in one of the three modes using the following options: for TCP there is -tcp (basic mode), -stcp (stealth mode) and -atcp (advanced mode); for UDP it can be -udp, -sudp, -audp.

Integrity analysis

TripWire allows to check the file system integrity; the home page is at http://www.tripwire.org and it is freely available for Linux and commercial for Windows NT, Solaris, AIX and HP-UX.

On Debian it can be installed typing the following instruction:

apt-get install tripwire

To store the information two keys are needed: the first one, the "site key" is used to cipher the policies and the configuration files, and the second one, the "local key" is used to cipher the information showing

the monitored files status.

The configuration is simply done in the /etc/tripwire/twpol.txt file and once it has been adapted, you can "install" it typing:

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

To create the initial database containing the present status of the files, we execute the command:

tripwire -m i 2

To check the integrity of the file system we type the instruction:

tripwire -m c

The configuration file can be deleted to prevent an intruder from knowing which files have been changed, using this command:

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

To create them if needed, type the following:

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

Logs analysis

LogCheck is part of LogSentry and allows logs analysis in a very efficient way since it classifies and makes reports about activity and errors that require reading. It provides 4 different logging levels: ignore, unusual activity, violation of security and attack.

Its home page is at http://www.psionic.com/products/logsentry.html. It is available for Solaris, BSD, HP-UX and Linux.

On Debian it can be installed typing the following instruction:

apt-get install logcheck

This installs the logtail program in /usr/local/bin to keep a list of the already analyzed logs. The following files are also installed:

Logcheck.sh,
A script holding the basic configuration.

Logcheck.hacking,
Holds the rules defining the activity levels.

Logcheck.ignore,
Holds expressions to be ignored.

Logcheck.violations,
Holds expressions that can be considered as violation of security.

Logcheck.violations.ignore,
The expressions found in this file are to be ignored.

You can use cron to run logcheck every hour: 0 * * * * /bin/sh /usr/local/etc/logcheck.sh

Network tools

We use Snort to detect the network attack attempts. Its home page can be found at http://www.snort.org and it is available for BSD, Solaris, AIX, Irix, Windows, MacOS X and Linux.
On Debian it can be installed typing the following instruction:

apt-get install snort

It works in three different modes: sniffer, packet logger and intrusion detector.

It can use the following parameters:

-l directory
indicates the directory where to store the files.

-h IP
defines the network IP address we want to control.

-b
captures every packet as binary.

-r file
processes a binary file.

Snort Sniffer and Packet Logger modes

In sniffer mode, it reads every packet circulating through the network and displays them on the console while in packet logger mode it sends the data to a file in a directory.

Snort -v

Shows IP and headers.

Snort -dv

Also shows the data circulating.

Snort -dev

A more detailed way.

Snort Intrusion Detection mode

In this mode, snort informs us about portscans, DoS (Denial of Service) attacks, exploits, etc. It relies on rules found in /usr/local/share/snort that you can download from the website and the server updates them about every hour.

Its configuration is very simple since it consists in making changes to the snort.conf file, where we provide our network details and the working directories. Just change the IP:

var HOME_NET IP

To execute snort, type:

snort -c snort.conf

The log files are stored in /var/log/snort where we can see the IPs of the attackers. This is of course a very short review of what you can do with snort and I recommend reading more about it. Most of the organizations, magazines, security groups consider this great tool as the best Intrusion Detection system for any Unix or Windows platform and recommend it. There is commercial support from companies such as Silicon Defense and Source Fire and GUIs are beginning to appear to provide a more attractive presentation of the results.

Sometimes emergency situations appear requiring a deeper analysis since there are problems that have not been taken into account and that must be solved at once.

These problems usually are caused by ill-intentioned people or intruders trying to access our servers for one reason or the other, either stealing or altering our data or attacking other machines from ours, either installing a sniffer or a rootkit which are sets of tools allowing an intruder to gain more privileges on any system.

Other useful tools

Sniffer detection

A sniffer is a tool that changes our network interface to promiscuous mode with the goal of listening to the whole network traffic. The ifconfig command provides us with the full information about the network interface:

```
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
```

However, if the ifconfig command has been replaced or if the sniffer works from another machine in the network, you have to check the outside connections, for instance, sending mail to "strange" accounts or detecting the logs of the sniffer.

There is a tool called neped, designed by a Spanish hacker group, which informs us about the interfaces working in promiscuous mode within our network. It is not part of Debian but it can be downloaded from ftp://apostols.org/AposTools/snapshots/neped/neped.c
Note: this server seems to have been down for a few weeks.

Executing this program gives a result like the following:

```
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.
```

When sending an IP packet from 191.168.0.1 to 192.168.0.2 we need to know its MAC address. This is done sending a broadcast packet to the network asking for the MAC address of the specified IP: all the machines get the request but the right host is the only one answering.

In this case neped asks every network IP, however it does not send a broadcast but uses a non-existent IP address instead. Only the hosts having their interface in promiscuous mode will answer since they are the only ones able to see these packets.

I discovered this program in an article about spy detection found on the net. It was providing a similar example. If you know the URL for this article, feel free to send it to me by mail, since I lost it:-)

Rootkits detection

The rootkits provide a means of getting more privileges than a normal user can have. Generally, they replace our system binary files with different versions to gain a later access to the system. This is why we must check if we still have the original ones using chkrootkit. It can be installed like this:

apt-get install chkrootkit

The website is at www.chkrootkit.org and it checks the following files:

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

To use it, type:

chkrootkit

It checks the files, looks for known sniffers and rootkits. There are other tools to check log files alteration (chkwtmp and chklastlog) and also ifpromisc to tell us if our network interface is in promiscuous mode.

References

Reading these programs man pages is recommended. I provide you with a few references I did use. Please, feel free to send me suggestions and comments to my email address.

- 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

Translation information:
es --> -- : José Salvador González Rivera <jsgr(at)tec.com.mx>
es --> en: Georges Tarbouriech <gt(at)linuxfocus.org>

2005-01-14, generated by lfparser_pdf version 2.51