

 woanware

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
- [CsvHelper](#): Used to export to delimited files
- [Utility](#) (woanware) : My helper library
- [NPoco](#): Data access
- [SQL Server CE](#): SQL Server CE used for rule storage

Requirements

- Microsoft .NET Framework v4.5

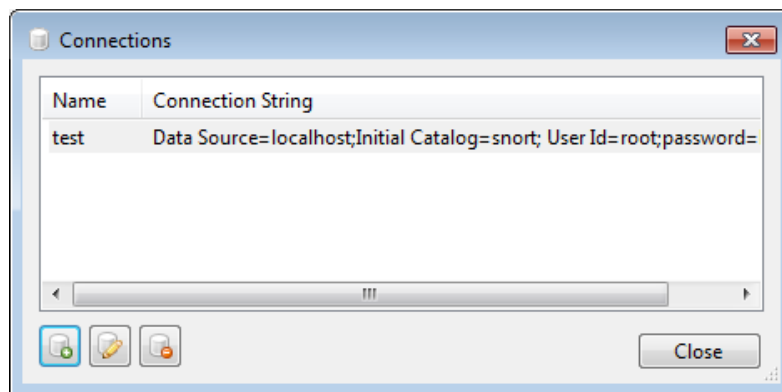
Database

snorbert requires a change to the snort/barnyard database schema. Currently the change simply consists of one new table (Exclude). To add the new table just run the Create.sql file under the database directory of the repository. The table facilitates the ability to exclude particular rules, IP addresses etc.

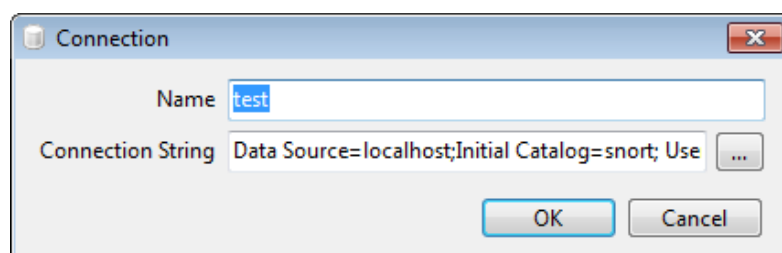
Usage

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:



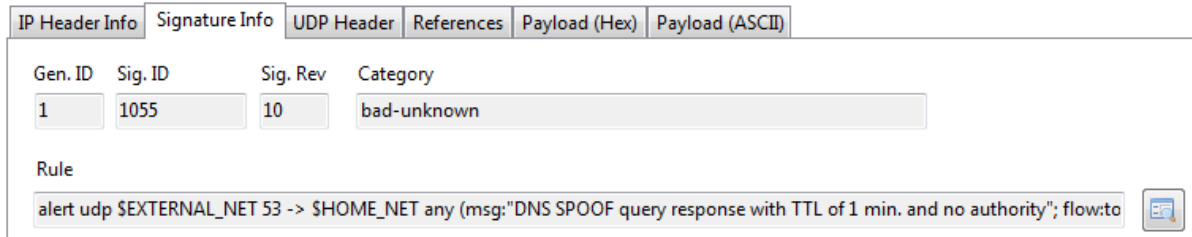
The ellipsis button will perform a connection test for the currently configured connection string. The connection string must be in the following format:

```
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:



The screenshot shows a window with several tabs: IP Header Info, Signature Info (selected), UDP Header, References, Payload (Hex), and Payload (ASCII). Below the tabs is a table with the following data:

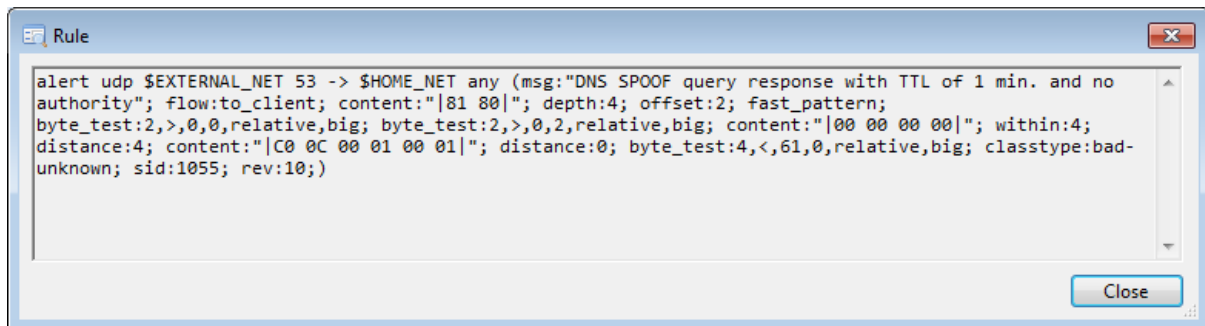
Gen. ID	Sig. ID	Sig. Rev	Category
1	1055	10	bad-unknown

Below the table, there is a 'Rule' section with a text box containing the following rule:

```
alert udp $EXTERNAL_NET 53 -> $HOME_NET any (msg:"DNS SPOOF query response with TTL of 1 min. and no authority"; flow:to
```

To the right of the text box is a small icon of a document with a magnifying glass.

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

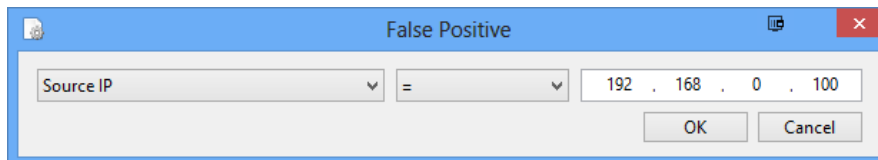


The rules can be imported manually via the Tools->Import Rules menu or they can be copied into the Rules directory located in the applications installation directory. The automated import will check the file names/timestamps and only import new or changed files.

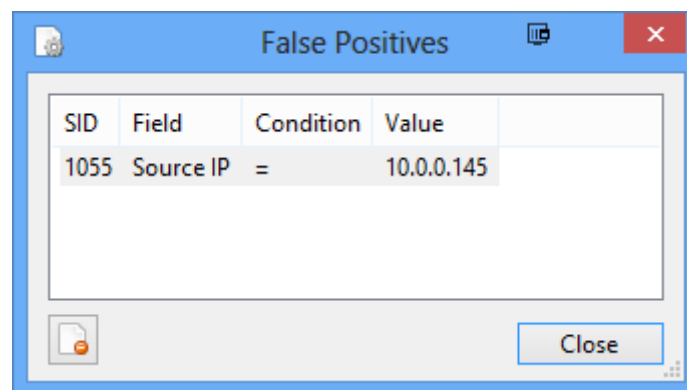
False Positives

To help reduce the amount of “noise” returned by snort it is possible to add false positive filters to the data set. The false positive filters are only applicable 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

v1.0.13

- Modified to allow the filtering of Rules on a per sensor basis
- Modified to allow user configurable commands to be executed via the Rules list context menu. The commands are stored in the Commands.xml file located in the user's application data directory for the application. The command strings will have data substitutions applied using the following mark up so that event data can be passed to the commands:

```
#IP_SRC#  
#IP_DST#  
#PORT_SRC#  
#PORT_DST#  
#PROTO#  
#SENSOR_ID#
```

- Modified to allow better multi-user collaboration. The user can now right click on an event(s) and use the Acknowledgment context menu item to categorise the event. The user should set event(s) to "Unclassified" when initially looking into an Event, and then assign the actual category once the analysis is complete
- Modified to set use F1 key to set the current set of events to Taken

v1.0.12

- Modified to allow the deletion of multiple excludes in one go. Thanks DannyF
- Modified to allow the export of the current rules on the Rules tab. This is designed to make off line working/note taking easier
- Added two new NetWitness queries e.g. prior traffic to a source host, and prior traffic to a destination host. These queries will locate all traffic to the selected host for a period of two minutes before the event timestamp and one minute after

v1.0.11

- Modified to change mutex permissions

v1.0.10

- Updated NetWitness query. Thank DanO

v1.0.9

- Fixed the search tab so that condition combo box is showing. Thanks DannyF
- Modified the NetWitness query generate to include the NWS prefix for SSL connections

v1.0.8

- Fixed bug in copy functionality
- Modified the NetWitness query generation as the generated query was too complex. Thanks ChrisB
- Added Find window/functionality for use in the Payload window. Thanks ChrisB
- Added the ability to copy the Host column value via the context menu
- Added Enter key event handler to the Rule list which displays the Payload window. Escape now closes the Payload window

- Modified Find window to catch F3 to continue finding text

v1.0.7

- Modified the context menu displayed on the Rule tab so that the menu items are more appropriately enabled/disabled depending on what is selected
- Added new window to display the payload details. Double click the entry to display. Thanks ChrisB
- Added the ability to group the list items. Use the context menu by right clicking on the list header. Thanks MattN
- Enabled the ability to filter the list items. Use the context menu by right clicking on the list header
- Added Host column to list views (Events, Rules, Search) which is parsed from the ASCII payload. Thanks ChrisB
- Recoded all data access to use NPoco rather than Massive
- Removed the preloading of all possible signature names and ID's for the Search facility due to performance issues on slow infrastructure
- Moved the localised rule storage from ESENT to SQL Server CE to permit the opening of multiple instances of the application
- Added Netwitness query string generation. Right click on an event, select Netwitness Query menu item. Thanks MattN

v1.0.6

- Corrected Exclude functionality to reverse byte order of IP addresses. Thanks ChrisB

v1.0.5

- Added the ability to export the current events from the Rules tab to a TSV file. Use the context menu to export
- Added the ability to export all events associated with the current ruleset/time period defined on the Rules tab to a TSV file. Use the context menu to export
- Modified the event loading to recalculate the total records loaded using the number of records loaded
- Reworking of the Hide functionality. It now uses a table within the snort database e.g. "exclude". Thanks MattN
- Added the ability to export all Excludes to TSV for offline analysis
- Added the ability to filter the Rules by Priority. Thanks MattN
- Added alternative row colours. Thanks ChrisB

v1.0.4

- Fixed Rules paging label positioning/anchoring
- Added the ability to extract distinct source/destination IP addresses for a specific rule/date/date range. Access the functionality by using the context menu on an Event. This functionality applies to the Rules tab

v1.0.3

- Updated the rule import to prevent old rules being discarded
- Fixed bug where the Rules drop down list displayed duplicate rules
- Fixed import paths e.g. from application directory to user app data directory
- Added a default MySql connection string example when creating a new connection

v1.0.2

- Modified the Sensor tab to prevent it automatically loading at start up, as some instances may not be accessible. To refresh the Sensor data a new refresh button has been added to the top of the tab
- Removed the Error & Exclamation error handlers within the four main user controls as they were unnecessary

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. Thanks ChrisB

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