Suricata - Feature #423

pkt_data keyword

03/19/2012 03:10 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Xavier Lange
Category: 
Target version: 1.4beta3
Effort: 
Difficulty: 
Label: 

Description
Should be simple as file_data just sets a flag during parsing, so pkt_data should unset this flag.

History
#1 - 03/23/2012 10:32 AM - Victor Julien
- Due date set to 03/27/2012
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Xavier Lange

DetectFiledataSetup sets the per signature flag SIG_FLAG_INIT_FILE_DATA when "file_data" is encountered in a rule. The pkt_data code should simply unset it.

Please add some unitests that show this parsing in action.

#2 - 03/28/2012 09:42 AM - Victor Julien
- Tracker changed from Bug to Feature

#3 - 04/04/2012 08:53 AM - Victor Julien
- Target version changed from 1.3beta1 to 1.3beta2

#4 - 06/07/2012 03:10 AM - Victor Julien
- Target version changed from 1.3beta2 to 1.4

#5 - 08/23/2012 03:07 AM - Victor Julien
- Target version changed from 1.4 to 1.4beta2

#6 - 08/23/2012 03:17 AM - Victor Julien
- Due date changed from 03/27/2012 to 08/31/2012

#7 - 09/04/2012 01:25 PM - Xavier Lange
This is a feature request for something done in Snort and it essentially forces pattern match from the beginning of a stream, not its "body".

As for unit testing this rule, from Victor:

check for example DetectHttpServerBodyTest01. It parses a sig and checks the internal state of the Signature structure. In such a test you can for example test 'file_data; content:"http"; pkt_data; content:"packet";'

This should result in 2 sigmatches, one in the http server body list, the other in the pattern list.

#8 - 09/12/2012 03:08 AM - Xavier Lange
Getting closer. I have a pkt-data.c in place and compiling but I need to get a handle on the sig (out of the engine) so I can check that the flag is set properly. Any tips on that?
What are you trying to do? Can you show some code?

Hey Victor, why do you think the engine is not loading the rule in to sig_lists? Do I need to do something else after calling SigInit?

Take a look at the most recent branch diff. It shows a fully-registered unit test. [https://github.com/xrl/suricata/compare/keyword-pkt_data](https://github.com/xrl/suricata/compare/keyword-pkt_data)

I run the unit test with this command: "./src/suricata -u -U PktData"

Right, SigInit doesn't do that. Other tests use it like this:

```c
    de_ctx->sig_list = SigInit(de_ctx,"alert tcp any any -> any any {msg:"HTTP TEST"; content:"Host: one.example.org"; offset:20; depth:39; sid:1;}";
    if (de_ctx->sig_list == NULL) {
```

- Due date changed from 08/31/2012 to 10/05/2012
- Target version changed from 1.4beta2 to 1.4beta3

- Status changed from Assigned to Closed
- % Done changed from 0 to 100