Wikiprint Book

Title: Getting started with a simple analysis example

Subject: ThirdEye - simpleanalysis

Version: 25

Date: 09/15/14 11:40:20

Table of Contents

Getting started with a simple analysis example

The following is a step-by-step guide for performing a basic analysis task using the semantic analysis framework.

Analysis Problem

Given a sample packet capture, our objective is to

1. Understand the TCP connection setups in the capture.
2. Understand the connection teardowns from the packet capture.
3. Additionally, for each teardown we want to know about the specific type of teardown.

We will demonstrate the analysis using an existing model of TCP connection setup and TCP connection teardown from the knowledge base to analyze the packet capture.

Initial setup

Install

Download and install the latest release.

Get the capture

Create a data directory under SAF and download a sample packet capture from here.

```
$ cd /path/to/SAF/
$ mkdir data
```

Normalize packets to events

To normalize events we will use the p2db tool to convert the raw packets to **PACKET_TCP** events and dump them to a SQLite database. If you haven't already, please follow the installation instructions for p2db.

```
$ cd /path/to/SAF/data/
$ p2db sample2.pcap sample.sqlite
```

The tool output is as follows and indicates that 78 TCP packets (and others) were converted and stored to the SQLite database sample.sqlite. For this example we are only interested in the TCP packets.

```
Creating database 'sqlite3 sample2.sqlite .databases'
seq  name             file
---  ---------------  ----------------------------------------------------------
0    main             /home/neoblitz/workspace/@isi/SAF/data/sample2.sqlite
journal_mode = off

Created database !
Created Tables !
Starting to read packets - time : Thu Jun  9 15:05:07 2011
Transaction Size:  20000 packets

Statement preparation successful for PACKET_UDP
Statement preparation successful for PACKET_TCP
Statement preparation successful for PACKET_DNS
Cleaning up...
Committing pending transactions...
```

```
Freeing pcap resources...
Freeing sqlite resources...

Started processing packets at : Thu Jun  9 15:05:07 2011
Finished processing packets at: Thu Jun  9 15:05:07 2011


========
SUMMARY
========
Processed 9220 records in 0 secs (0.000000 sec per record)
Time of First Event: 1238567803
 Time of Last Event: 0
        TCP Packets: 78
        UDP Packets: 8439
        DNS Packets: 6
       ICMP Packets: 0
         IP Packets: 0
 Invalid IP Packets: 514
       IPv6 Packets: 0
    Unknown Packets: 183
```

The output SQLite database contains the following:

```
sqlite> select * from PACKET_TCP;
eventno     eventtype   timestamp   timestampusec  origin      sipaddr       dipaddr         sport
----------  ----------  ----------  -------------  ----------  ------------  -------------  -------
1           PACKET_TCP  1267192686  584044         localhost   192.168.3.65  188.72.243.72  1032
2           PACKET_TCP  1267192686  693493         localhost   188.72.243.7  192.168.3.65   80
3           PACKET_TCP  1267192686  694094         localhost   192.168.3.65  188.72.243.72  1032
4           PACKET_TCP  1267192686  694921         localhost   192.168.3.65  188.72.243.72  1032
5           PACKET_TCP  1267192687  8814           localhost   188.72.243.7  192.168.3.65   80

...
<output snipped ... another 1100 events displayed>
```

Model the problem by using existing models from database

Instead of writing our model for now, we will directly use the TCP connection setup model from the knowledge base to analyze our data. The TCP connection setup model captures the basic behavior of the TCP three way handshake abstractly, that is, independent of any data set specific attributes and values. The model exists in the database under SAF/knowbase/net/base_proto/tcpconnsetup.b

---

Analysis using SAF

Analysis of TCP connection setups

Finally, analysis using the SAF involves inputting the model (**--model tcpconnsetup.b**) and SQLite database of events (**--db sample.sqlite**) to the framework as shown below. The *--pretty* flag enables outputting the results in a pretty columnar format.

```
$ cd /path/to/SAF
$ ./saf.py --model knowbase/net/base_proto/tcpconnsetup.b --db data/sample.sqlite --pretty
```

The following output from the framework shows that:

1. There are **5** matching TCP 3-WAY handshakes found.
2. Each instance is separated by a line and contains the SYN, SYN-ACK and ACK events that make up each instance.
3. Additionally, each instance contains an annotation (**TCP_CONNSETUP.3way_handshake**) that identifies the corresponding behavior definition that was satisfied by each instance.

You can manually confirm this output by opening the raw-data in wireshark and counting the number of actual connections.

```
##############################################
#    Semantic Analysis Framework - v0.1a     #
##############################################

Reading input event database 'data/sample2.sqlite' ..
Found 8523 events in database
       PACKET_TCP - 78 events [ Wed Apr  1 06:36:47 2009 (1238567807) to Wed Apr  1 06:43:56 2009 (1
       PACKET_DNS - 6 events [ Wed Apr  1 06:36:55 2009 (1238567815) to Wed Apr  1 06:36:56 2009 (12
Creating temporary directory for storing state /tmp/temp
Initializing global symbol table..
Reading and initializing from the knowledge base 'knowbase'..
Parsing specified model : 'knowbase/net/base_proto/tcpconnsetup.b'..
Processing model TCP_CONNSETUP
   QUALIFIER matched 78 instances
   State tcp_pkt_syn .. found 13 instances
   State tcp_pkt_synack .. found 7 instances
   State tcp_pkt_ack .. found 7 instances
 Behavior 3way_handshake .. found 7 instances
Model TCP_CONNSETUP satisfied by 7 instances

==================================
Instances satisfying TCP_CONNSETUP
==================================

Total Matching Instances: 7

-------------------------------------------------------------------------------------------------------
    eventno      |    timestamp     |  timestampusec   |     sipaddr      |     dipaddr      |
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
       5         |    1238567807    |      746028      |  192.168.1.101   |  192.168.1.102   |
       8         |    1238567810    |      588954      |  192.168.1.102   |  192.168.1.101   |
       9         |    1238567810    |      588978      |  192.168.1.101   |  192.168.1.102   |
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
       17        |    1238567810    |      609792      |  192.168.1.101   |  192.168.1.102   |
       19        |    1238567810    |      618788      |  192.168.1.102   |  192.168.1.101   |
       20        |    1238567810    |      618804      |  192.168.1.101   |  192.168.1.102   |
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
       28        |    1238567810    |      632058      |  192.168.1.101   |  192.168.1.102   |
       30        |    1238567810    |      640885      |  192.168.1.102   |  192.168.1.101   |
       31        |    1238567810    |      640901      |  192.168.1.101   |  192.168.1.102   |
```

```
-------------------------------------------------------------------------------------------------------
                                                    Behavior: TCP_CONNSETUP.3way_handshake
      39        |    1238567810    |      655166      |  192.168.1.101   |  192.168.1.102   |
      41        |    1238567810    |      661959      |  192.168.1.102   |  192.168.1.101   |
      42        |    1238567810    |      661973      |  192.168.1.101   |  192.168.1.102   |
-------------------------------------------------------------------------------------------------------
                                                    Behavior: TCP_CONNSETUP.3way_handshake
      51        |    1238567815    |      777635      |  192.168.1.101   |  66.114.124.141  |
      52        |    1238567815    |      854902      |  66.114.124.141  |  192.168.1.101   |
      53        |    1238567815    |      854941      |  192.168.1.101   |  66.114.124.141  |
-------------------------------------------------------------------------------------------------------
                                                    Behavior: TCP_CONNSETUP.3way_handshake
      62        |    1238567815    |      951377      |  192.168.1.101   |  75.126.138.202  |
      63        |    1238567815    |      988428      |  75.126.138.202  |  192.168.1.101   |
      64        |    1238567815    |      988450      |  192.168.1.101   |  75.126.138.202  |
-------------------------------------------------------------------------------------------------------
                                                    Behavior: TCP_CONNSETUP.3way_handshake
      72        |    1238567816    |      47398       |  192.168.1.101   |   208.78.69.70   |
      74        |    1238567816    |      129519      |   208.78.69.70   |  192.168.1.101   |
      75        |    1238567816    |      129559      |  192.168.1.101   |   208.78.69.70   |
-------------------------------------------------------------------------------------------------------
```

You will notice that the number of attributes for PACKET_TCP events is way more than the ones that are shown here. This is due to the definition of the model which can specify the number of attributes that are exported by each model. In the case of our model, the following is defined.

```
TCP_CONNSETUP(eventno,timestamp,timestampusec,sipaddr,dipaddr,sport,dport,tcpflags) =  3WAY_HANDSHAK
```

Analysis of TCP connection teardowns

Similarly, we use the TCP connection teardown model over the same dataset to understand the connection teardown.

```
$ cd /path/to/SAF
$ ./saf.py --model knowbase/net/base_proto/tcpconntdown.b --db data/sample.sqlite --pretty
```

Following output is produced. The type of teardown in easily inferred by the annotations that are provided above each instance and correspond to the behavior names defined in the model.

```
###############################################
#    Semantic Analysis Framework - v0.1a      #
###############################################

Reading input event database 'data/sample2.sqlite' ..
Found 8523 events in database
       PACKET_TCP - 78 events [ Wed Apr  1 06:36:47 2009 (1238567807) to Wed Apr  1 06:43:56 2009 (1
       PACKET_DNS - 6 events [ Wed Apr  1 06:36:55 2009 (1238567815) to Wed Apr  1 06:36:56 2009 (12
Creating temporary directory for storing state /tmp/temp
Initializing global symbol table..
Reading and initializing from the knowledge base 'knowbase'..
Parsing specified model : 'knowbase/net/base_proto/tcpconntdown.b'..
```

```
Processing model TCP_CONNTDOWN
   QUALIFIER matched 78 instances
   State tcp_pkt_fin .. found 0 instances
 Behavior full_teardown .. found 0 instances
   QUALIFIER matched 78 instances
   State tcp_pkt_piggyfin .. found 10 instances
   State tcp_pkt_finack_from_d .. found 3 instances
   State tcp_pkt_ack_from_s .. found 2 instances
 Behavior full_teardown_piggyfin .. found 2 instances
   QUALIFIER matched 78 instances
   State tcp_pkt_piggyfin .. found 10 instances
   State tcp_pkt_ack_from_d .. found 9 instances
 Behavior half_close .. found 8 instances
   QUALIFIER matched 78 instances
   State tcp_pkt_syn .. found 13 instances
   State tcp_pkt_rst_sd .. found 0 instances
 Behavior close_by_rst .. found 0 instances
Model TCP_CONNTDOWN satisfied by 10 instances

==================================
Instances satisfying TCP_CONNTDOWN
==================================

Total Matching Instances: 10

-------------------------------------------------------------------------------------------------
    eventno      |    timestamp     |  timestampusec   |     sipaddr      |     dipaddr      |
-------------------------------------------------------------------------------------------------
                                                      Behavior: TCP_CONNTDOWN.full_teardown_piggyfin
       57        |    1238567815    |      933598      |  66.114.124.141  |  192.168.1.101   |
       59        |    1238567815    |      933677      |  192.168.1.101   |  66.114.124.141  |
       66        |    1238567816    |       6743       |  66.114.124.141  |  192.168.1.101   |
-------------------------------------------------------------------------------------------------
                                                      Behavior: TCP_CONNTDOWN.full_teardown_piggyfin
       78        |    1238567816    |      216303      |  192.168.1.101   |   208.78.69.70   |
       79        |    1238567816    |      216481      |   208.78.69.70   |  192.168.1.101   |
       80        |    1238567816    |      216502      |  192.168.1.101   |   208.78.69.70   |
-------------------------------------------------------------------------------------------------
                                                         Behavior: TCP_CONNTDOWN.half_close
       16        |    1238567810    |      609555      |  192.168.1.101   |  192.168.1.102   |
       18        |    1238567810    |      618322      |  192.168.1.102   |  192.168.1.101   |
-------------------------------------------------------------------------------------------------
                                                         Behavior: TCP_CONNTDOWN.half_close
       27        |    1238567810    |      631867      |  192.168.1.101   |  192.168.1.102   |
       29        |    1238567810    |      640296      |  192.168.1.102   |  192.168.1.101   |
-------------------------------------------------------------------------------------------------
                                                         Behavior: TCP_CONNTDOWN.half_close
       38        |    1238567810    |      655012      |  192.168.1.101   |  192.168.1.102   |
       40        |    1238567810    |      660640      |  192.168.1.102   |  192.168.1.101   |
-------------------------------------------------------------------------------------------------
                                                         Behavior: TCP_CONNTDOWN.half_close
```

```
      45        |    1238567815    |      647476      |  192.168.1.101   |  192.168.1.102   |
      48        |    1238567815    |      651075      |  192.168.1.102   |  192.168.1.101   |
-------------------------------------------------------------------------------------------------
                                                      Behavior: TCP_CONNTDOWN.half_close
      57        |    1238567815    |      933598      |  66.114.124.141  |  192.168.1.101   |
      58        |    1238567815    |      933618      |  192.168.1.101   |  66.114.124.141  |
-------------------------------------------------------------------------------------------------
                                                      Behavior: TCP_CONNTDOWN.half_close
      59        |    1238567815    |      933677      |  192.168.1.101   |  66.114.124.141  |
      66        |    1238567816    |       6743       |  66.114.124.141  |  192.168.1.101   |
-------------------------------------------------------------------------------------------------
                                                      Behavior: TCP_CONNTDOWN.half_close
      69        |    1238567816    |      29493       |  192.168.1.101   |  75.126.138.202  |
      73        |    1238567816    |      71145       |  75.126.138.202  |  192.168.1.101   |
-------------------------------------------------------------------------------------------------
                                                      Behavior: TCP_CONNTDOWN.half_close
      79        |    1238567816    |      216481      |   208.78.69.70   |  192.168.1.101   |
      80        |    1238567816    |      216502      |  192.168.1.101   |   208.78.69.70   |
-------------------------------------------------------------------------------------------------
```