Minute 16/12/2010

Writer: Tan

Content:

Discuss about HIDS:

Tripwire : To be eliminated <Money ^^>

Under consider:

OSSEC: <Windows server: N/A>

SAMHAIN:

We will use tool , not develops by ourselves.

What is the “server data” dataflow:

File Integrity:

Small size <because of using Hash function>

File system Databases are stored at server => hard to be attack

But:

We don’t know what are changed on those files….

Log File:

We will know more details about the changes of our system file , info about some special action such as user logon/logoff…

But:

We must face with the problem of log files size

Easy to be attacked by hacker …

Both:….

Decision:

<Log File>

Task:

Each member does some research about:

Windows logs file types <Maybe we will use Windows Event Viewer>

Linux logs file types : some main logs file types in common Linux/Unix versions.