

Sunday, August 27, 2006

Analyzing aide (advanced intrusion detection environment) output with PHP

Since we started hosting our sites on our own server we had some nasty cracker-attacks (most often certainly script-kiddies) causing lots of traffic by hosting crappy italian movies or by installing rootkits. To at least have a chance recognizing whether the system had been compromised we started to use aide some time ago. Aide keeps track of changes in the filesystem and provides us with a human-readable report once a day.

However, sometimes changes in the filesystem happen because of (security-)updates and not because a cracker exchanged your ps binary against his own personal version. Of course aide has no chance to identify such valid and invalid changes. 3rdPEARty's Util_AideAnalyzer is a solution to that problem - read on if you're interested.

The output aide produces when it checks the filesystem against the database looks something like this:

AIDE found differences between database and filesystem!!

Start timestamp: 2006-08-27 12:48:40

Summary:

Total number of files: 78400

Added files: 44

Removed files: 7

Changed files: 958

Added files:

...
added: /var/backups/dpkg.status.2.gz
added: /var/backups/dpkg.status.3.gz
...

Removed files:

...
removed: /var/backups/dpkg.status.4.gz
removed: /var/backups/dpkg.status.5.gz
...

Changed files:

...
changed: /usr/lib/menu
changed: /usr/lib/menu/lynx
...

Detailed information about changes:

...
File: /usr/lib/menu/lynx

Blog Export: a programmer's best friend, <http://blog.php-tools.net/>

```
Mtime : 2005-10-08 13:30:57 , 2006-08-14 01:36:12
Ctime : 2006-06-17 16:14:23 , 2006-08-26 16:19:35
Inode : 5947970 , 5948063
```

...

It lists some statistics, a list of added, removed and changed files/directories and a detailed summary of what exactly changed.

As mentioned above the summary often contains files/directories that were changed because of updates on our machine. To avoid the tedious task of separating the good ones from the bad ones you can put the output into a file and let Util_AideAnalyzer do the filtering for you. The following code snippet shows you how easy it is.

```
// necessary includes
require_once '3p/Util/AideAnalyzer.php';
require_once '3p/Util/AideAnalyzer/ItemChecker/Ctime.php';
require_once '3p/Util/AideAnalyzer/ItemChecker/Mtime.php';
require_once '3p/Util/AideAnalyzer/ItemChecker/Composite.php';

// the file containing the results of the aide-check
$file = 'rsrc/check-2006-08-27.txt';

// Analyzed-item checkers to be used in compound
// to sort out valid changes.
$checkers = array(
    new Util_AideAnalyzer_ItemChecker_Ctime(strtotime('2006-08-27 12:43:26'), 10),
    new Util_AideAnalyzer_ItemChecker_Mtime(strtotime('2006-08-27 12:43:26'), 10),
    new Util_AideAnalyzer_ItemChecker_Ctime(strtotime('2006-08-26 00:50:55'), 10),
    new Util_AideAnalyzer_ItemChecker_Mtime(strtotime('2006-08-26 00:50:55'), 10),
    new Util_AideAnalyzer_ItemChecker_Ctime(strtotime('2006-08-26 16:19:33'), 10),
    new Util_AideAnalyzer_ItemChecker_Mtime(strtotime('2006-08-26 16:19:33'), 10));

// a composite analyzed-item checker
$compChkr = new Util_AideAnalyzer_ItemChecker_Composite($checkers);

// creating an analyzer instance and performing analyzation
$analyzer = new Util_AideAnalyzer($file, $compChkr, false);
$analyzer->analyze();

// print the results
echo $analyzer->printTestResult() . "\n\n";
echo $analyzer->printDebugInformation();
```

You see that I create six item-checker objects (for each date one mtime and one ctime checker) which will sort out items whose mtime/ctime property changed at the given time (with a bias of 10 seconds, which is the second parameter). Each of those three timestamps represents a date/time when I updated the system. Thus the following change aide noticed:

```
File: /usr/lib/menu/lynx
Mtime : 2005-10-08 13:30:57 , 2006-08-14 01:36:12
Ctime : 2006-06-17 16:14:23 , 2006-08-26 16:19:35
Inode : 5947970 , 5948063
```

is a valid one, now (compare the ctime-property and keep the 10 second bias in mind).

The rest is as simple as cooking coffee. I take the \$checkers array and create a composite checker implementing the Util_AideAnalyzer_AnalyzedItemChecker interface. Then I create an Util_AideAnalyzer instance and call the analyze() method. The rest is just printing out the filtered information which will look like that:

Invalid items:

...
File: /etc/postfix/prng_exch
Directory: /root
File: /root/.viminfo
File: /root/.bash_history
File: /root/.rnd
File: /home/luckec/.bash_history
...

Valid items:

Directory: /etc
Directory: /etc/alternatives
...

Analyzation statistics:

Number of added items : 44
Number of removed items : 7
Number of changed items : 958

Number of valid items : 904
Number of invalid items : 54

Number of added/removed/changed items: 1009
Number of valid/invalid items : 958

I think you will agree that checking the validity of the remaining changed files/directories (invalid items) is done pretty fast as there are only a few left.

If you like what you read feel free to download and install Util_AideAnalyzer. Type

```
pear channel-discover 3rdparty.net
```

Then you will be able to install the package by using:

```
pear install 3p/Util_AideAnalyzer
```

Have phun!

Posted by luckec in PHP at 22:47

>> Since we started hosting our sites on our own server we had some nasty cracker-attacks (most often certainly script-kiddies) causing lots of traffic by hosting crappy italian movies or by installing rootkits.

What about hiring a professional administrator instead of writing an aide analyzer?
Anonymous on Aug 28 2006, 12:26

Ummmm ok. What exactly do you mean?

(a) Professional admins do not need a tool like aide?

(b) Professional admins enjoy looking manually through lengthy logs even if they had the chance to make their life easier?

(c) Something else?

Anonymous on Aug 28 2006, 13:46

The sentence i quoted, suggest the php-tools.net servers has been hacked more than once.

There i one conclusion for me, instead of thinking about how to parse and evaluate a logfile of a tool which only detects a hack, the hack itself should be prevented by hiring a professional administrator.

Further, i for myself have removed every pear package from this site, because of the following fact:

If this site has got hacked often enough to think about writing an aide parser, i do not want possible tampered code from your pear repository on my servers anymore. - At least not until i had the time to inspect every package by myself.

Remember, security is only as strong as the weakest part in the chain, and from reading the first sentence, which suggest a total lack of security sense the part has to be removed from the chain.

Anonymous on Aug 28 2006, 14:35

Hi Eremit,

what you understood about the the post regarding that our server had been hacked is correct. But apart from that you have quite an ability to pervert the facts!

You can be damn sure that there is none of the pat nor the 3rdPEARty code tampered in any way! It is a pity if you think you have to uninstall those packages (BTW: The sources are open and readable to anyone, just try it).

Furthermore, you seem to be pretty confident that we're not very skilled in administration concerns. Be sure, whenever the server got hacked (which happened quite some time ago) we did of course setup everything from scratch and checked everything. I'm properly convinced that a lot of people had a cracker on their server who can be considered good administrators. Anyhow, I see no sense in arguing with you about those skills.

And finally let me make one last thing clear: I didn't write the AideAnalyzer because I fear each day that the system could have been hacked because I am such a poor admin. The only reason I did this is because it saves me some minutes every time I analyze the aide-output (and maybe some other people, too).

I definitely agree with you that a rock-solid and secure system is a must have. But after all I think one is better off with aide knowing the system has been compromised than someone who thinks he owns a secure system of which he doesn't know what's going on behind the scenes.

Anonymous on Aug 28 2006, 20:28

Hi Luckec,

first please take my apology. I was reading out of your post something like:

"We got hacked several times now, and to detect a successful hack we use aide, without rethinking anything of our base setup."

The last part of the sentence was something I interpreted into your post, without it being actually there.

Anonymous on Aug 29 2006, 07:56