

Reporting

BASE - Basic Analysis and Security Engine

Based on the code from the Analysis Console for Intrusion Databases (ACID) project

Provides a web front-end to query and analyze the alerts coming from a SNORT IDS system

Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Added 248 alert(s) to the Alert cache

Queried on : Thu December 04, 2014 19:34:39

Database: snort@localhost (Schema Version: 107)

Time Window: [2014-11-06 11:35:41] - [2014-12-03 18:21:11]

[Search](#)

[Graph Alert Data](#)

[Graph Alert Detection Time](#)

[Use Archive Database](#)

Sensors/Total: 1 / 1

Unique Alerts: 3

Categories: 2

Total Number of Alerts: 562

- Src IP addrs: 1
- Dest. IP addrs: 165
- Unique IP links 165

- Source Ports: 471

- TCP (471) UDP (0)
- Dest Ports: 1

- TCP (1) UDP (0)

Traffic Profile by Protocol

TCP (87%)



UDP (0%)



ICMP (13%)



Portscan Traffic (0%)



[Alert Group Maintenance](#) | [Cache & Status](#) | [User Preferences](#) | [Logout](#) | [Administration](#)

BASE 1.4.5 (lilias) (by Kevin Johnson and the BASE Project Team)

Built on ACID by Roman Danyliw)

Basic Analysis and Security Engine (BASE)

[Home](#) | [Search](#) | [User Preferences](#) | [Logout](#)
[\[Back \]](#)

Queried on : Thu December 04, 2014 19:37:49

Meta Criteria	any
IP Criteria	any
Layer 4 Criteria	none
Payload Criteria	any

Displaying alerts 1-48 of 165 total

	< Dst IP address >	Sensor #	< Total # >	< Unique Alerts >	< Src. Addr. >
<input type="checkbox"/>	4.79.82.143	1	2	1	1
<input type="checkbox"/>	5.39.74.126	1	2	1	1
<input type="checkbox"/>	8.39.37.25	1	6	1	1
<input type="checkbox"/>	8.39.37.35	1	1	1	1
<input type="checkbox"/>	8.39.37.41	1	4	1	1
<input type="checkbox"/>	12.129.199.103	1	1	1	1
<input type="checkbox"/>	12.129.199.104	1	3	1	1
<input type="checkbox"/>	23.4.136.180	1	3	1	1
<input type="checkbox"/>	23.4.137.11	1	6	1	1
<input type="checkbox"/>	23.4.145.199	1	21	1	1
<input type="checkbox"/>	23.4.148.194	1	1	1	1
<input type="checkbox"/>	23.4.150.218	1	8	1	1
<input type="checkbox"/>	23.4.153.139	1	1	1	1
<input type="checkbox"/>	23.9.91.27	1	8	1	1
<input type="checkbox"/>	23.14.133.151	1	2	1	1
<input type="checkbox"/>	23.21.114.59	1	1	1	1
<input type="checkbox"/>	23.23.159.118	1	1	1	1
<input type="checkbox"/>	23.61.194.49	1	1	1	1
<input type="checkbox"/>	23.61.194.56	1	1	1	1
<input type="checkbox"/>	23.61.194.59	1	4	1	1
<input type="checkbox"/>	23.61.194.160	1	8	1	1
<input type="checkbox"/>	23.61.194.161	1	5	1	1
<input type="checkbox"/>	23.61.194.162	1	5	1	1
<input type="checkbox"/>	23.61.194.169	1	4	1	1
<input type="checkbox"/>	23.61.194.170	1	5	1	1
<input type="checkbox"/>	23.61.194.171	1	1	1	1
<input type="checkbox"/>	23.61.194.176	1	8	1	1
<input type="checkbox"/>	23.61.194.178	1	5	1	1
<input type="checkbox"/>	23.61.194.179	1	2	1	1



Added 2 alert(s) to the Alert cache

What do you want to know:

Dst. IP address vs. Number of Alerts

How should it be displayed?

As ☐ bar ☒ line ☐ pie

... with a size of:

(width x height) 600 x 600

Do you want to know
the data just of a
particular time frame? (optional)

Chart Begin: {hour} {day} {month} {year}

Chart End: {hour} {day} {month} {year}

Chart Title:

BASE Chart

How many columns or elements do you want to see?

{all of them}

... and starting from which element on?

From element no. 0

Graph Alerts

X / Y AXIS CONTROLS:

X Axis

Data Source: { data source (AG) }

Minimum Threshold Value: 0

☒ Rotate Axis Labels (90 degrees)☐ Show X-axis grid-lines

Y Axis

☐ Show Y-axis grid-lines>

BASE

Simple Web interface

Provides summary information and reports on network traffic

Future Work

Make network traffic reporting more user friendly

Domain Names in addition to/instead of IP

Automate process to maintain whitelist addresses