REMOTE WATCHING - BETTER CHECKSUMMING

I previously did a paper on using md5 checksumming for watching the local files on your linux servers (see it here), but I was often asked about whether it is worth doing because if an attacker manages to get root on the server, he can change the record files anyway. Well there is an easy way to get around this, really. I'll give you a hint .. it is similar to keeping your log files safe. Still not? Oh well, you're in luck, I got tired of answering the same question the whole time, so I figured I would put the solution up here. The trick is to do local file checking remotely.

What do you Need?
First you need to be able to use ssh to remotely run commands on the server you want to check (see here for help on that) from the checking server, which I will call the checksum server. You will need to be able to do something like..

```
[root@10.0.0.10 check]# ssh 10.0.0.20 "uname -a"
Linux localhost 2.4.20-8 #1 Thu Mar 13 17:54:28 EST 2003 i686 i686 i386 GNU/Linux
```

Once you can do that we will need to create the home directory for our checking scripts. I generally use */admin/check*, and we will start with the the *file.lst* which is used to specify what files we will be checking, for this example I only have the following (add any others you want) in the *file.lst*..

```
/etc/passwd
/etc/shadow
/etc/group
```

Next we will look at the *setup* script. This script is called with an argument of the IP of the remote server you want to to checks on in the future. It creates a record file (using the actual IP as part of the file name) of baseline checksums which we will use to check against. The script looks like this..

```
TGT=$1
LST=/admin/check/file.lst
KEEP=/admin/check/$TGT-keep.db

rm -rf $KEEP

for x in `cat $LST`
 do
  ssh $TGT "md5sum $x" >> $KEEP
 done

chmod 600 $LST $KEEP
```

You would call it with the IP and it would create a file, like so..

```
[root@10.0.0.10 check]# ./setup 10.0.0.20
[root@10.0.0.10 check]# ls *.db
10.0.0.20-keep.db
[root@10.0.0.10 check]# cat 10.0.0.20-keep.db
4f0c9578ca38d2303fa39e98b5550e6b  /etc/passwd
de83d9e9afa30353188f531cb27fd3f6  /etc/shadow
06cca61eb8946f48f309f23c5de380c4  /etc/group
[root@10.0.0.10 check]#
```

Now that we have a baseline, lets look at the script we call to actually check the checksum on a regular basis. I call it *check* (original hey?), and you call it with the IP of the system you will be checking. The actual script looks like..

```
TGT=$1
LST=/admin/check/file.lst
TMP=/tmp/check.lt
KEEP=/admin/check/$TGT-keep.db

touch $TMP
for x in `cat $LST`
```

```
 do
  ssh $TGT "md5sum $x" >> $TMP
 done

if [ `diff $KEEP $TMP | wc -l` = "0" ]
 then
  echo "All seems fine.."
 else
  diff $KEEP $TMP
 fi

rm -rf $TMP
```

It is used as so..

```
[root@10.0.0.10 check]# ./check 10.0.0.20
All seems fine..
```

But to test it I will change one of the files we are watching, and then run it again..

```
[root@10.0.0.10 check]# ./check 10.0.0.20
3c3
< 06cca61eb8946f48f309f23c5de380c4  /etc/group
---
> ed1a14ad9174cbeeebd357e49aa84f47  /etc/group
```

So at the end of all this we should have a folder with files in it which looks a bit like this (do not forget to set the permissions) ..

```
[root@10.0.0.10 check]# pwd
/admin/check
[root@10.0.0.10 check]# ls -l
total 16
-rw-------    1 root     root          137 Jul 20 13:12 110.0.0.20-keep.db
-rwx------    1 root     root          268 Jul 20 12:45 check
-rw-------    1 root     root           35 Jul 20 12:40 file.lst
-rwx------    1 root     root          163 Jul 20 12:46 setup
[root@10.0.0.10 check]#
```

Final Thoughts
See, not at all difficult. Doing this means that even if a hacker gains root access on your machine he cannot alter the baseline checksums as they are not there. As always, the scripts are not meant to be works of art, so feel free to improve them if you want. Some suggestions could be..

- keeping the baselines in a separate folder
- using different file lists for different servers
- using more than just md5, perhaps use sha1 checksums

As always have fun and learn