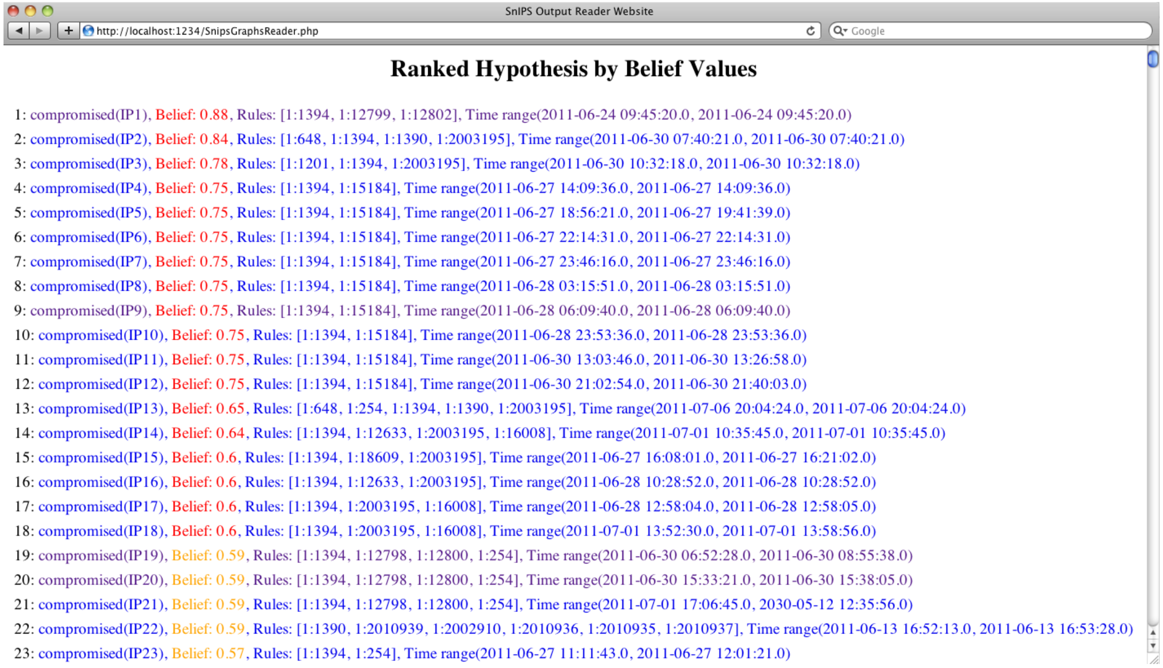
Kansas State University
CIS dept., Argus Lab
by Loai Zomlot

SnIPS User Manual

SnIPS output is on cyber2 server. The user can access it by ssh forwarding. SnIPS output is ranked hypothesis about network's machines. The rank is by the belief of how the hypothesis is true.

1) The first page of SnIPS output is the ranked hypothesis. The beliefs values colored by the criticality of it. They are from red > orange > yellow > blue. Figure1 illustrates example of the output. The *Rules* set is the snort supporting rules numbers for the hypothesis. The *Time range* is when the hypothesis is valid or may occurred.

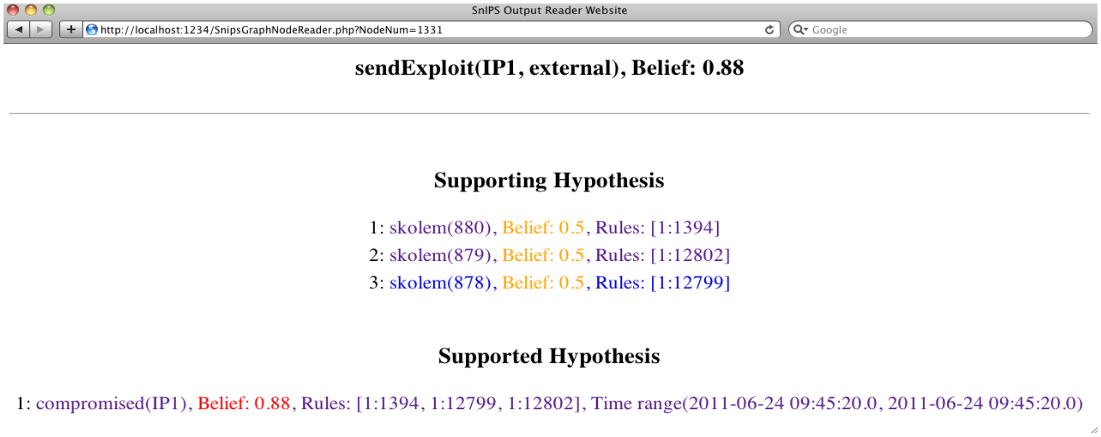

SnIPS Output Reader Website
http://localhost:1234/SnipsGraphsReader.php
Google

```
Ranked Hypothesis by Belief Values

1: compromised(IP1), Belief: 0.88, Rules: [1:1394, 1:12799, 1:12802], Time range(2011-06-24 09:45:20.0, 2011-06-24 09:45:20.0)
2: compromised(IP2), Belief: 0.84, Rules: [1:648, 1:1394, 1:1390, 1:2003195], Time range(2011-06-30 07:40:21.0, 2011-06-30 07:40:21.0)
3: compromised(IP3), Belief: 0.78, Rules: [1:1201, 1:1394, 1:2003195], Time range(2011-06-30 10:32:18.0, 2011-06-30 10:32:18.0)
4: compromised(IP4), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 14:09:36.0, 2011-06-27 14:09:36.0)
5: compromised(IP5), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 18:56:21.0, 2011-06-27 19:41:39.0)
6: compromised(IP6), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 22:14:31.0, 2011-06-27 22:14:31.0)
7: compromised(IP7), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-27 23:46:16.0, 2011-06-27 23:46:16.0)
8: compromised(IP8), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-28 03:15:51.0, 2011-06-28 03:15:51.0)
9: compromised(IP9), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-28 06:09:40.0, 2011-06-28 06:09:40.0)
10: compromised(IP10), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-28 23:53:36.0, 2011-06-28 23:53:36.0)
11: compromised(IP11), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-30 13:03:46.0, 2011-06-30 13:26:58.0)
12: compromised(IP12), Belief: 0.75, Rules: [1:1394, 1:15184], Time range(2011-06-30 21:02:54.0, 2011-06-30 21:40:03.0)
13: compromised(IP13), Belief: 0.65, Rules: [1:648, 1:254, 1:1394, 1:1390, 1:2003195], Time range(2011-07-06 20:04:24.0, 2011-07-06 20:04:24.0)
14: compromised(IP14), Belief: 0.64, Rules: [1:1394, 1:12633, 1:2003195, 1:16008], Time range(2011-07-01 10:35:45.0, 2011-07-01 10:35:45.0)
15: compromised(IP15), Belief: 0.6, Rules: [1:1394, 1:18609, 1:2003195], Time range(2011-06-27 16:08:01.0, 2011-06-27 16:21:02.0)
16: compromised(IP16), Belief: 0.6, Rules: [1:1394, 1:12633, 1:2003195], Time range(2011-06-28 10:28:52.0, 2011-06-28 10:28:52.0)
17: compromised(IP17), Belief: 0.6, Rules: [1:1394, 1:2003195, 1:16008], Time range(2011-06-28 12:58:04.0, 2011-06-28 12:58:05.0)
18: compromised(IP18), Belief: 0.6, Rules: [1:1394, 1:2003195, 1:16008], Time range(2011-07-01 13:52:30.0, 2011-07-01 13:58:56.0)
19: compromised(IP19), Belief: 0.59, Rules: [1:1394, 1:12798, 1:12800, 1:254], Time range(2011-06-30 06:52:28.0, 2011-06-30 08:55:38.0)
20: compromised(IP20), Belief: 0.59, Rules: [1:1394, 1:12798, 1:12800, 1:254], Time range(2011-06-30 15:33:21.0, 2011-06-30 15:38:05.0)
21: compromised(IP21), Belief: 0.59, Rules: [1:1394, 1:12798, 1:12800, 1:254], Time range(2011-07-01 17:06:45.0, 2030-05-12 12:35:56.0)
22: compromised(IP22), Belief: 0.59, Rules: [1:1390, 1:2010939, 1:2002910, 1:2010936, 1:2010935, 1:2010937], Time range(2011-06-13 16:52:13.0, 2011-06-13 16:53:28.0)
23: compromised(IP23), Belief: 0.57, Rules: [1:1394, 1:254], Time range(2011-06-27 11:11:43.0, 2011-06-27 12:01:21.0)
```

Figure 1: ranked SnIPS output

2) The user can click on any of these hypothesis to investigate the supporting hypothesis of it. Fig2 illustrate an example of the output when the user clicks on one of the Fig1 hypothesis. The upper most line is the chosen hypothesis. The first list has *skolem* which is has the supporting snort rule with some information about the triggered alerts list.


SnIPS Output Reader Website
http://localhost:1234/SnipsGraphNodeReader.php?NodeNum=1331
Google

sendExploit(IP1, external), Belief: 0.88

Supporting Hypothesis

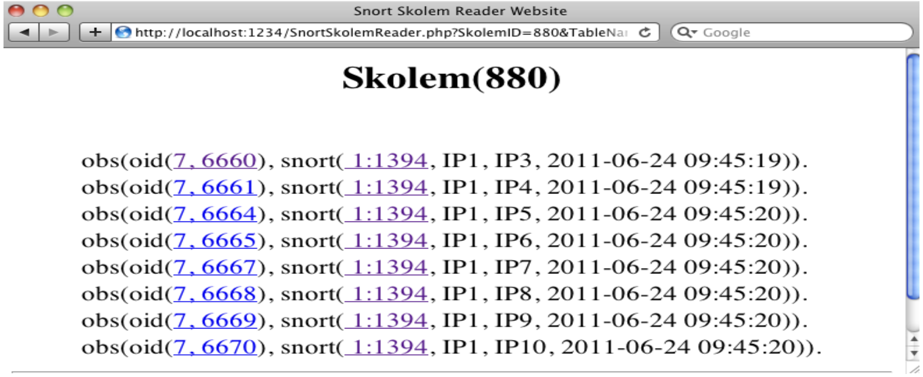
1: skolem(880), Belief: 0.5, Rules: [1:1394]
2: skolem(879), Belief: 0.5, Rules: [1:12802]
3: skolem(878), Belief: 0.5, Rules: [1:12799]

Supported Hypothesis

1: compromised(IP1), Belief: 0.88, Rules: [1:1394, 1:12799, 1:12802], Time range(2011-06-24 09:45:20.0, 2011-06-24 09:45:20.0)

Figure 2: Supporting and supported hypothesis by sendExploit(IP1,external) hypothesis

3) Fig3 illustrates the details of the *skolem*. The *oid* number is the payload of each alert that can be shown. Also, the user can click on snort rule id to read the snort rule and its description.


Snort Skolem Reader Website
http://localhost:1234/SnortSkolemReader.php?SkolemID=880&TableNa
Google

Skolem(880)

obs(oid(7, 6660), snort(1:1394, IP1, IP3, 2011-06-24 09:45:19)).
obs(oid(7, 6661), snort(1:1394, IP1, IP4, 2011-06-24 09:45:19)).
obs(oid(7, 6664), snort(1:1394, IP1, IP5, 2011-06-24 09:45:20)).
obs(oid(7, 6665), snort(1:1394, IP1, IP6, 2011-06-24 09:45:20)).
obs(oid(7, 6667), snort(1:1394, IP1, IP7, 2011-06-24 09:45:20)).
obs(oid(7, 6668), snort(1:1394, IP1, IP8, 2011-06-24 09:45:20)).
obs(oid(7, 6669), snort(1:1394, IP1, IP9, 2011-06-24 09:45:20)).
obs(oid(7, 6670), snort(1:1394, IP1, IP10, 2011-06-24 09:45:20)).

Figure 3: Snort's rule triggered alerts list