SANE 2006 – CF Engine 2

15/05/06 11:03

< We gaan door na de lunch pauze >

Helaas ging er iets fout met de opname. Word ging hangen... :(

Peer groupings = a group of autonomous CFE clients working together. To begin with, there is no structure whatsoever. You just need a list of all clients in your network.

One possible application for this is a “neighborhood watch” where systems monitor each other.

Appointing a leader is not necessary, but it will ensure that you will need to open less holes in your firewall.

Chapter 7: values and functions

CFE knows two “variables” -> macros and classes. The first is defined in the control section and the latter is defined in the classes section.

Lvalue = Left value = on the left of the “equals” sign. Rvalue is the opposite :p

There are three types of Lvalues -> scalar, array, list. Arrays are currently not used in CFEv2.

When using the IPRange directive you should be able to use dashes (to define ranges) in each octet of the address.

Chapter 8: interaction with sub-programs

Don’t use modules when you can use CFE functions. These functions were created to be convergent, so they ensure proper functioning of your configuration.

In a method definition the *sendclasses* directive only passes on classes that are applicable to the system running the method.

The *alert* action section cannot use the class *any*.

Methods are wonderful to use as a faux package manager or to read remote, private databases. <3 However, remote methods are quite tricky and are actually only included as a proof-of-concept.

Remote methods are not sent as requests, but rather advertised. Other autonomous systems then fulfill the request on a voluntary basis.

< na de koffie pauze > Ik heb helaas een paar minuten opname gemist. We gaan door bij de case over password synchronisatie.

Niet veel te melden voorlopig :) Zit eigenlijk te surfen... *schaam*

More examples of filters can be found on the CFE website. Apparently people –are- willing to share these...

RESEARCH: try and research the whole key-exchange bit. How do you automate the opening and closing of “trust keys”?

Debugging security issues should be done on the server side since CFE does not send error messages back across the network. This in order to not provide crackers with valuable information.

CFE actually keeps track of your running system to see what is normal, as opposed to depending on your view (entered in the policy). Resetting what the system has “learned” is as easy as deleting the database.