Demonstration of The Realeyes Intrusion Detection System

Jim Sansing May 14, 2008

For more information, see the project website and blog:

http://realeyes.sourceforge.net http://realeyes-tech.blogspot.com The Realeyes project consists of an analysis library that is used to build a network Intrustion Detection System (IDS). This paper describes a live demonstration that was presented to the Columbia Area Linux Users Group (<u>http://www.calug.org</u>) at the monthly meeting.

The project designers have used several security tools for monitoring networks and wanted to incorporate the most useful features of them, and some unique ones, in a single application. These features include:

- Collection of enough data to provide context for reported detects
- Reduction of false positives by supporting rule definitions that include both halves of TCP sessions
- Playback of both halves of TCP sessions
- Statistics collection
- The capability to save serious incidents for trends analysis and reporting
- Built in reports

The Realeyes IDS system consists of four components:

- IDS sensor
- Database
- Database IDS interface (database daemon or DBD)
- User interface

All four were running on the demonstration host, but may be installed in separate hosts or other reasonable combinations. The demonstration did not include an installation of the system, but at the end the IDS installation script was run partially as an example of how the scripts eliminate the need for editing configuration files.

This demonstration was intended to show the current status of the project, which is in Beta testing. The members of CALUG in attendance were mostly familiar with security tools in general and network IDSes in particular, so the focus was on the specifics of the application.

The following screenshots were taken after the presentation, to give a sense of what was covered. A few screenshots have been added of material that was not covered during the demonstration.

-	Shell - Konsole <4>												
top -) - 10:25:47 up 13 days, 23:13, 1 user, load average: 1.63, 0.66, 0.30 主												
Tasks	201 tota	ι,	3 r	unnınç	j, 197	/ slee	epp	Lng,	0 s	topped,	l zombie		
Cpu (s)): 34.4%us	, е	5.4%s	у, O.	.0%ni	, 1.0	381	id, 57	7.2%w	/a, 0.3%hi	, 0.7%si, 0.0%si	t	
Mem:	1035776k	tot	tal,	10200	060k i	used,		1571	.6k f	ree,	772k buffers		
Swap:	1510100k	tot	tal,	10174	472k ι	used,		49262	28k f	ree, 601	328k cached		
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEN	1 TIME+	COMMAND		
5596	root	16	0	891m	178m	2892	D	2.3	17.6	6 127:38.83	Xorg		
25045	root	5	-10	480m	7552	7312	S	0.0	0.7	0:00.01	rids_evta		
25046	root	7	-8	460m	9000	8612	S	0.0	0.9	0:00.08	rids_acta		
25043	root	15	0	458m	1556	1260	R	0.3	0.2	2 0:00.03	realeyesIDS		
25052	root	16	0	458m	9.8m	9816	D	1.0	1.0	0:00.29	rids coll		
25050	root	7	- 8	458m	9m	9928	S	30.6	1.0	0:05.53	rids_stra_data		
25047	root	7	-8	458m	9m	9992	S	0.3	1.0	0:00.08	rids_stra_tcp		
25049	root	7	- 8	458m	9.9m	9980	S	0.0	1.0	0:00.07	rids_stra_ip4		
25051	root	8	-7	458m	9m	9.8m	S	2.7	1.0	0:00.35	rids_strh		
25048	root	7	-8	458m	9.9m	9940	S	0.3	1.0	0:00.05	rids stra udp		
31628	jim	15	0	297m	24m	7540	S	0.0	2.5	42:22.20	soffice.bin		
19430	jim	15	0	225m	70m	28m	D	0.0	7.0	3:49.10	firefox-bin		

9					Si	iell - I	٤o	nsole	<4>				
top - Tasks: Cpu(s) Mem: Swap:	10:26:33 : 201 tota): 58.4%us 1035776k 1510100k	up 1 l, , 13 tot tot	.3 da 6 r 3.5%s :al, :al,	ys, 23 unning y, 0, 10188 1083]	3:14, g, 194 .0%ni, 396k u L32k u	l us 4 slee , 13.5 used, used,	ser epi 5%i	r, la ing, id, 13 1680 42690	oad a 0 s 3.9%w 30k f 58k f	iverage topped va, O. ree, ree,	: 4.] ,] 3%hi, 2] 6690	13, 1.49, 0.60 L zombie . 0.3%si, 0.0%s 164k buffers 092k cached	t
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	1 TI	ME+	COMMAND	
5596	root	16	0	887m	146m	2728	S	4.3	14.5	5 127:3	9.95	Xorg	
25045	root	5	-10	480m	23m	23m	S	0.0	2.3	3 0:0	0.11	rids_evta	
25046	root	5	-10	460m	26m	26m	S	0.7	2.7	7 0:0	0.50	rids_acta	
25043	root	15	0	458m	1624	1328	R	0.7	0.2	2 0:0	0.16	realeyesIDS	
25052	root	15	0	458m	26m	26m	R	5.3	2.6	6 0:0	1.97	rids_coll	
25050	root	8	-7	458m	25m	24m	S	41.1	2.5	5 0:2	1.05	rids_stra_data	
25047	root	7	-8	458m	26m	26m	S	2.3	2.6	6 0:0	0.95	rids_stra_tcp	
25049	root	7	-8	458m	26m	26m	S	1.3	2.6	6 0:0	0.55	rids_stra_ip4	
25051	root	9	-6	458m	26m	26m	S	12.3	2.6	6 0:0	3.13	rids_strh	
25048	root	7	- 8	458m	26m	26m	S	2.3	2.6	6 0:0	0.57	rids_stra_udp	
31628	jim	15	0	297m	16m	6620	S	0.3	1.7	42:2	2.23	soffice.bin	
19430	jim	15	0	225m	43m	10m	R	0.3	4.3	3 3:4	9.18	firefox-bin	ŧ

The demonstration began by running the IDS, which is a C application. In these screenshots of top, the columns to notice are NI, RES, and %CPU. The 'Nice' values of the rids_* processes are modified according to the number of buffers or structures queued for each process, versus the number that have been handled. The values are relative to each other, so that processes which are falling behind are given the most (lowest) priority.

Shell - Konso	le <4>
<pre>11350.129371 Collector has processed 317849 *** MAIN LOOP time=47fb2c57, segs=172/1014 11361.320359 Collector has processed 321126 *** MAIN LOOP time=47fb2c6a, segs=176/1014 11371.877194 Collector has processed 324403 11384.860134 Collector has processed 327680 11399.160128 Collector has processed 320956 *** MAIN LOOP time=47fb2c88, segs=180/1014 Streams: New 3393, Current 8924, Largest Stream Sz 16k: 2687 85 51 29 20 11410.519292 Collector has processed 334233 *** MAIN LOOP time=47fb2c95, segs=184/1014 11422.281238 Collector has processed 337510 *** MAIN LOOP time=47fb2ca6, segs=188/1014 11432.313156 Collector has processed 344064 *** MAIN LOOP time=47fb2cc4, segs=192/1014</pre>	6 packets *** 4 packets *** 2 packets 0 packets 8 packets *** 438460222, CmpSAWEs 19694 7 12 5 6 3 36 (58298175) 6 packets *** 4 packets *** 2 packets ***
<pre>11460.309344 Collector has processed 347340 Streams: New 3958, Current 9927, Largest Stream Sz 16k: 2681 87 42 30 20 11475.477420 Collector has processed 350617 *** MAIN LOOP time=47fb2cd9, segs=196/1014 11488.266662 Collector has processed 353894 *** MAIN LOOP time=47fb2cef, segs=200/1014 11505.762056 Collector has processed 357171 GCB CB Start b484f000, Size 32b3000, Hd b48 11518.714184 Collector has processed 360448 *** MAIN LOOP time=47fb2cff</pre>	B packets 460202262, CmpSAWEs 22226 13 6 6 8 6 56 (27440921) 6 packets *** 4 packets *** 2 packets 4f000, Tl b484f000 0 packets ***
*** MAIN LOOP time=4/fb2cff, segs=204/1014 Streams: New 3474, Current 10536, Largest Stream Sz 16k: 2571 99 58 36 18 11533.210307 Collector has processed 363724 :∎	*** 487496706, CmpSAWEs 15675 19 9 3 7 7 38 (67259671) B packets

This screenshot shows the console output of the IDS. Every 32K packets, the Collector displays the total number of packets it has processed. The MAIN LOOP shows the number of 1Meg segments allocated, out of the total memory allocated (in Meg).

The Streams information is displayed each minute, and the interesting fields are New, Current and Largest. For the IDS, a Stream is $\frac{1}{2}$ of a TCP session, so this display shows that approximately 5,000 sessions are active. The maximum number that has been recorded is just over 70,000 streams = 35,000 TCP sessions, and that is using a 733 MHz CPU and 1Gig of memory.

Near the bottom is a line that starts with GCB. This indicates that the 'Get Circular Buffer' function has been called, which means that a report is being generated for a session and needs additional buffer space.

	Realeyes IDS version 0.9.2 Console - Toolbox	[_ 🗆 X		
<u>F</u> ile <u>E</u> dit <u>A</u> dmin	<u>R</u> ules <u>H</u> elp				
No Alerts Analysis Trends Reports					
15:19:57 (UTC)	▶ 🚥 dc_s1 2007-04-15 16:24:03 TCP 192.168.1.5 ::	53959 -> 69.44.123.102	:80 📤		
	▶ 🚥 dc_s1 2007-04-15 16:24:03 TCP 192.168.1.5 ::	53959 -> 69.44.123.102	:80		
	dc_s1 2007-04-16 04:09:49 TCP 192.168.1.5 :	54760 -> 206.46.232.10	:110		
	L ▷ 🚥 dc_s1 2007-04-16 05:04:49 TCP 192.168.1.5 ::	54771 -> 206.46.232.10	:110		
	C_s1 2007-04-16 05:54:49 TCP 192.168.1.5 ::	54780 -> 206.46.232.10	:110		
Summary	Image: Arrow of the second	1261 -> 66.230.200.228	:80		
Information	↓ m dc_s1 2007-04-21 14:51:58 TCP 192.168.1.10 ::	25414 -> 204.2.179.49	:80		
New incidents: 0	↓ 🚥 dc_s1 2007-04-21 18:38:47 TCP 192.168.1.10 ::	25044 -> 206.190.39.95	:80		
	↓ m dc_s1 2007-04-21 20:09:34 TCP 192.168.1.5	47546 -> 192.168.1.10	:21		
	↓ 🚥 dc_s1 2007-04-21 20:10:14 TCP 192.168.1.5 :	47569 -> 192.168.1.10	:617		
	▶ 🚥 dc_s1 2007-04-21 20:10:43 TCP 192.168.1.5 :	47593 -> 192.168.1.10	:10000		
Status Information	♥ 🚥 dc_s1 2007-04-21 20:11:15 TCP 192.168.1.5 :	47620 -> 192.168.1.10	:4152:		
	dc_s1 2007-04-21 20:11:40 TCP 192.168.1.5 :	47640 -> 192.168.1.10	:1061		
	↓ 🚥 dc_s1 2007-04-21 20:11:47 TCP 192.168.1.5 :	47644 -> 192.168.1.10	:80		
	▶ 🚥 dc_s1 2007-04-21 20:11:53 TCP 192.168.1.5 :	47648 -> 192.168.1.10	:80		
	▶ 🚥 dc_s1 2007-04-21 20:12:19 TCP 192.168.1.5 :	47672 -> 192.168.1.10	:80		
	↓ mm dc s1 2007-04-21 20:12:37 TCP 192.168.1.5	47676 -> 192.168.1.10	:80		
			4 1 •		
Displaying 20 of 20) incidents!				

The next part of the demo was to show the results in the user interface, which is a Java application. The information for each record reported is inserted into the database, and the user interface displays it on a single line. The total number of incidents is indicated at the bottom. The maximum number displayed can be set in the preferences.

	Preferences 🗖 🗙
Login	Incidents
Password	
Incidents	Maximum incidents: 256
	Restore <u>D</u> efaults <u>Apply</u>
	OK Cancel

Realeyes IDS version 0.9.2 Console - Toolbox								
<u>F</u> ile <u>E</u> dit <u>A</u> dmin	jile <u>E</u> dit <u>A</u> dmin <u>R</u> ules <u>H</u> elp							
No Alerts	Analysis Trends Reports							
15:36:12 (UTC)	Playback Session 10:43 TCP 192.168.1.5 :47593 -> 19	92.168.1.10 :1000						
	Create/View Report 10:14 TCP 192.168.1.5 :47569 -> 19	92.168.1.10 :617						
	▶ 🚥 (Ignore Incident ▶ b9:34 TCP 192.168.1.5 :47546 -> 19	92.168.1.10 :21						
1	Crder Incidents By ► Date/Time Refresh	06.46.232.10 :110						
Summary	▲ ▶ m dc_s1 2007-04-15 16: Hostile IP (Desc) 3.1.5 :53959 -> 69	9.44.123.102 :80						
Information	▶ 🚥 dc_s1 2007-04-15 16: Target IP (Asc) 8.1.5 :53959 -> 69	9.44.123.102 :80						
New incidents: 0	▶ 🚥 dc_s1 2007-06-02 15: Target IP (Desc) 36578 -> 64	4.233.161.147 :80						
	▶ 🚥 dc_sl 2007-06-02 21:08:15 TCP 192.168.1.5 :37020 -> 64	4.233.161.91 :80						
1	t ▶ 🚥 dc_s1 2007-06-02 14:56:09 TCP 192.168.1.5 :36544 -> 64	4.233.161.103 :80						
Status Information	♥ 🚥 dc_s1 2007-04-16 05:04:49 TCP 192.168.1.5 :54771 -> 20	06.46.232.10 :110						
status information i	↓ 🚥 dc_s1 2007-04-16 05:54:49 TCP 192.168.1.5 :54780 -> 20	06.46.232.10 :110						
	▶ 🚥 dc_s1 2007-04-21 18:38:47 TCP 192.168.1.10 :25044 -> 20	06.190.39.95 :80						
	▶ 🚥 dc_s1 2007-04-21 13:44:56 TCP 192.168.1.10 :1261 -> 66	5.230.200.228 :80						
	■ dc_s1 2007-04-21 14:51:58 TCP 192.168.1.10 :25414 -> 20	04.2.179.49 :80 🛔						
1								
isplaving 20 of 20 incidents!								

	Realeyes IDS version 0.9.2 Console - Toolbox		
<u>F</u> ile <u>E</u> dit <u>A</u> dmin <u>I</u>	<u>R</u> ules <u>H</u> elp		
No Alerts	Analysis Trends Reports		
15:36:42 (UTC)	▶ 🚥 dc_s1_2007-06-02_21:08:15 TCP_192.168.1.5 :3	37020 -> 64.233.161.91	:80 单
	Create/View Report 56:09 TCP 192.168.1.5 :3	36544 -> 64.233.161.103	:80
	Ignore Incident 10:35 TCP 192.168.1.5 :3	86578 -> 64.233.161.147	:80
1	▶ 🚥 Order Incidents By ▶ Date/Time 8.1.10 :1	.261 -> 66.230.200.228	:80
Summary 🛉	Hostile IP (Asc) 8.1.5 :5	3959 -> 69.44.123.102	:80
Information	▷ 🚥 dc_s1 2007-04-15 16: ✔ Target IP (Asc) 8.1.5 :5	3959 -> 69.44.123.102	:80
New incidents: 0	▷ 🚥 dc_s1 2007-04-21 20: Target IP (Desc) 8.1.5 :4	17620 -> 192.168.1.10	:4152:
	▷ 🚥 dc_s1 2007-04-21 20:10:14 TCP 192.168.1.5 :4	17569 -> 192.168.1.10	:617
±	▷ 🚥 dc_s1 2007-04-21 20:09:34 TCP 192.168.1.5 :4	17546 -> 192.168.1.10	:21
Status Information	▷ 🚥 dc_s1 2007-04-21 20:11:47 TCP 192.168.1.5 :4	47644 -> 192.168.1.10	:80
	▶ 🚥 dc_s1 2007-04-21 20:11:53 TCP 192.168.1.5 :4	47648 -> 192.168.1.10	:80
	▷ 🚥 dc_s1 2007-04-21 20:12:19 TCP 192.168.1.5 :4	47672 -> 192.168.1.10	:80
	▶ 🚥 dc_s1 2007-04-21 20:12:37 TCP 192.168.1.5 :4	47676 -> 192.168.1.10	:80
	▶ 🚥 dc_s1 2007-04-21 20:10:43 TCP 192.168.1.5 :4	47593 -> 192.168.1.10	:1000(
Ī			
Displaying 20 of 20 in	ncidents!		

The order of the incidents can be selected from a popup menu by right clicking on the Analysis tab.

	Realeyes IDS version 0.9.2 Console - Toolbox	_ 🗆 🗙				
<u>F</u> ile <u>E</u> dit <u>A</u> dmin	<u>R</u> ules <u>H</u> elp					
No Alerts	Analysis Trends Reports					
15:17:26 (UTC)	▼ 🔤 dc_s1 2007-04-15 16:24:03 TCP 192.168.1.5 :53959 -> 69.44.123.102	:80 单				
 ✓ Possible malware in hidden IFrame (CLIENT:EXPLOIT:MEDIUM) W/T: 100/100 ✓ Hidden IFrame W/T: 110/110 						
						Src 80
	IFrame tag					
Summary -	▲ Width attribute					
Information	▶ 🚥 dc_s1 2007-04-15 16:24:03 TCP 192.168.1.5 :53959 -> 69.44.123.102	:80				
New incidents: 0	▼ 🚥 dc_s1 2007-04-16 04:09:49 TCP 192.168.1.5 :54760 -> 206.46.232.10	:110				
	✓ Activity at invalid time W/T: 50/50					
-	▲ Time monitor Verizon network					
Status Information	Activity at invalid time (SERVER:THEFT:MEDIUM) W/T: 100/100					
	▶ 🚥 dc_s1 2007-04-16 05:04:49 TCP 192.168.1.5 :54771 -> 206.46.232.10	:110				
	▶ 🚥 dc_s1 2007-04-16 05:54:49 TCP 192.168.1.5 :54780 -> 206.46.232.10	:110				
	▶ 🚥 dc_s1 2007-04-21 13:44:56 TCP 192.168.1.10 :1261 -> 66.230.200.228	:80				
	▶ 🚥 dc_s1 2007-04-21 14:51:58 TCP 192.168.1.10 :25414 -> 204.2.179.49	:80				
	♦ mm dc s1 2007-04-21 18:38:47 TCP 192.168.1.10 :25044 -> 206.190.39.95	:80 🖡				
		#I#				
Trends tree comple	ited!					

An incident is reported if the Event, Action, and Trigger thresholds in a rule definition are met or exceeded. In the Analysis tab of the main window, the Event and its Actions and its Triggers are displayed by clicking on the 'twisties'.

The 'Possible malware in hidden IFrame' Event consists of the 'Hidden IFrame' Action, which consists of the 'Src 80', 'IFrame tag', and 'Width attribute' Triggers.

Session Playback: 192.1	68.1.10:25414 -> 204.2.179.49:80
Requester Pkts: 62, Bytes: 9787	Listener Pkts: 27, Bytes: 32220
GET /cnn/.element/ssi/js/1.3/ad_head0.js HTTI Host: i.a.cnn.net User-Agent: Mozilla/5.0 (X11; U; Linux i686; er S; rv.1.8.0.10) Gecko/20060911 SUSE/1.5.0.1 Firefox/1.5.0.10 Accept: */* Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0 Keep-Alive: 300 Connection: keep-alive Referer: http://www.cnn.com/2007/US/04/17/v hooting/index.html GET /cnn/cnn_adspaces/cnn_adspaces.js HTT Host: i.a.cnn.net User-Agent: Mozilla/5.0 (X11; U; Linux i686; er S; rv.1.8.0.10) Gecko/20060911 SUSE/1.5.0.1	<pre> // function cnnad_createAd(adld,cnnad_url,cnnad_heig ht,cnnad_width) { document.write('</pre> iframe hspace="0" vspace="0" ma rginHeight="0" marginWidth="0" src="" + cnnad_url + '&tile=' + cnnad_tileID + '&page.allowcompete= yes&domId=' + adId + '" border="0" frameBorder="0 " height="0" width="0" scrolling="no" id="+adId +" style="position: absolute; visibility: hidden :" >'); } function cnnad_writeAd(cnnad_callid,cnnad_url) { if(cnnad_enabled == true) { document.write(" <script "\"="" +="" \"="" cnnad_callid="" d='\"cnnSendData();\"");' document.write("="" id='\""' l+"&tile="+cnnad_tileID+" onloa="" src='\""+cnnad_ur' type='\"text/javascript\"'></script>

By selecting 'Playback Session' from the Analysis tab popup menu, the data captured from the TCP session is displayed. By scrolling down through the server data, the Triggers that caused the record to be reported are found to be highlighted.

Also notice that the width of the frames have been adjusted by moving the center scroll bar.

Two of the Triggers that were defined for this rule are displayed on the next page. The Plugin name defines which IDS process uses the definition, which in these cases are rids_stra_data and rids_stra_tcp. The Function allows Triggers to be organized into groups. The Trigger type defines whether it is matching on any string in a packet payload or a specific location in a TCP/IP header.

The only condition flag set for the 'IFrame tag' Trigger is to allow Mixed case. The Global flag set for the 'Dest 80' Trigger indicates that it is true for the entire session and should be reported only once.

ſ	Rules: Triggers						
•	~	da	ata		Plugin name:	data	
			FLNAME		Function:	ESCODE	
			SIG				
		⊳	URL		Trigger Name:	IFrame tag	
		⊳	CODE		Trigger Type:	String	
		~	ESCODE		Value:	\x3ciframe	
			Height attribute		Location:	0	
			Height style attribute		Length:	0	
			IFrame tag		Length.		
			RealMedia heap overl		Mixed case:	True 💌	
			Width attribute		Regular expression:	False	
			Width style attribute		Global:	False 🔻	
		⊳	CMD		Mask:	False	
			VALUE				
			PROT		Number comparison:	False	
			PORT		Backspace:	False	
			ADDR		Backspace List:		
			FLAG	ŧ	Gound	Indu Canadi Delatal New	
	•		+ +				

	Rules: Triggers							
Dest 6897	Plugin name:	tcp						
Dest 6898	Function:	PORT						
Dest 6899	Trimmer Manage							
Dest 6900	irigger Name:	Dest 80						
Dest 7000	Trigger Type:	Location						
Dest 7777	Value:	80						
Dest 80	Location:	2						
Dest 8000	Length:	2						
Dest 8008								
Dest 8080	Mixed case:	False						
Dest 8083	Regular expression:	False						
Dest 9000	Global:	True						
Dest 9999	Mask:	False 🗸						
Src 110	Number comparison	Falsa						
Src 111	Number comparison.							
Src 119	Backspace:	False						
Src 123	Backspace List:							
Src 135	Save	Add Cancel Delete New						
+								

Session Playback: 192.168.1.5:54	760 -> 206.46.232.10:110
Requester	Listener
Pkts: 9, Bytes: 49	Pkts: 14, Bytes: 364
 2007-4-16 4:9:49 UTC (4622F70D 000110CA) IPv4: Len: 003C, ID: 22F7, Frag: 4000, TTL: 40, Prot: 06, CF TCP: Seq: 7FEFE8E9, Ack: 00000000, Flags:S., Win: 10 Options (Sz=x14) MSS: 05B4, SACKok, TS: CA75CA1E 00 2007-4-16 4:9:49 UTC (4622F70D 0001DDBB) IPv4: Len: 0034, ID: 22F8, Frag: 4000, TTL: 40, Prot: 06, CF TCP: Seq: 7FEFE8EA, Ack: ED7EA1DD, Flags: .A, Win: 1 Options (Sz=xC) NOP. NOP. TS: CA75CA52 1A868584 	Iksum: 9FDE 6D0, Chksum: E58B,U IVV4: Len: 0040, ID: 1909, Frag IVV4: Len: 0040, ID: 1909, Frag IVV4: Seq: ED7EA1DC, Ack: 7F Options (Sz=x18) NOP, NOP 2007-4-16 4:9:49 UTC (4622F: IVV4: Len: 00BC, ID: 190A, Frag CP: Seq: ED7EA1DD, Ack: 7F Options (Sz=x18) NOP, NOP 2007-4-16 4:9:49 UTC (4622F: IVV4: Len: 00BC, ID: 190A, Frag TCP: Seq: ED7EA1DD, Ack: 7F Options (Sz=x0) NOP, NOP
2007-4-16 4:9:49 UTC (4622F70D 00035142) IPv4: Len: 0034, ID: 22F9, Frag: 4000, TTL: 40, Prot: 06, Ch TCP: Seq: 7FEFE8EA, Ack: ED7EA265, Flags: .A, Win: 1 Options (Sz=xC) NOP, NOP, TS: CA75CAB2 1AB6B5BE	nksum: 9FE4 920, Chksum: B103,U ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

The playback for the 'Activity at invalid time' is displaying the session headers after clicking on the 'Show Headers' button at the bottom of the window (which then becomes the 'Show Payload' button). The Trigger that was detected for this session is a Special Trigger, and is shown on the next page. It looks for activity occurring between certain times and reports everything detected.

The headers display the timestamp of the packet, the IP header, and any other appropriate header data. In this case, there are TCP headers which have options.

			Rules: 7	Triggers 📃 🗖 🗙
Þ	data	e	Plugin name:	ip4
Þ	tcp		Function:	ADDR
₽	udp in4		Trigger Name:	Time monitor Verizon network
Ť	FLNAME		Trigger Type:	Special 🗸
	SIG		Value:	IPTIME,2300,0200,NET,206.46.232.0,255.255.255.0
	URL		Location:	0
	CODE		Length:	0
	ESCODE		Mived case:	False
	СМД		Mixed case.	
	VALUE		Regular expression:	False 💌
	PROT		Global:	False 💌
	PORT		Mask	False
	▼ ADDR			
	Hot IP		Number comparison:	False 💌
	Time monil		Backspace:	False 💌
	FLAG		Backspace List:	
▽	⊽ ip6		15	avel Add Cancel Delete New
	₩			

Special Triggers are created by writing code in the IDS plugin processes to search for conditions that are not simple string or location matches. In this case, the IPTIME Trigger looks for any activity occurring between 11:00 pm and 2:00 am, local time, on the network 206.46.232.0.

Shell - Konsole <4>
2008-4-21 11:23:55 UTC (480C794B 00046B5D) IPv4: Len: 0030, ID: 0988, Frag: 4000, TTL: 6F, Prot: 06, Chksum: 007C 54110C17 00000000 7002FFFF 1B450000 020405B4 01020402
2008-3-16 21:30:39 UTC (47DD917F 000269A9) IPv4: Len: 0040, ID: BF7E, Frag: 4000, TTL: 30, Prot: 06, Chksum: 55E3 97C159E6 00000000 B002FFFF 57CF0000 020405B4 01030300 0101080A 32108EB6 00000000 04020802 2008-3-16 21:30:42 UTC (47DD9182 0001253E)
IPv4: Len: 0034, ID: C065, Frag: 4000, TTL: 30, Prot: 06, Chksum: 5508 TCP: Seq: 97C159E7, Ack: E9B0D2EB, Flags: .A, Win: 05B4, Chksum: D532,Urg: 0000 Options (Sz=xC) NOP, NOP, TS: 32108EBC 00000000
2008-4-5 20:32:15 UTC (47F7E1CF 000CDEA2) IPv4: Len: 0040, ID: 5ACA, Frag: 4000, TTL: 2D, Prot: 06, Chksum: 9D13 TCP: Seq: 24091E9E, Ack: 00000000, Flags:S., Win: 7FFF, Chksum: AFE8,Urg: 0000 Options (Sz=x18) MSS: 05AC, EOL, EOL, EOL, EOL, NOP, NOP, TS: 00000000 00000000, NOP, NOP, SACKok :■

Another Special Trigger parses the TCP options field for invalid use. This screenshot is of a few of the incidents that have been reported on this Trigger. They may be buggy code, or they may be crafted packets doing OS fingerprinting.

The first example displays a hex dump of the TCP header (minus the ports field). The 7 at the beginning of the third word is the number of 4 octet words in the header, including options. But the last word, '01020402' is extending beyond that length:

- 01 = NOP
- 02 = Maximum segment size option
- 04 = Length (including option and length)
- 02 = First octet of MSS value

The second example option field has an invalid length in the last word, '04020802':

- 04 = SACK permitted
- 02 = Length
- 08 = Time Stamp option
- 02 = Length (should be 10 or x0A)

The third example has End of Line (EOL) options followed by more options.

REFERENCE: TCP_Options	×
The Transmission Control Protocol (TCP) has provision for optional header fields identified by an option kind field. Options 0 and 1 are exactly one octet which is their kind field. All other options have their one octet kind field, followed by a one octet length field, followed by length-2 octets of option data.	•
Kind Length Meaning Reference	
0 - End of Option List [RFC793] 1 - No-Operation [RFC793] 2 4 Maximum Segment Size [RFC793] 3 3 WSOPT - Window Scale [RFC1323] 4 2 SACK Permitted [RFC2018] 5 N SACK [RFC1072] 7 6 Echo Reply (obsoleted by option 8) [RFC1072] 8 10 TSOPT - Time Stamp Option [RFC1632] 9 2 Partial Order Connection Permitted[RFC1693] 10 3 Partial Order Service Profile [RFC1644] 12 CC. NEW [RFC1644] 13 CC.ECHO [RFC1644] 14 3 TCP Alternate Checksum Request [RFC1146] 15 N TCP Alternate Checksum Data [RFC13235] 17 Bubba [Knowles] [Knowles] 18 3 Trailer Checksum Option [RFC2385] 20 SCPS Capabilities [Scott] 21 Selective Negative Acknowledgements [Scott] [Sectt] 22 Record Boundaries [Scott] <td></td>	
exp-2780-05.txt]	ŧ

Included in the user interface help are some reference files, including the list of registered (and unregistered, ie. 33 and 76) TCP options. Any reference data may be added to the system by creating a text file, naming it something.ref, and copying it to the directory where the application code is located.

		Rules: Actions	
MSSYS	Target type:		TRIGGER: Src 80 Plugin:tcp Function:PORT Type:Location
P MSAPP	Attack type:	EXPLOIT	Loc:0 Len:2 Mix:F Glb:T Msk:F Num:F Bsp:F
	Action name:	Hidden IFrame	Wt:50 Sup:T Seq:0 EOL:F NOT:F XOR:F
► APSVS	Action threshold:	110	Dist:0 DisTp:F EOL:F Num:0 VALUE: 80
▶ APAPP	End of line	x3c/ifr \x3c/IEB	
✓ CLIENT RECON	Gave Add	Cancel Delete New	TRIGGER: IFrame tag Plugin:data Function:ESCODE Type:String Loc:0 Len:0 Mix:T Glb:F Msk:F Num:F Bsp:F
▼ EXPLOIT	Plugin name:	data 💌	ASSOCIATION Wt:50 Sup:F Seq:1 EOL:T NOT:F XOR:F
Hidden IFra THEFT	Hidden IFr: Function:	ESCODE	VALUE: \x3ciframe
DOS	Trigger name:	IFrame tag	TRIGGER: Height attribute
VANDAL	Weight:	50	Plugin: data Function: ESCODE Type: String
RESPONSE	Sequence:	1	ASSOCIATION
▶ SERVER	Distance triggers:	0	Wt:10 Sup:F Seq:2 EOL:T NOT:F XOR:F Dist:0 DisTp:F EOL:T Num:0
▶ ROUTER	Distance:	0	VALUE: \x20height=0
	Distance type:	False	TRIGGER: Height style attribute
	Support Trigger:	False 💌	Loc:0 Len:0 Mix:T Glb:F Msk:F Num:F Bsp:F
	Same line:	True 💌	ASSOCIATION Wt:10 Sup:F Seq:2 EOL:T NOT:F XOR:F
	NOT Trigger:	False	Dist:0 DisTp:F EOL:T Num:0 VALUE: \x20height="0
	XOR Trigger:	False	
+	Save) (A	dd (Cance) Deletej (New)	TRIGGER: Width attribute

The Action definitions are more complicated because they associate Triggers with an Action. The 'Hidden IFrame' Action has six Triggers associated with it.

The highlighted 'IFrame tag' Trigger definition has a weight of 50. The total weights of detected Triggers must equal or exceed the threshold weight of 110 defined in the Action for it to be reported. This Trigger also has a sequence number defined. On the right panel, it can be seen that the 'Height attribute' Triggers have a sequence number of 2. This means that the attributes must follow the tag to be counted.

Finally, the 'IFrame tag' Trigger has the Same line flag set. The Action End of line field defines what characters end a line, in this case the end of an IFrame tag, so the attribute Triggers must be between the start and end IFrame tags.

			Rules: Events	
Þ	MSSYS	Target type:	SERVER	ACTION: FTP login prompt
⊳	MSAPP	Attack type:	EXPLOIT	ASSOCIATION
Þ	UXSYS	Event Name	ETP brute force login attempt	Wt:25 Seq:0 Req:T Rply:F Sup:F NOT:F)
Þ	UXAPP	Event Ivanie.		ACTION: ETP login rejected
Þ	APSYS	Severity:		Target: SERVER Attack: EXPLOIT
Þ	APAPP	Event Threshold	200	ASSOCIATION Wt:25 Seg:0 Reg:F Rplv:T Sup:F NOT:F)
Þ	CLIENT	Threshold 2:	0	
~	SERVER	HotIP:	False	
	RECON	Hotip Time (bour		
	✓ EXPLOIT	Hour Time (nour	57: 0	
	FTP brute force l	Sensor group:	ALL	
	GNU Mailutils ima	Vulnerability Link	s: http://www.ritasa.com	
	IA WebMail Serve	Information:	Check for more than 4 login	
	IIS Source Code I	Active:	True 💌	
	Microsoft BizTalk	Savel II	Vid Cancel Delete New	
	Microsoft IIS HTR			
	Microsoft IIS ISAP	Target:	SERVER	
	Microsoft MSSQL	Attack:	EXPLOIT	
	Microsoft Window	Action name	ETP login prompt	
	Possible buffer o	Action nume.		
	Raxnet Cacti Gra	weight:	25	
		Sequence:	0	
	DUS	Request:	True 💌	
		Reply:	False 🔻	
N		Support Action: False		
	NUTER	NOT Action	Talaa a	
		NUT Action:	Faise	
		XOR Action:	False	
	• ••	(Save)	add Cancel Delete New	 ↓

The Event definitions are similar to the Action definitions, but with more information in the Event, which should help an analyst learn about the potential exploit.

The 'FTP brute force login attempt' Event is an example of a Request/Reply. The highlighted 'FTP login prompt' Action, is a password from a FTP client. The other Action, 'FTP login rejected', is an error reply from an FTP server. If both are detected, then the reply must immediately follow the request, based on the TCP packet's Sequence and Acknowledgment numbers.

The total weight of both rules is 50, so there must be at least 4 Request/Reply pairs for the Event to be reported. This reduces reporting user typos.

			Statistics				
Host:	dc_s1	Host:	dc_s1	Host:	dc_sl	Host:	dc_sl
Active:	True 💌	Network:	192.168.1.0	Protocol:	IPv4	Protocol:	TCP 💌
Minimum data:	16384	Protocol:	IPv4	Monitor IP:	192.168.1.10	Monitor Port:	443
Hour 1:	0	Subnet bit size:	24	Expire date:	2008-04-15	Expire date:	2008-04-15
Minute 1:	0	Enabled:	No	Comment:	Desktop	Comment:	HTTPS
Hour 2:	8	Save) (Can	e) Delete New	Save	Cancel	Save	Cancel
Minute 2:	0						
Hour 3:	16			192.168.	1.10 IPV4 200 💻	443 tuCP :	2008-04-15
Minute 3:	0	192.168.1.0	IP∨4 24	192.168.	1.5 IPV4 2008	0 tuCP 20	08-03-19
	-			0.0.0.0 IF	V4 2008-03-1	0 tucP 20	08-03-19
(Sav	(Cancel)			0.0.0.0 IF	°V4 2008-03-1	0 tuCP 20	08-03-19
				0.0.0.0 IF	vV4 2008-03-1	0 tuCP 20	08-03-19
				0.0.0.0 IF	vV4 2008-03-1	0 tuCP 20	08-03-19
				0.0.0.0 IF	vv4 2008-03-1 💻	0 tuCP 20	08-03-19 🛄
				0.0.0.0 IF	vV4 2008-03-1	0 tuCP 20	08-03-19
				0.0.0.0 IF	v√4 2008-03-1	0 tuDP 20	08-03-19
				0.0.0.0 IF	vv4 2008-03-1 🔺	0 tuDP 20	08-03-19
				0.0.0.0 IF	∨4 2008-03-1 🖡	0 tuDP 20	08-03-19 🖡
				+		•	◆ I →

Statistics may be collected on all monitored networks. The statistics are total number of bytes transferred inbound and outbound. They are collected during three periods of the day, and the start time of each period is configurable. When the networks for statistics collection are defined, the totals for each TCP and UDP port detected are maintained until the end of the collection period, when they are transferred to be stored in the database.

It is also possible to monitor specific hosts or ports. When that is defined, the total inbound and outbound byte counts for every connection to that host or port are maintained.

		Rules: Export	
IDS Host:	ALL 💌		
Export to:	Network 💌		
	Network		
Proaress:	File		±
	•		
		Submit	

The export window allows the rules definitions to be saved in a file or sent directly to the IDS hosts.

Security Report: 1	92.168.1.5:53959 -> 69.44.123.102:80
Report Number	Events Whois Notes
	Source
Date/Time (GMT) 2007-04-15 16:24:03 Site DC office Severity MEDIUM	NetRange: 192.168.0.0 - 192.168.255.255 CIDR: 192.168.0.0/16 NetName: IANA-CBLK1 NetHandle: NET-192-168-0-0-1 Parent: NET-192-0-0-0 NetType: IANA Special Use NameServer: BLACKHOLE-1.IANA.ORG NameServer: BLACKHOLE-2.IANA.ORG Comment: This block is reserved for special purposes. Comment: Please see RFC 1918 for additional information.
ТСР	US - UNITED STATES
Source IP: 192.168.1.5 Hostname: guitar Port: 53959 Destination IP: 69.44.123.102 Hostname: 69.44.123.102 Port: 80	Destination OrgName: Level 3 Communications, Inc. OrgID: LVLT Address: 1025 Eldorado Blvd. City: Broomfield StateProv: CO PostalCode: 80021 Country: US NetRange: 69.44.0.0 - 69.45.255.255 CIDR: 69.44.0.0/15 NetName: LVIT-ORG-69.44
Save Report Close Report	US - UNITED STATES

If an incident is serious, it may be saved in a report for trends analysis. This is done by selecting the Create/View Report button on the Analysis tab. The report window has three tabs, and the Whois tab is shown in this screenshot. A whois query is run in the background to determine where both IP addresses in the reported session are registered.

The information in the left frame is automatically added, but may be modified by an analyst. Then the Save Report button is clicked to save the report to the database.

	Realeyes IDS version 0.9.2 Console - Toolbox	×
<u>F</u> ile <u>E</u> dit <u>A</u> dmin <u>R</u> ules	Help	
No Alerts 2008-05-15 17:50:21 (UTC)	Analysis Trends Reports	
	From: 2007 V Jan V 01 V Site: ANY V Type: Incident Reports V	
	To: 2008 V Jul V 01 V Sensor: ANY V Refresh Selections	
	Host(s): Port(s): Host: Either	
Summary Information	Network: Severity: ANY Port: Either	
New incidents: 0	▶ dc 2007-04-15 16:24:03 TCP 192.168.1.5 :53959 -> 69.44.123.102 :80	Í
	▼ dc 2007-04-21 14:51:58 TCP 192.168.1.10 :25415 -> 204.2.179.49 :80	
1 T	Possible malware in hidden IFrame Action Weight: 100 Hidden IFrame Trigger Weight: 120 Src 80 IFrame tag	
Status Information	Height style attribute Width style attribute	
1		
Trends tree completed!		

In the Trends tab of the main window, the reports may be displayed based on a variety of search criteria. The From/To dates are mandatory, but the reports may be limited to specific hosts or ports. The playback window may be displayed by using the same popup window as found n the Analysis tab.

	Realeyes IDS version 0.9.2 Console - Toolbox	×
<u>F</u> ile <u>E</u> dit <u>A</u> dmin <u>R</u> ules	Help	
No Alerts 2008-05-15 17:54:37 (UTC)	Analysis Trends Reports From: 2007 • Jan • 01 • Site: ANY • Output: Output: Window • Refresh Selections To: 2008 • Jun • 01 • Sensor: ANY • Refresh Selections Itimit: 10 Host(s): Port(s): Limit: 10 Network: Severity: ANY • Interval: 2 • Interval:	
New incidents: 0	Output Incident Reports Incident Report Totals by Severity Incident Report Totals by Target Host Incident Report Totals by Target Port	•
Status Information	Analysis Statistics Output Analysis Statistics O Ports With Most Received Data - CONDITIONS: Sensor O Ports With Least Received Data Sensor O Monitored Hosts Sensor O Monitored Ports Sensor	
Trends tree completed!		

The Report tab on the main window provides several predefined reports. The reports may display the information from the Analysis tab or Trends tab.

	Report 📃 🗖	×
l	Incident Totals 2007-01-01 to 2008-06-01	
Site: [CRIT	DC office	
MED	H II NUM 7	
		†
•		

	Rep	ort	
Ports Wit 2007-01-	h Most Receive 01 to 2008-06	ed Data -01	
Sensor: dc_s1			
2007-04-15 Interval: 2 TCP Ports Port 80 443 110	Data In 795240 508815 36216	Data Out 110731 96538 3798	
Interval: 3 TCP Ports Port 80 8080 443 110 25	Data In 660636011 3516892 1456404 146147 2168	Data Out 2147927 1499 150530 17851 22122	
UDP Ports Port 34997 34995 34993 53	Data In 29938 20620 19602 0	Data Out 0 0 0 55878	
2007-04-16 Interval: 1 TCP Ports Port 80 110 UDP Ports	Data In 45430186 47586	Data Out 166672 4197	
Port 35008 21302 5000	Data In 16393 0 0	Data Out 0 8959680 103668	†
•			+ +

The reports also display information from Statistics that may be collected. This screenshot is a display of the port statistics.

	Rep	ort			
Monitored Hosts Interval 2					
2007-01-01 to 200	8-06-01				
Sensor: dc_s1					
2007-04-15					
2007 01 10					
Monitored host: 192.	168.1.10				
Conn. Host	Port	Data In	Data Out 🛛 🚺		
12.180.111.218	80	74018	13734		
12.180.111.218	443	79544	17778		
64.187.43.35	80	421	832		
65.206.60.120	80	90187	19667		
66.102.1.147	80	658	869		
67.109.145.40	80	23633	924		
72.9.255.178	80	44845	8806		
72.14.219.99	80	1010	1464		
140.90.113.200	80	0	2112		
140.90.121.156	443	521	1048		
140.90.121.157	443	3322	1574		
140.90.121.168	443	97332	6942		
206.213.211.171	80	4511	7687		
206.213.211.173	443	71618	26118		
206.213.253.171	80	114656	1600		
206.213.253.171	443	182829	11641		
206.213.253.173	443	73649	31437		
209.85.165.104	80	6226	2527		
216.38.80.20	80	7657	1168 🚖		
			•		

This screenshot shows the results of monitoring a host. It is for the second monitoring interval of one day. This allows detailed information to be collected on connections being made to a host.

	Report		
Monitored Ports _In 2007-01-01 to 200	terval 2 8-06-01		•
Sensor: dc_s1			
2007-04-15			
Monitored port: 443 (Conn. Host 12.180.111.218 140.90.121.156 140.90.121.157 140.90.121.168 192.168.1.10 206.213.211.173 206.213.253.171 206.213.253.173	TCP) Data In 0 0 0 508815 0 0 0	Data Out 17778 1048 1574 6942 0 26118 11641 31437	
2007-06-02			
Monitored port: 443 (Conn. Host 63.160.50.126 192.168.1.10 216.168.252.103	TCP) Data In 0 78986 0	Data Out 73053 0 6451	* *
•			+

This screenshot shows the results of monitoring a port. It shows all hosts external to the monitored networks that made connections using the monitored port.

This script will prompt for the configuration data required to start a Realeyes IDS sensor and communicate with a Realeyes DBD host.	↑
!!! This script generates the following files: !!! !!! /etc/realeyes !!! !!! realeyesIDS.conf !!! !!! rae_analysis.xml !!! !!! rids_collector.xml !!! !!! Running it will backup existing files but !!! !!! create all new values from input data. !!!	
Enter 'q' to quit at any time.	
Enter home directory [/usr/share/realeyes/realeyesIDS]: Enter Memory allocation (percent of real) [33]: Enter IDS sensor hostname: myhost Enter IDS sensor IP address: 192.168.1.2 Enter IDS monitoring interface [<intfc> eth0]: The Realeyes IDS will monitor the following protocol selections: 1) TCP only 2) TCP and UDP only 3) All IP protocols Enter protocol selection [<prot> 1]: 2 Enter Manager logging options [W(arn) I(nfo) S(tat) D(one)]: w Enter Manager logging options [W(arn) I(nfo) S(tat) D(one)]: d Use encryption to DBD host [Y n]: n Spooler home directory [<dir> spool]: Port for data transmission [<port> 1332]: Port for control transmission [<port> 1333]: Enter DBD hostname: dbdhost Enter DBD hostname: dbdhost Enter DBD lP address: 192.168.1.3 Another DBD definition [y/N]: Enter Plugin logging options [W(arn) I(nfo) S(tat) D(one)]: w Enter Plugin logging options [W(arn) I(nfo) S(tat) D(one)]: d</port></port></dir></prot></intfc>	
<pre>#RIDS_CFG_DIR_RIDS_CFG_DIR=/etc/realeyes #RIDS_HOME_RIDS_HOME=/usr/share/realeyes/realeyesIDS #RIDS_MEM_ALLOC_RIDS_MEM_ALLOC=33 LOC_HOST_myhost LOC_ADDR 192.168.1.2 MGR_MSG_Warning ENCRYPT_NO SPOOL_HOME spool DATA_PORT_1332 CTL_PORT_1333 DBD_HOST_dbdhost DBD_ADDR 192.168.1.3 PLUG_MSG_Warning IDS_HOME_/usr/share/realeyes/realeyesIDS LOG_DIR_/var/log/realeyes SPOOL_USER_reids INTFC_eth0 PROTOCOLS_ip_and (tcp_or_udp) Accept_these_values [Y[d]:</pre>	

The previous screenshot shows part of the installation and configuration script for the IDS. There are scripts for each of the four components that eliminate the need for editing configuration files. However, all configuration is maintained in text files that can be edited if necessary.

9						realey	yes@violin: ~ - Shell - Konsole <2>	X
May	14	, 2008	23:21:37	Realeyes	Analysis	Manager	r (NOTE)	
***	r k (Startir	a Poplay	oe Intrue:	ion Dotoci	tion Svet	stom 0 0 0	
***	* .	StartI	iy nearey	es inclus.	ton Detec	LIUN SYST	stem 0.5.0	
May	14	, 2008	23:21:37	Realeyes	Analysis	Manager	r (NOTE) init_manager: Manager Process ID: 0 Process group ID: 2571, Buffer Al.	1
oc :	117	7440512	2					
May	14	, 2008	23:21:37	Realeyes	Analysis	Manager	r (NOTE) interrupts_init: Interrrupt initialization complete	
May	14	, 2008	23:21:3/	Realeyes	Analysis	Manager	r (NOTE) manager_parser: Parsing manager configuration	
мау	14.	, 2008	23:21:37	Realeyes	Analysis	Manager	r (NOTE) spool_init: Spooler Started (2573, 2573)	
May	14	2008	23.21.37	Realeves	Analysis	Manager	r (NOTE) Component 'Event Analyzer' initialized	
Mav	14	2008	23:21:37	Realeves	Analysis	Manager	r (NOTE) dispatch plugin: Child process started: rids acta (2575, 2575)	
May	14	, 2008	23:21:37	Realeyes	Analysis	Manager	r (NOTE) Component 'Action Analyzer' initialized	
May	14	, 2008	23:21:37	Realeyes	Analysis	Manager	r (NOTE) dispatch_plugin: Child´process started: rids_stra_tcp (2576, 2576)	
May	14	, 2008	23:21:37	Realeyes	Analysis	Manager	r (NOTE) dispatch_plugin: Child process started: rids_stra_udp (2577, 2577)	
May	14	, 2008	23:21:38	Realeyes	Analysis	Manager	r (NOTE) dispatch_plugin: Child process started: rids_stra_ip4 (2578, 2578)	
May	14	, 2008	23:21:38	Realeyes	Analysis	Manager	r (NOTE) dispatch_plugin: Child process started: rids_stra_data (2579, 2579)	
May	14	, 2008	23:21:38	Realeyes	Analysis	Manager	r (NOTE) diapatah plugip. Child presses startad, rida atrh (2500, 2500)	
May	14	, 2008	23:21:38	Realeyes	Analysis	Manager	r (NOTE) dispatch_plugin: child process started: rids_strh (2080, 2080) r (NOTE) Component 'Stream Handler' initialized	
Mav	14	2008	23:21:30	Realeves	Analysis	Manager	r (NOTE) dispatch plugin. Child process started, rids coll (2581, 2581)	
Mav	14	2008	23:21:38	Realeves	Analysis	Manager	r (NOTE) Component 'Collector' initialized	
May	14	, 2008	23:21:38	Realeyes	Analysis	Manager	r (NOTE) init manager: Data Stream Analysis initialized	
May	14	, 2008	23:21:38	Realeyes	Analysis	Manager	r (NOTE) manager: Initialization complete, starting Data Stream Analysis	
May	14	, 2008	23:21:38	Realeyes	Analysis	Manager	r (SPOOL) (NOTE) spooler_main: Spooler processing started	
spo	pole	er_mair	n: Spoole	r_process:	ing starte	ed		
May	14	, 2008	23:25:12	Realeyes	Analysis	Manager	r (NOTE) comp_child_handler: Child process ended: 2581	
1								

Logs of the IDS and DBD are kept in the directory, /var/log/realeyes. This screenshot shows the log of the main IDS process. All times are based on Universal Time Coordinates (UTC) so that if the system is distributed across time zones, all reports are synchronized. So the demonstration actually occurred at 7:21 Eastern USA time.

写 realeyes@violin: ~ - Sl	iell - Konsole <2>	_ 🗆 🗙
realeyesIDS.xml(5) RealeyesID	DS config realeyesIDS.xm	l(5) 🔂
NAME realeyesIDS.x∎l - Realeyes Intrusi	on Detection System configuration	
SYNOPSIS The Realeyes Intrusion Detection format. The manager and each plugi nition. The names of the DTDs are:	n System configuration files are in In level have a unique Data Type D	XML Defi-
· rae_analysis.dtd		
 rids_collector.dtd 		
 rids_stream_handler.dtd 		
 rids_stream_analyzer.dtd 		
 rids_action_analyzer.dtd 		
 rids_event_analyzer.dtd 		
DESCRIPTION ANALYSIS: The manager configura tag and the namespace is rae_dsan.	ation file is contained in the Anal	ysis
<u>Manager</u> : Defines the Manager, whic child processes	ch initializes memory management	and
<u>MgrHost</u> : The manager hostna	ame	
Attribute Proto: IP prot	tocol (IPV4 IPV6)	
<u>MgrHome</u> : The manager home o	lirectory	
<u>ConfigDir</u> : Concatenated wit absolute path for all confi Manual page realeyesIDS.xml(5) line 1	th configuration filenames to creat iguration files	e an

This screenshot shows the man page for IDS configuration files. The following man pages for the IDS and the DBD are included in the packages:

- Configuration scripts
- Configuration files
- Startup scripts

Demonstration of The Realeyes Intrusion Detection System

Jim Sansing May 14, 2008

For more information, see the project website and blog:

http://realeyes.sourceforge.net http://realeyes-tech.blogspot.com