snorbert

About

woanware is the name for a set of tools and applications I have written. The majority of the tools/applications are related to networking, network security, application security or digital forensic tasks.

Introduction

snorbert is a snort data viewer, loosely based on snorby. It is written in C# and uses .Net 4.5.

The aim of the application is to provide a fast, usable interface for accessing snort data. Depending on the snort deployment, the underlying data set can be extremely large, so care has been taken to optimise the data access.

Features

- Paged data access
- Configuration for multiple snort instances
- Signature based grouping of events
- User configurable searching
- Correlation of snort signatures to events for easy viewing of the signatures

Third party libraries

- ObjectListView : Data viewing via lists
- Be.HexEditor : HEX view of packet data
- IP Address Control : Easy validation of IP addresses
- ManagedEsent : Fast storage of rule data
- MySql : Access to the snort MySQL databases
- Utility (woanware) : My helper library

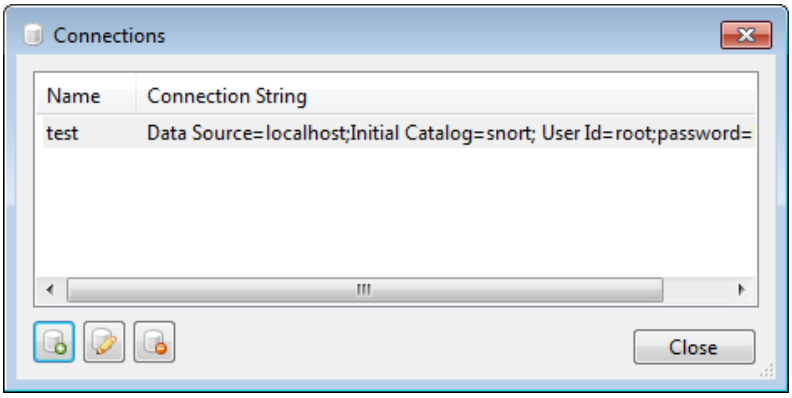
Requirements

- Microsoft .NET Framework v4.5

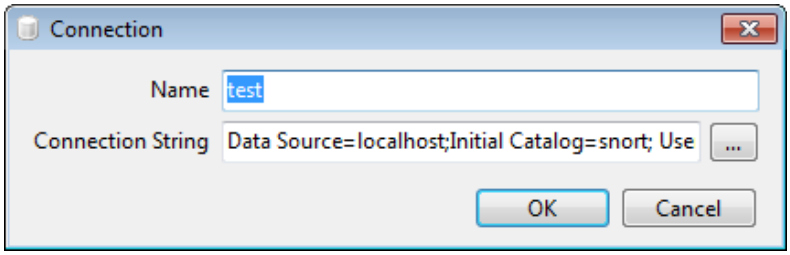
Usage

Connections

snorbert can connect to multiple snort instances. The database connections need to be defined for each snort instance. The database connections can be configured via the Tools->Connections menu. The Connections window will display all of the configured snort databases.



The Connections window allows the adding, editing and deleting of database connections. The Connection window is shown below:



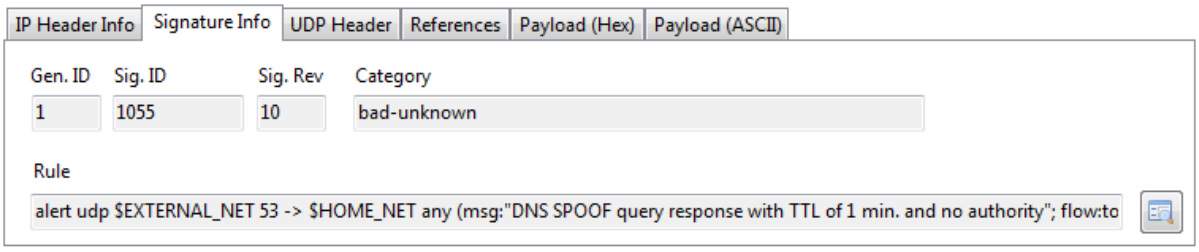
The ellipsis button will perform a connection test for the currently configured connection string. The connection string must be in the following format:

```
Data Source=#IP#;Initial Catalog=#Database#; User
Id=#username#;password=#password#; default command timeout=60;
```

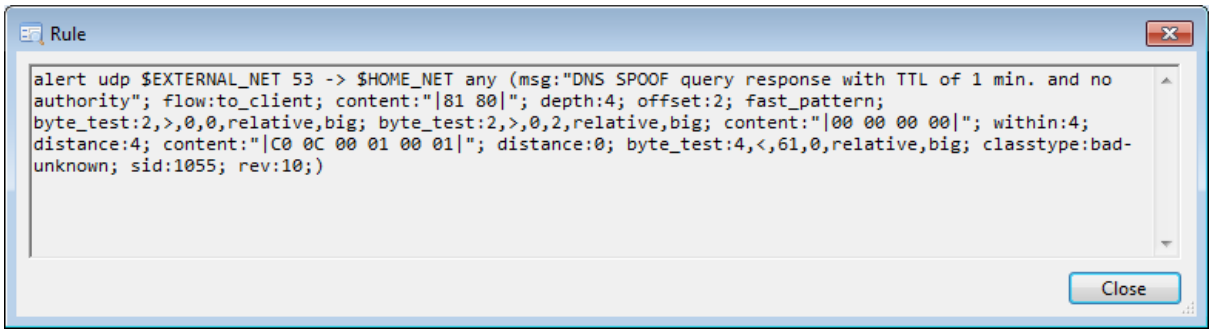
Note that the default command timeout can be configured for each instance, this allows for slow network connections, large datasets etc.

Rules/Signatures

The snort rule set can be imported into snorbert, this allows the signature/rule to be displayed that relates to a specific event. The screenshot below shows the signature details:



To view the full rule in a separate window, click the button next to the rule, the following window will be displayed:

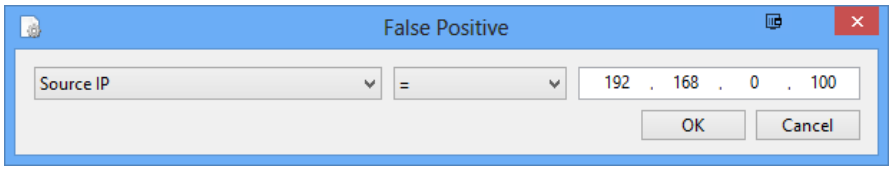


The rules can be imported manually via the Tools->Import Rules menu or they can be copied into the Rules directory located in the applications installation directory. The automated import will check the file names/timestamps and only import new or changed files.

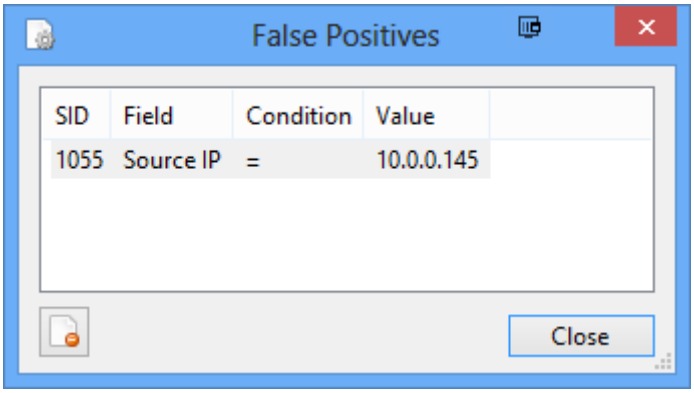
False Positives

To help reduce the amount of “noise” returned by snort it is possible to aid false positive filters to the data set. The false positive filters are only application to the Rules tab since they relate a filter to a specific snort rule.

To add a false positive filter, load the events for a rule, then right click on the Event line within the list. A context menu will be displayed, choose the **Hide** item. The following window will be displayed:



The values will be pre-populated using the event selected in the list; this is to speed up the process. To remove false positive filters, use the Tools->False Positive menu item, which will display the False Positives window:



Select the false positive filter that you want to delete and use the delete button on the window or use the DEL key.

History

v1.0.1

- Modified the Rules database to store within the users local app data directory. This prevents issues when running with multiple users logged into the same time. Thanks DanO for reporting this on behalf of TomB ;-)
- Modified the Connections config file to store within the users local app data directory
- Modified the Settings config file to store within the users local app data directory
- Modified the HEX view context menu to allow copying of the HEX with and without spaces
- Added the ability to filter out particular events e.g. false positives. The functionality only applies on the Rules list. A false positive entry relates to a particular attribute e.g payload LIKE “test” or Source IP = 192.168.0.100. The false positive data is stored in an XML file under the users local app data directory.

v1.0.0

- Help file added
- Public release

v0.0.3

- Updated the rule import to update existing rules
- Added event handlers for Sensor user control so that messages can be transmitted back to the main UI
- Modified the Event user control to just use next/previous paging as a record count takes too long
- Added the ability to search on Sensor
- Added the ability to search on Protocol (TCP, UDP and ICMP)
- Moved all of the querying to a separate object so that the queries can now be easily run on a background thread
- Increased the granularity of the Page Limits, for very slow connections!
- Moved the “Connections.xml” and “Settings.xml” to a new “Config” folder
- Moved all of the hard coded SQL queries to a new config file (“Sql.xml”). The file resides in the new “Config” folder
- Added TCP flag decoding to the events list. The events is displayed on the Event, Rules and Search tabs

v0.0.2

- Fixed context menu Source Port copy
- Fixed import rules error which resulted in a Disposed object exception
- Added To Date/Time filtering. Thanks TomB
- All controls/lists clear when the Rules combo is refreshed
- Fixed “No Object in Sequence” error when editing an existing connection
- Moved the Connections/Page Limit controls to the toolbar

- Added new Events tab, which displays all events, ordered by event.timestamp, includes paging support
- Rule files are now copied to the Import directory when a manual rule import is performed. This will ensure that the Settings file will contain the file details and reimport will not occur
- Add new Search tab, which allows for user configurable searching on the key fields
- Re-implemented UI code base using User Controls rather than one massive code dump in the main window
- Added custom context menu to the HEX control to allow the copying of the HEX value as well as the ASCII
- Added Sensor tab which displays information relating to the snort sensors

v0.0.1

- Initial release