RPM - MORE THAN INSTALLING

For those of us who use a linux distribution that uses *rpm* for it's package management program are probably very used to using the *rpm* command. Especially for the installing and uninstalling of packages. But the *rpm* command has some other handy functions, here we will be looking at the verification functionality of this command. Details of each package rpm installs are stored, and *rpm* can verify packages to see if these details have been changed and which have been changed.

How Is It Done?
Well this part is simple, just use the -V switch. You can either do a specific package (*rpm -V <package name>*) or you can do every single package (*rpm -Va*). There are other switches you can use to help trim down the output you get, these are..

- *--nodeps*, used to exclude dependencies (*rpm -V --nodeps <package name>*)
- *--nofiles*, used to exclude file checks (*rpm -V --nofiles <package name>*)
- *--nomd5*, used to exclude md5 checksum checks (*rpm -V --nomd5 <package name>*)

What Am I Seeing?
The output you will get from running these commands should look something like this;

S.5....T c /etc/inetd.conf
.M....G. c /var/named/chroot/dev/null
.M..... c /var/named/chroot/dev/random
.....U.. c /var/named/chroot/etc/rndc.key
....L... c /etc/localtime

Now if you get a "." then it means that the test was passed, anything else is an indicator to show you which test failed.

- S, the file size is different
- M, the file permissions or type have changed
- 5, the md5 checksum is different
- D, there is a device mismatch
- L, there is a path mismatch
- U, the user of the file has changed
- G, the group of the file has changed
- T, the time of the file has changed
- c, means that the file indicated is a configuration file

Checking Specific Files
This functionality can also be used to check a file you may be suspicious of. If you want to check the ls command for example, you would first check the package it came with (*rpm -qf /bin/ls*), then you verify that package (*rpm -V coreutils-xxx*). If you get nothing back then the file still matches the stored details, if you get something back though, you now know how to see what has changed.

Final Thoughts
While this functionality is useful and can help, I must say that it does not negate the need for a proper host based IDS with the full suite of system checks. This verification function should be seen as an additional defense against attacks, not the total defense. Anyway, try it out, have fun, and don't forget the *man* pages.