Database Schema

Versioning

The snort database schema is version-ed in order to allow for debugging and upgrading. The `schema.vseq` field store the version number of the database. In order to determine the current schema version (without examining the snort database plugin output) using the following SQL:

```
SQL> SELECT * from schema;

+------+---------------------+
| vseq | ctime               |
+------+---------------------+
|  104 | 2001-10-15 10:56:30 |
+------+---------------------+
```

In this example, the database is version 104 and was created on October 15, 2001 at 10:56.

For every change made to the schema, the version number will be incremented. It is sometimes possible that a change will be made only a particular database script. For example, the MySQL script might be changed but not PostgreSQL. Regardless, a change in any of the databases necessitates incrementing the version number in all databases.

In cases where the database schema version number has changed for a particular database type, but no actual change to the schema was made, the following SQL can be used to upgrade the schema:

```
SQL> UPDATE schema SET vseq = 'the new version number';
```

ER Diagrams and Documentation

The following are ER diagrams and table level documentation of the Snort database schema:

- schema **v0**,
- schema **v100-103**

Schema CHANGELOG

```
2002-02-28 -- v105
  + ORACLE: event.timestamp redefined as a DATE

2001-09-26 -- v104
  + ALL: enlarged reference.reg_tag field ( TEXT or VARCHAR(100) )

2001-06-15 -- v103
  + ALL: removed 4-octet representation from iphdr
  + ALL: removed all classification/priority definitions from the
         DDL scripts
  + ALL: added support for signature priorities, ID, and revision ID

2001-05-12 -- v102
  + ALL: added support for signature classification

2001-05-07 -- v101
  + POSTGRESQL: fixed bug from v100 to properly define event.signature

2001-03-16 -- v100
  + ALL: normalization of the signature representation
```

```
    + ALL: created schema table to self-document the schema version
    + ALL: added support for signature references

  2000-02-08 -- v0
    + initial release
```

Example SQL
