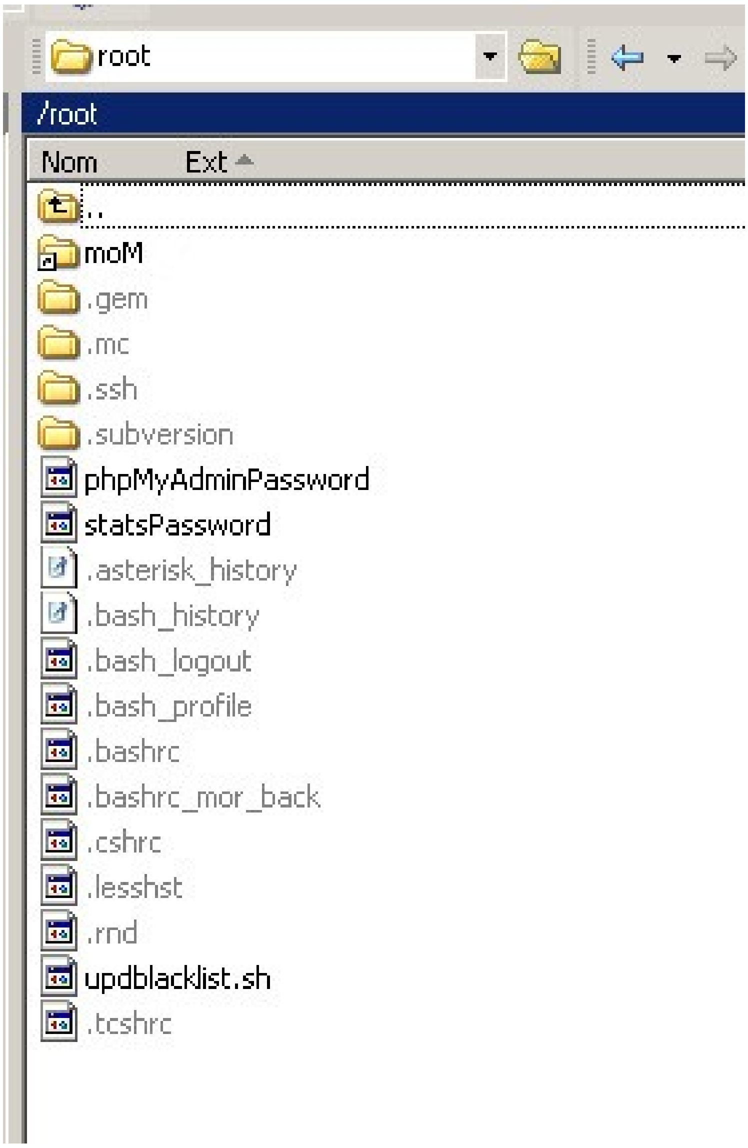
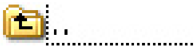
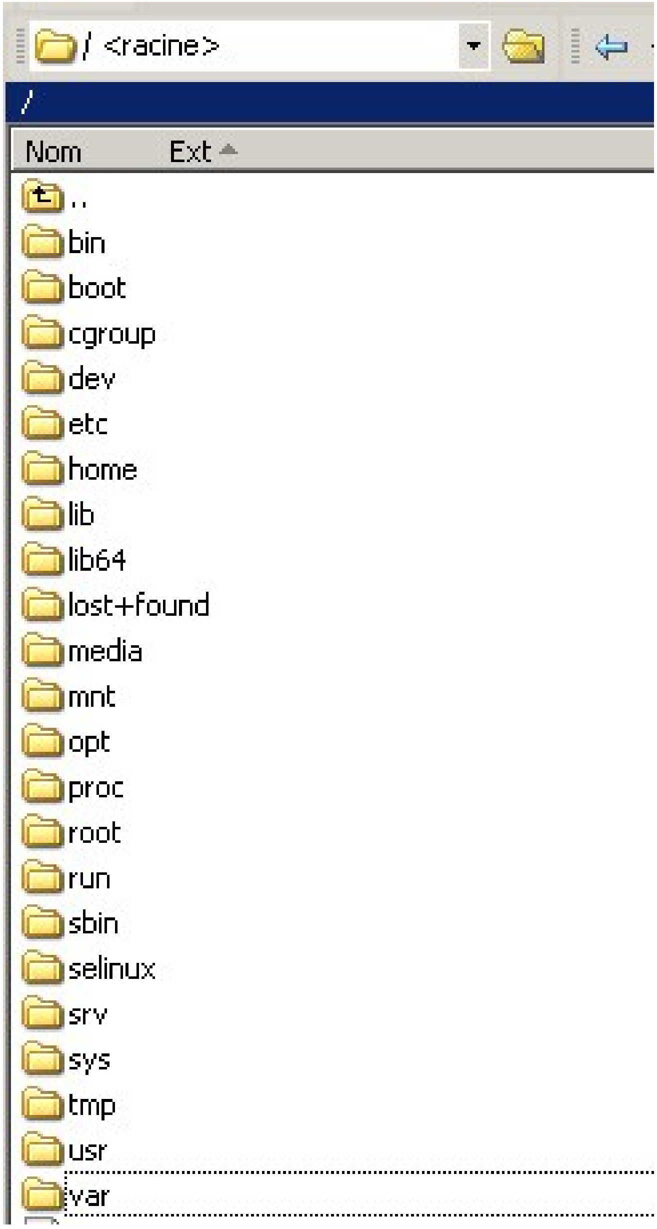
Author: Jean-Marc LAMBERT
Boulevard de Dixmude, 30 Box 10
1000 BRUSSELS
Email: navis.lambert@gmail.com
Skype account: thegreatmonarch
http://www.specialistes.be

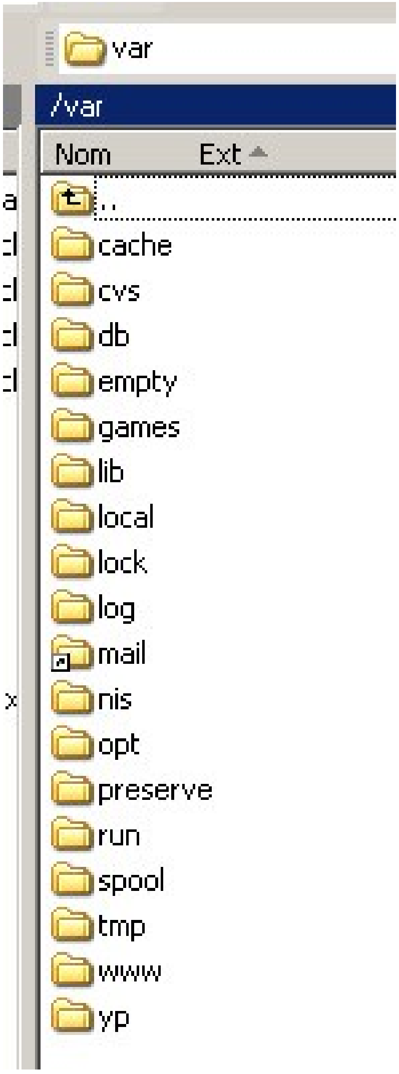
How to detect VoIP hackers

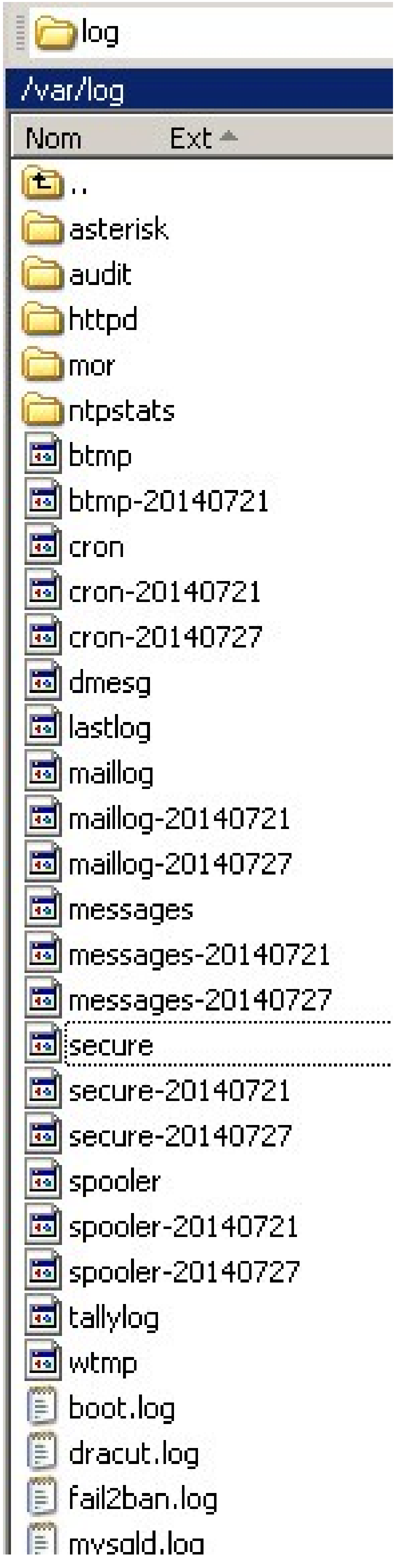
We invite you to print this document

Enter inside your server with **WinSCP** by preference.

On the rigth side of this software, you will see this: (You are in the directory “root”)	 root /root Nom Ext .. moM .gem .mc .ssh .subversion phpMyAdminPassword statsPassword .asterisk_history .bash_history .bash_logout .bash_profile .bashrc .bashrc_mor_back .cshrc .lesshst .rnd updblacklist.sh .tcshrc
Click twice on this icon on the top	 ..

No you are in the directory the main directory of the hard disk of your server	 / <racine> / Nom Ext .. bin boot cgroup dev etc home lib lib64 lost+found media mnt opt proc root run sbin selinux srv sys tmp usr var
Click twice on this icon on the top	 var

No you are in the directory “**var**”	 var /var Nom Ext .. cache cvs db empty games lib local lock log mail nis opt preserve run spool tmp www yp
Click twice on this icon on the top	 log

No you are in the directory “**log**”	 log /var/log Nom Ext .. asterisk audit httpd mor ntpstats btmp btmp-20140721 cron cron-20140721 cron-20140727 dmesg lastlog maillog maillog-20140721 maillog-20140727 messages messages-20140721 messages-20140727 secure secure-20140721 secure-20140727 spooler spooler-20140721 spooler-20140727 tallylog wtmp boot.log dracut.log fail2ban.log mysqld.log

Examine those files, by simply clicking twice with the left button of your mouse. (do not forget to close the new opened windows after you have examined the content of to)	Files: **secure** **===>** show hackers attemps on ssh access **httpd/error.log** **asterisk/messages** **===>** show hackers attemps on VoIP accounts, using port 5060
	(by the way, fail2ban would be configured to stock VoIP hackers attemps in another file, **/var/log/fail2ban.log** is rather much better)

Examples:

Hackers attemps on phpmyadmin, detected by a analysis of the file **/var/log/httpd/error.log**

Here, I clearly see that hackers has attempted to enter in my phpadmin software, using various name ===> Those ip have to be blocked.

Some of them ip are not hackers, but <u>only single webscrubbers</u>, such as 82.221.109.194 and 54.87.79.197 ===> Nothing to fear.

```
[error] [client 82.221.109.194] Directory index forbidden by Options directive: /var/www/html/
[error] [client 67.229.56.34] File does not exist: /var/www/html/web-console
[error] [client 203.188.11.132] File does not exist: /var/www/html/phpTest
[error] [client 203.188.11.132] File does not exist: /var/www/html/phpMyAdmin
[error] [client 203.188.11.132] File does not exist: /var/www/html/pma
[error] [client 203.188.11.132] File does not exist: /var/www/html/myadmin
[error] [client 54.87.79.197] Directory index forbidden by Options directive: /var/www/html/
[error] [client 37.58.100.83] File does not exist: /var/www/html/presentation/acharius
[error] [client 179.26.244.71] File does not exist: /var/www/html/phpTest
[error] [client 179.26.244.71] File does not exist: /var/www/html/phpMyAdmin
[error] [client 179.26.244.71] File does not exist: /var/www/html/pma
[error] [client 179.26.244.71] File does not exist: /var/www/html/myadmin
```

* * *

Technical note written by Jean-Marc LAMBERT www.specialistes.be