CHECKSUMMING - WATCHING YOUR FILES

Linux is cool, linux is fun, but getting hacked is not cool. In fact, even having a legitimate user screw with your files is also no fun. And file problems are like any other problem on your box, you should know about it before anyone else. Here we are going to look at a way that you can keep an easy track of whether any of your important files have changed. We are going to checksum our files. Sounds like fun, hmmm?

What is it?
A checksum is created when you run a hashing algorithm against a file. The process runs a mathematical process which uses multiple attributes of the file to return a checksum result. It doesn't matter how big or small the file is, the checksum process will only return a checksum figure *x* characters long. We will be using the MD5 algorithm (there are others but this one ships with linux by default). We can use it by using the *md5sum* command. This command will always return a 32 character long hash/checksum result. Let's give it a try.

Let's Hash
Let's start off easy, we'll checksum our password file;

Command	*md5sum /etc/passwd*
Result	*c1ada30d1bad6c315a9fca99531fed9d /etc/passwd*

Next we'll add a new user and then run the md5sum command again;

Command 1	*useradd test*
Command 2	*md5sum /etc/passwd*
Result	*0411041fe041586c71cf206a32ae3135 /etc/passwd*

As you can see, even just the addition of a single user, the command created an entirely different hash result. Now if you had a record of the original checksum, and someone else added a new user, by running the checksum against the password file and comparing the original and new results you would be alerted to the fact that something had changed.

Making it Useful
That's great and all, but if you have 30 files you want to check, you do not want to type the command in 30 times each time you want to check them. Well let me help, here is a way to do some automagical testing using linux scripting.

1. Create directory called *check* off your root directory. All your files for this will sit there.

2. Create a file in */root/check* called *md5start* and *md5check*. Make these files owners and groups root, and give the owner all rights and nothing to anyone else. This is to ensure that only *root* can run, read or modify the files.

3. Create a file in */root/check* called *list*. Inside this file put all the files you want to check. Lets start with;
   /etc/passwd
   /etc/group
   /etc/shadow

4. Put the following lines into */root/check/md5start*;

   ```
   echo "INTIALISING MD5 CHECKSUMS..."
   md5sum `cat /root/check/list` > /root/check/list.md5
   ```

5. When you run */root/check/md5start* it will create a baseline of results for all the files specified in */root/check/list*. You will be comparing future results against these baseline results. Run it now, it will create *root/check/list.md5* and in there you should see something similar to;

   ```
   0411041fe041586c71cf206a32ae3135 /etc/passwd
   53a817891bdbbd94c4464ec2943ab77f /etc/group
   626996458be34d99994392cb317efde9 /etc/shadow
   ```

6. Put the following lines into */root/check/md5check*;

   ```
   echo "CHECK MD5 CHECKSUMS..."
   md5sum `cut -c 35- /root/check/list.md5` >> /tmp/keep
   if [ `diff /root/check/list.md5 /tmp/keep | wc -l` = "0" ]
   then
   echo "All seems fine.."
   else
   diff /root/check/list.md5 /tmp/keep
   fi
   rm -rf /tmp/keep
   ```

   What this file will do each time it is run, is redo the checksum for all the original files, compare the results to the original baseline, and then it will either say that nothing has changed or it will show you which files have changed.

7. If you run */root/check/md5check* straight away you should get a result like this;

   ```
   CHECK MD5 CHECKSUMS...
   All seems fine..
   ```

   But lets test it by adding a new test user and running it again;

   ```
   [root@syplh check]# useradd testmd5
   [root@syplh check]# /root/check/md5check
   CHECK MD5 CHECKSUMS...
   1,3c1,3
   < 0411041fe041586c71cf206a32ae3135 /etc/passwd
   < 53a817891bdbbd94c4464ec2943ab77f /etc/group
   < 626996458be34d99994392cb317efde9 /etc/shadow
   ---
   > a0807d05498d456d7a944a1b9d66e89e /etc/passwd
   > 0bf5488fae10bd02992096df113f38f6 /etc/group
   > bd5bfae3d83921e33b8ea45cbfff3d9b /etc/shadow
   [root@syplh check]#
   ```

   Here we can see that these 3 files have changed, which is normal for adding a new user.

8. If, as in the above example, the changes were valid as they were effected by you, then you can update the baseline with the new checksums by running */root/check/md5start* again. This way when you check against the baseline, you will not get alerts which are not valid. Also to add other files to check, just add them (using the full path) to */root/check/list and run the baseline script again.*

Final Words

Well I hope that this was educational and helps you in your daily administration, now you have a quick and easy way to check if any important files have changed, if you do find unauthorized changes you can now restore from safe copies or look for suspicious activity on your server. Knowing that something has changed can give you a head start on any problems. Also carry on fiddling, schedule the script to run regularly with *cron*, get it to email you the results, or even run the script against a remote server using SSH for maximum security.