Network Security Monitoring with Sguil and Open Source Tools

Eile Que	.3.1 ry <u>R</u> eports <u>D</u> a	atabase	Sound: Off								×
RealTime	Events Escalate	ed Events									
ST_CNT	Sensor	sid cid	Date/Time	Src IP	_	SPort	Dst IF)	DPort	Pr	Event Message
BT 1	-sensor-va	1 30889	2004-04-27 16:26:22	200 148	08 200	3604		13 196	80	6	WEB-PHP admin php access
BT 1	-sensor-va	1.30896	2004-04-27 16:44:48	67,234,73	3.114	0		13,199	8080	6	SCAN Proxy Port 8080 attempt
BT 2	-sensor-va	1.30904	2004-04-27 17:12:43	165.83.4	1.53	1099		13.196	80	6	WER-FRONTPAGE / vti bin/ access
RT 2	-sensor-va	1.30911	2004-04-27 17:32:45	167.24.10	04.150	31947		13.196	80	6	WEB-FRONTPAGE / vti bin/ access
BT 8	-sensor-va	1.30953	2004-04-27 19:05:26	207.46.24	18.113	80		13.194	1433	6	LOCAL RST conx attempt to port 1433
RT 2	-sensor-va	1.30963	2004-04-27 19:40:41	67.18.117	7.150	50361		13.196	8080	6	SCAN Proxy Port 8080 attempt y
ST CNT	Sonear	aid aid	Doto/Time	See 1D		CDout	Dat II	•	DDout	D.	Fuent Menness
DT 10	Sensor va	1 21/02	2004.04.28.12:40:57	216 1/0 1	246 199	59	Datil	12 104	DI UII	17	PAD TRAFFIC udp port 0 traffic
BT 5	-sensor-va	1 31477	2004-04-28 12:40:57	170 224 3	224 100	53		13 194	0	17	BAD-TRAFFIC udp port 0 traffic
BT 10	-sensor-va	1 31478	2004-04-28 12:41:00	170 224 3	24.100	53		13 194	ů.	17	BAD-TBAFFIC udp port 0 traffic
BT 10	-sensor-va	1.31512	2004-04-28 12:45:02	216 148 2	244.36	53	u i	13 194	Ň	17	BAD-TBAFFIC udp port 0 traffic
BT 1	-sensor-va	1.31589	2004-04-28 14:16:52	209.61.18	38,248	80		13.194	32771	6	spp rpc decode: Incomplete RPC segment
							_				
ST. CNT	Sensor	sid cid	Date/Time	Src IP		SPort	Dist IP	,	DPort	Pr	Event Message
BT 2	-sensor-va	1 31645	2004-04-28 17:38:16	12 43 23	3 212	3108	0.50 11	13 198	135	6	spp. portscap: Portscap Detected
BT 1	-sensor-va	1 31649	2004-04-28 17:38:10	80 35 178	3 206	2668	i i	13 202	135	6	spp_portscan: Portscan Detected
BT 1	-sensor-va	1.31650	2004-04-28 17:54:59	12.44.14	3.90	3638		13.199	135	6	spp_portscan: Portscan Detected
BT 1	-sensor-va	1.31651	2004-04-28 18:05:22	195 205	16 195	4729		13 198	135	6	spp_portscan: Portscan Detected
RT 1	-sensor-va	1.31652	2004-04-28 18:10:40	81.59.95.	5.30 1689 .13.199 135 6 spp portscan: Portscan Detected						spp_portscan: Portscan Detected
											· · · =·
Sec IP:	200 149 109 200	•					_				
Src Name	200.148.108.200	, del toloen i	net hr		Sho	w Packe	et Data	Show	Rule v	www.:	snort.org
0.010	12 108-200	J.dai.teleap.	ilet.bi		alert to	p \$EXTE	RNAL	_NET any -	-> \$HTTP	_SEI	RVERS \$HTTP_PORTS (msg:"WEB-PHP admin.php access";
Dst IP:	.13.196										X
Dst Name	.13.196				IP		Source	IP	Dest	IP	Ver HL TOS Ien ID Flags Offset TTL ChkSum
Revers	e DNS WI	nois Query:	🔶 None 🔶 Src IP 🗸	> Dst IP		200.	148.10	3.200	.13.19	96	4 5 0 427 65038 2 0 108 0
inetnum:	200.128/9								JAPF	۱S	F
status:	allocated		- Due - il	- Ini	тер	Sou	rce D	est R R I	RCSS	S Y	
owner:	BB-CGIN-LACN	ia internet n	o Brasil		TOP	Po	rt P	ort 10	<u>акн</u>		N Seq # Ack # Offset Res Window Urp ChkSum
responsib	le: Frederico A C	Neves				3604	1 80		. XX.		. 329488105 250565255 5 0 64800 272 0
address:	Av. das Nações	s Unidas, 11	541, 7° andar			50 ·	4F 53	54 20 2	F 61 64	4 6D) 69 6E 2E 70 68 70 3F POST /admin.php?
address:	04578-000 - São	o Paulo - SP				6F	70 3D	41 64 6	4 41 7	5 74	68 6F 72 26 61 64 64 op=AddAuthor&add
country:	ыл	_		<u>7</u>		SF 5	51 69 6F 61	6D 65 3	D 69 63	567 F64	65 72 61 26 61 64 64 5F 70 name=Goda&add p
					77	64 3D	70 6C 6	1 79 6	2 6F	79 61 26 61 64 64 5F wd=playboya&add_	
System I	vlessages User	Messages			DAI	• 65 ·	6D 61	69 6C 3	D 72 30	0 30	0 74 5F 53 79 73 74 65 email=r00t_Syste
						61	64 6D	69 6E 7	3 75 70	0 65	5 72 3D 31 26 61 64 6D adminsuper=1&adm
[2004-04-2	28 18:17:26] sguil	d: User sgu	il is monitoring sensor	s:		69	GE 3D	65 43 6	3 67 50	6 55	35 4A 54 30 34 67 55 in=eCcgVU5JT04gU
-sense	or-fl -sensor-v	/a	-			30	56 4D	52 55 4	E 55 49	9 44 0 00	45 76 4B 6A 6F 78 20 0VMRUNUIDEvKjox
1				FX	1	140	.,-+ .,4	30 71 3			VA 41 0.5 0.5 05 /V /4 III II / I.V. HULEDI.

Richard Bejtlich richard@taosecurity.com www.taosecurity.com / taosecurity.blogspot.com

Overview

- Introduction to NSM
- The competition (ACID, etc.)
- Sguil
- Case 1: 403 forbidden
- Case 2: MS-SQL grinding
- Case 3: MS-SQL version overflow attempt
- Case 4: Portscan
- Case 5: Admin-PHP access
- Case 6: SMB grinding
- Case 7: Port 20 to port 20
- Future developments

Introduction: My Background

- Hired 1 March 2004 by ManTech Intl. Corp.
- Previously at Foundstone (02-04), Ball Aerospace & Technology Corp (01-02)
- Captain in US Air Force CERT (98-01), trained as intel officer (96-01)
- Author of <u>The Tao of Network Security</u> <u>Monitoring</u> (Addison-Wesley, 800+ pages)
- Co-author of <u>Real Digital Forensics</u> (Addison-Wesley) with Keith Jones, Curtis Rose (Spring 2005)



Introduction: Network Security Monitoring

- NSM is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions
- NSM != IDS
- Intrusion detection vendors are alert-focused and consider their job done when they activate the "red blinking light"
- NSM assumes prevention eventually fails and some intruders are smarter than you
- Prepare for the worst by collecting everything you can, technically and legally

The Competition: ACID, etc.

- ACID (acidlabs.sf.net) and the like are Webbased alert browsers
- They only query, display, and store Snort alerts
- Do not give enough information for an analyst to make a decision
- Predominantly consider the number of alerts as a proxy for their severity
- No capability for workflow, alert categorization, analyst responsibility, or information sharing



ACID's high count implies 'bad'

Netscape:				0
File Edit View Go Communica	ator			Help
🛾 🌿 Bookmarks 🤳 Location: 🌆	p://127.0.0.1:8080/acid/aci	d_main.php	Y C	🗊 🕻 What's Related 🔟
Back Forward Reload	Home Search Netscape	Print Security	Shop Sto	ip.
Sport Apolygia C	oncolo for Intruci	n Databaaa	~	11
Short <u>A</u> nalysis <u>C</u>	onsole for Intrusi	on <u>D</u> atabase:	5	
Time window: [2000-07-29 10:05:05] - [2000-08-05 14:09:40]			
<u> </u>	Traffic Profile by Protocol			1
# of Sensors: 2	TCP (19%)			
Unique Alerts: 3 Total Number of Alerts: 11962	UDP (74%)			
 Source IP addresses: 460 Dest. IP addresses: 26 	ICMP (7%)			
 Search 				
 Snapshot 				
Alert Listing	MINISTRATION CONTRACTOR			
 Most recent 15 Alerts: any pro Graph Alert detection time 	tocol, TCP, UDP, ICMP			
	at of the Arcient project)			
ACID VU.3.2 (by Roman Danginy as pa	IT OF THE AIROCKT PROJECT)			<u>.</u>
a 100%				🏨 🔊 🖬 🥩

ACID's clunky query screen

Netscape: SnortACID: Query by Packet	0
File Edit View Go Communicator	Help
🛛 🌿 Bookmarks 🤳 Location: http://127.0.0.1:8080/acid/acid_pkt_main.php 👘 📝	🕼 What's Related 🚺
Back Forward Reload Home Search Netscape Print Security Shop ACID Query by Packet	Stop 10me Search Alert Listing
Meta Criteria	
Signature: { signature } 🖬	
Alert Time: = Jly [31 2000 _ [: [: []	ADD Time
IP Criteria	5.27
Address:	DD Addr
Misc:	
Layer-4: TCP UDP ICMP	
Payload Criteria	
Input Criteria Encoding Type: {Encoding } 🗖 Convert To (when searching): {Convert To } 🗖	The second
{payload } _ [ADD Payload
100%	🦝 🏎 🔊 🖬 🥓

ACID's questionable results

le Edit View	Go Communi	cator			
🎻 Bookmarks	🔳 🕹 Location: ht	tp://127.0.0.1:8080/a	cid/acid_pkt_main.p	hp	That's Relate
Back Forwa	ard Reload	Home Search Net	scape Print S	ecurity Shop	Stop
ACID	Query F	Results			Home Search Alert Listing
ueried DB on : I Aeta Criteria	Mon September 11 time = [07 /	1,200020:29:11 31 / 20001 [<i>any time</i>]			
P Criteria	201				
CP Criteria	anv				
avload Criteria	any				
	· ~···		J		
		Displaving	rows 1-50 of 2014		
ID	Signature	TimeStamp	Source Address	Destination Address	Layer 4 Proto
ID #0-(1-1792)	Signature TCP	TimeStamp 2000-07-31 11:42:49	Source Address 128.2.66.93	Destination Address 128.2.237.74	Layer 4 Proto TCP
ID #0-(1-1792) #1-(1-1793)	Signature TCP TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74	Destination Address 128.2.237.74 128.2.66.93	Layer 4 Proto TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794)	Signature TCP TCP TCP TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93	Destination Address 128.2.237.74 128.2.66.93 128.2.237.74	Layer 4 Proto TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795)	Signature TCP TCP TCP TCP TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93	Destination Address 128.2.237.74 128.2.66.93 128.2.237.74 128.2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796)	Signature TCP TCP TCP TCP TCP TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93	Destination Address 128 2.237.74 128 2.66.93 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796) #5-(1-1797)	Signature TCP TCP TCP TCP TCP TCP TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93	Destination Address 128 2.237.74 128 2.66.93 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796) #5-(1-1797) #6-(1-1798)	Signature TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93	Destination Address 128.2.237.74 128.2.66.93 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796) #5-(1-1797) #6-(1-1798) #7-(1-1799)	Signature TCP	Time Stamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.67.74	Destination Address 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796) #5-(1-1797) #6-(1-1798) #7-(1-1799) #8-(1-1800)	SignatureTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCPTCP	Time Stamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93	Destination Address 128 2.237.74 128 2.66.93 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796) #5-(1-1797) #6-(1-1798) #7-(1-1799) #8-(1-1800) #9-(1-1801)	Signature TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93	Destination Address 128.2.237.74 128.2.66.93 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796) #5-(1-1797) #6-(1-1798) #7-(1-1799) #8-(1-1800) #9-(1-1801) #10-(1-1802)	Signature TCP	TimeStamp 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93	Destination Address 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.66.93 128.2.237.74 128.2.237.74 128.2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1796) #5-(1-1797) #6-(1-1798) #7-(1-1799) #8-(1-1800) #9-(1-1801) #10-(1-1803)	Signature TCP	Time Stamp 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.237.74 128.2.66.93 128.2.237.74	Destination Address 128 2.237.74 128 2.66.93 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.237.74 128 2.66.93 128 2.237.74 128 2.66.93 128 2.237.74 128 2.66.93 128 2.237.74	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP
ID #0-(1-1792) #1-(1-1793) #2-(1-1794) #3-(1-1795) #4-(1-1795) #5-(1-1797) #6-(1-1797) #6-(1-1798) #7-(1-1799) #8-(1-1800) #9-(1-1801) #10-(1-1802) #11-(1-1803) #12-(1-1804)	Signature TCP TCP	TimeStamp 2000-07-31 11:42:49	Source Address 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.237.74 128.2.66.93 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74	Destination Address 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.237.74 128.2.66.93 128.2.66.93 128.2.237.74 128.2.66.93 128.2.237.74 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93 128.2.66.93	Layer 4 Proto TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP

A packet -- so what?

Netsca	ape: Packet Display t View Go Communicator				0 He
🐠 Во	okmarks 🤳 Location: [http://127.0.0.1:8080/acid/acid_pkt_main.php?submit=	=%230-%21	BT y 🕼	What's Relat	ed
Back	Forward Reload Home Search Netscape Print Security S	Shop	Stop		
ACID	Packet Display		Home Search	Alert Listin	ıg
Meta	ID # 1 - 11594 Time 2000-08-05 13:23:57 Signature TCP				
IP	source addrdest addrVerHdr LenTOSlengthIDflagsoffsetTTLoffset128.2.66.93205.164.217.3945071030160064Options0206	chksum 49982			
тср	source port dest port R 1 R 0 R R G P K K R S H S Y I N N F N N seq # ack offset res window 1120 80 X X 700156471 579464 255 0 32120	unp chks	sum 266		
	Options none				
	000 : 47 45 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A GET. /.HTTP/1.0 020 : 48 6F 73 74 3A 20 77 77 77 2E 73 6E 6F 72 74 2E Host: www.snor 040 : 6F 72 67 0D 0A 41 63 63 65 70 74 3A 20 74 65 78 org. Accept: t 060 : 74 2F 68 74 6D 6C 2C 20 74 65 78 74 2F 70 6C 61 t/html, text/p 080 : 69 6E 2C 20 61 75 64 69 6F 2F 6D 6F 64 2C 20 69 in, audio/mod, 0a0 : 6D 61 67 65 2F 2A 2C 20 76 69 64 65 6F 2F 2A 2C mage/*, video/ 0c0 : 20 76 69 64 65 6F 2F 6D 70 65 67 2C 20 61 70 70 .video/mpeq, .a	t. .ex la .i (*,			
4	Go to the next page in History list		H 🙀 3	2 dp 🕰	- 04

NSM Requirements

- Need to investigate different sorts of events
 - *Normal* activity triggers alerts but is not harmful
 - *Suspicious* activity is unusual but probably not harmful
 - *Malicious* activity is definitely designed to harm targets
- Need supporting data to make decisions
 - *Alert* data provides a potential indicator of security incidents
 - Session data is a content neutral summary of transactions
 - *Full content* data captures packet-level details, including application contents
 - Statistical data summarizes traffic



Sguil (sguil.sf.net)

- Sguil is an open source interface for NSM
- Written by Bamm Visscher, mostly in Tcl/Tk (cross-platform, especially the client)
- Consists of components to collect NSM data:
 - Alert data: Snort and Barnyard
 - Session data: SANCP or Snort stream4 keepstats
 - Full content data: Second instance of Snort
 - Statistical data: Nothing formal (yet)
- Detailed install docs for FreeBSD available; Linux, other BSDs work





Case studies

- The following case studies show real data collected during the last few weeks
- Local sensor watches traffic to and from various network perimeters
- Data has been sanitized to remove identifying information



SGUIL-0.3.1		en an	Manus Inves				×
<u>File Query Reports Database</u> Sound: Off		Ca	se 1			2004-04	⊦28 18:54:24 GMT
Estuded Events							
ST CNT Sensor sid.cid Date/Time RT 2 -sensor-va 1.30963 2004-04-27 1 RT 1 -sensor-va 1.30975 2004-04-27 2 RT 1 -sensor-va 1.30984 2004-04-27 2 RT 1 -sensor-va 1.30985 2004-04-27 2 RT 1 -sensor-va 1.30985 2004-04-27 2 RT 1 -sensor-va 1.30985 2004-04-27 2	Src IP 9:40:41 67.18.117.15 20:14:05 67.234.73.61 20:54:10 13.201 20:58:07 67.234.73.17 22:31:16 67.234.73.19	SPor 50 5036 0 80 73 0 30 0	t Dst IP 1 .13.196 .13.197 67.166.22.213 .13.200 .13.202	DPort Pr E 8080 6 S 8080 6 S 1547 6 A 8080 6 S 8080 6 S 8080 6 S 8080 6 S	Event Message SCAN Proxy Port 808 SCAN Proxy Port 808 SCAN Proxy Port 808 SCAN Proxy Port 808 SCAN Proxy Port 808	0 attempt 0 attempt <mark>5 403 Forbidden</mark> 0 attempt 0 attempt	
ST_CNT_Sensorsid_cidDate/Time	Src IP	SPor	t DstIP	DPort Pr F	vent Message		
RT 10 -sensor-va 1.31468 2004-04-28 1	2:40:57 216.148.246.	.132 53	.13.194	0 17 B	AD-TRAFFIC udp po	ort 0 traffic	
Why did the tar	get resp ul it's t	oond he i	with 4 ntrude	03 Fo r's att	rbidden empt wi	? This nich is	[]
ST CN more in	nortont		on tha		failed		
RT 1 MOLE III	iportant	. (ev	en tho	ugnit	ialieu)		
RT 1 -sensor-va 1.31652 2004-04-28 1	8:10:40 81.59.95.30	1689	13.199	135 6 s	pp_portscan: Portsc	an Detected	
RT 1 -sensor-va 1.31655 2004-04-28 1	8:22:36 205.205.1.11	6 3766	13.198	21 6 s	pp_portscan: Portsc	an Detected	
RI 1 -sensor-va 1.31659 2004-04-28 1	8:35:41 69.37.90.39	125 4066	13.198	135 6 s	pp_portscan: Portsc	an Detected	
Src IP: .13.201 Src Name: .13.201	Fio	Show Pac	ket Data 🔳 Show rver,established;	/ Rule www.sn content:"HTTP/1	ort.org .1 403"; depth:12; cl	asstype:attempted-re	con; sid:1201; re
Dst Name: a 07.100.22.213	I						
Dst Name: c-67-166-22-213.client.comcast.het		IP -	Source IP	Dest IP	Ver HL TOS len	ID Flags Offse	et ∏L ChkSum
Reverse DNS Whois Query: \diamondsuit None \diamondsuit	Src IP 🔶 Dst IP		.13.201 6	7.166.22.213	4 5 0 245	26242 2 0	128 1
CustName: Comcast Cable Communications, IP Ser Address: 3 Executive Campus Address: 5th Floor City: Cherry Hill	vices	TCP So P 80	ource Dest R R Port Port 1 0 1547	U A P R S F R C S S Y I G K H T N N . X X	Seq # Ack # 240608196 60453313	Offset Res Windo 30 5 0 64849	ow Urp ChkSum 383 0
StateProv: NJ PostalCode: 08002 Country: US RegDate: 2003-06-19 Updated: 2003-06-19 System Messages User Messages	- 	48 62 40 30 20 31 0F DATA 6E 6D	54 54 50 2F 69 64 64 65 69 63 72 6F 0D 0A 44 61 41 70 72 20 36 20 47 4D 6E 3A 20 63 74 2D 54 79 6C 0D 0A 43	31 2E 31 20 3 6E OD 0A 53 0 73 6F 66 74 2 74 65 3A 20 3 32 30 30 34 2 54 0D 0A 43 0 6C 6F 73 65 0 70 65 3A 20 0 6F 6E 74 65 0	34 30 33 20 46 6 65 72 76 65 72 3 2D 49 49 53 2F 3 54 75 65 2C 20 3 20 32 30 3A 35 3 6F 6E 6E 65 63 7 0D 0A 43 6F 6E 7 74 65 78 74 2F 6 6E 74 2D 4C 65 6	F 72 HTTP/1.1 40 A 20 biddenSer 5 2E Microsoft-I 2 37 0Date: Tu 5 3A Apr 2004 24 4 69 16 GMTCom 4 65 on: close 8 74 nt-Type: te E 67 mlContent	3 For ver: IS/5. e, 27 0:55: necti Conte xt/ht -Leng
-sensor-fl -sensor-va [2004-04-28 18:24:09] -sensor-fl: /snort_data 10% [2004-04-28 18:46:51] -sensor-va: /snort_data 80% [2004-04-28 18:50:54] -sensor-fl: /snort_data 10%	%	74 74 0D 20	68 3A 20 31 6F 72 61 67 0A 43 61 63 6E 6F 2D 63	34 31 0D 0A 4 65 3A 20 36 2 68 65 2D 43 0 61 63 68 65 0	4U 53 2D 57 65 6 2E 30 2E 36 32 3 6F 6E 74 72 6F 6 0D 0A 0D 0A	2 53 th: 141MS 4 39 torage: 6.0 C 3ACache-Con no-cache	-Web5 .6249 trol:

<u>F</u>ile

SRC: MOVE /exchange/	.EML HTTP/1.1
SRC: Accept: */*	
SRC: overwrite: F	
SRC: Referer:	
http:// /exchange/	/?Cmd=dialog&template=dlg_movecopy
SRC: Content-Type: text/xml	
SRC: translate: F	
SRC: allow-rename: t	
SRC: destination:	
http:// .com/exchange/	.EML
SRC: Accept-Language: en-us	
SRC: Accept-Encoding: gzip, deflate	
SRC: User-Agent: Mozilla/4.0 (compatible; I	MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)
SRC: Host: .com	
SRC: Content-Length: 0	
SRC: Connection: Keep-Alive	
SRC: Cache-Control: no-cache	
SRC: Cookie: sessionid=5a7bb6ea-7780-4a	37-8501-40aaeced3390,0x409
SRC: Authorization: Basic Y2hzLXZhXGpsa	W06cnVkZGVyMQ==
SRC:	
SRC:	
DST: HTTP/1.1 403 Forbidden	
DST: Server: Microsoft-IIS/5.0	i ranscript snows an
DST: Date: Tue, 27 Apr 2004 20:55:16 GMT	attempted HTTP MOVE was
DST: Connection: close	
DST: Content-Type: text/html	not accepted by the server.
DST: Content-Length: 141	
DST: MS-WebStorage: 6.0.6249	I NIS IS NOT AN ATTACK.
DST: Cache-Control: no-cache	
DST:	7
D	ebug Messages

Debug Message

snort.log.1083106800 Creating unique data file on sensor-va. Copying the file from sensor-va. Removing file from sensor-va.



×

Sec.

	SGUIL-0).3.1				54 A A A A						
<u>E</u> ile	e <u>Q</u> ue	ery <u>R</u> eports	atabase S	Sound: <mark>Off</mark>	C .			7			2004-04-28 18	3:40:17 GM
R	lealTim	e Events	Escalated Events	Event Qu	Li	as	e	2				
С	lose	Export	WHERE event.tin	nestamp > '2004-04-01	'AND event.stat	us = 1 a	nd even	t.signature	e like 'M	S-S(QL%' LIMIT 500	Submit
ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP		DPort	Pr	Event Message	
NA	1	sensor	1.344	2004-04-01 03:50:53	198.6.1.4	53		.153.34	1434	17	MS-SQL ping attempt	
NA	1	sensor	1.7039	2004-04-05 17:54:14	198.6.1.5	53		.153.34	1434	17	MS-SQL ping attempt	
NA	1	sensor	1.14957	2004-04-08 02:35:48	198.6.1.4	53		.153.34	1434	17	MS-SQL version overflow attempt	
NA	1	sensor	1.27616	2004-04-17 10:42:44	198.6.1.4	53		.153.34	1434	17	MS-SQL ping attempt	
NA	1	sensor	1.27653	2004-04-17 22:30:25	198.6.1.4	53		.153.34	1434	17	MS-SQL version overflow attempt	
NA	1	sensor	1.28690	2004-04-22 22:26:17	198.6.1.4	53		.153.34	1434	17	MS-SQL ping attempt	
NA	1	sensor	1.28691	2004-04-22 22:26:18	198.6.1.5	53		.153.34	1434	17	MS-SQL ping attempt	
NA	1	sensor	1.28965	2004-04-24 16:54:41	198.6.1.3	53		.153.34	1434	17	MS-SQL version overflow attempt	

MS-SQL version overflow attempt -- what caused this?

		1				
	Src IP:	198.6.1.3		Show P	ack	et Dat
	Src Name:	cache02.ns.uu.net	DI	ME NET	1434	1 (mse
4	Dst IP:	.153.34				
	Dst Name:	.com		10		Sour
ł	Reverse	DNS Whois Query: 💠 None 🔶 Src IP 💠 Dst IP		IP	198.	6.1.3
á	Qualitana					I
	OrgiName: OrgiD: U	JU		ODE	53	
THE REAL PROPERTY OF	Address: City: As StateProv: PostalCode Country:	22001 Loudoun County Parkway hburn VA 2: 20147 US		D 1 T 1	04 61 73 00 65 72 09	76 8 70 0 07 01 C 77 6 C0 2 30 8
	System M	essages User Messages		DATA		011 0
	[2004-04-28 [2004-04-28 [2004-04-28	3 17:21:26] sensor: /snort_data 71% 3 17:51:26] sensor: /snort_data 71% 3 18:21:26] sensor: /snort_data 71%				

Show Packet Data Show Rule OME_NET 1434 (msg:"MS-SQL version									w.s	nor	t.org	3				0.417.	."	-+-0.	danth	.1. da	i ne 1	100.
JME_NET 1434 (msg: MS-SQL versio									vern	ow a	atter	npι	; co	nter	ու։ լ	U4 ;	ons	et:0;	aepin	:1; as	IZE:>	100;
ID		Sou	ırce	IP			Dest IP Ver				er	r HL TOS len					FI	lags	Offset	ΠL	Chk	Sum
IF	198	6.1	.3				.153.34 4 5					5	0	13	1	4413	4 2		0	246	0	
		Port							Por	t				L	engi	th			С	hkSur	n	
UDP 53						143	4				1	111					47537					
DATA	04 61 73 00 65 72 09	76 70 07 01 77 C0 3A	81 04 69 21 80	83 5F 73 77 00	00 74 00 73 01	01 63 06 21 42 51	00 70 00 3D 80	00 02 01 70 00	00 64 00 6F 00	01 63 03 00 73 2A	00 06 63 1B 74 30	00 5F 62 6D 00	05 6D 00 61 00	5F 73 00 29 73 0E	6C 64 00 75 74 10	64 63 6C 65 00	.v. ap. s. ewis r.!	 _tcr s.!. wsB= Q.	posti 	lc _msdc om!).1 maste	 ; ;	

□ 198.6.1.3_53	×										
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp											
@ ┣━ 😭 × @ ≞ @ ♀ ♀ ♥ 吞 ⊉ Q Q @ № Մ∋ Њ ※ 🔯											
No. Time Source Destination Protocol Info											
1 0.000000 .153.34 198.6.1.3 DNS Standard query SRV _ldaptcp.dc. 2 0.084216 198.6.1.3 .153.34 DNS Standard query response, No such	_msdcscom name										
<pre>> Frame 1 (92 bytes on wire, 92 bytes captured) > Ethernet II, Src: 00:a0:cc:3d:77:c7, Dst: 00:30:19:1c:12:40 > Internet Protocol, Src Addr: .153.34 (.153.34), Dst Addr: 198.6.1.3 (198.6.1.3) > User Datagram Protocol, Src Port: 1434 (1434), Dst Port: 53 (53) > Domain Name System (query)</pre>											
Domain Name System (query) Transaction ID: 0x0476 Flags: 0x0100 (Standard query) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Because we capture everything technically and legally possible, we see the outbound DNS query prompted a response which triggered Snort											
▽ Queries											
<pre>V_Idaptcp.dcmsdcscom: type SRV, class inet Name: _ldaptcp.dcmsdcscom Type: Service location Class: inet</pre>											
0000 00 30 19 1c 12 40 00 a0 cc 3d 77 c7 08 00 45 00											
➡ Expression So Clear So Apply	P: 2 D: 2 M: 0										

			the second for the second	Constant Providence		Start Start	an a			90008X	<u> Manaka (</u> ()) () ()	u en sa	Classifi (1775) (187	12 14 18 19 10 10		and the second of the	
<u>F</u> ile <u>Q</u> ue	ry <u>R</u> eports	<u>D</u> atabase	Sound: Off					~ 2							2004-04-2	28 18:33:08	3 GMT
RealTime	Events Esc	alated Events	Event Query 7			LC	22										
Close	Export	WHERE event.	timestamp > '200	4-04-01' /	AND eve	ent.signatu	re = 'M	S-SQL sa logi	n failed'	LIMI	Г 5 00					Sub	omit
ST CNT	Sensor	sid.cid	Date/Time	S	Src IP	S	Port D	st IP	DPort	: Pr	Event M	essage	e				
<mark>C3</mark> 1	-sensor-v	a 1.15679	2004-04-10 21	:48:05	.13.1	196 14	433 1·	47.83.170.157	2999	6	MS-SQL	sa log	in failed				
C3 1	-sensor-v	a 1.15680	2004-04-10 21	:48:05	.13.1	196 14	4 3 3 1	47.83.170.157	2988	6	MS-SQL	. sa log	in failed				
C3 1	-sensor-v	a 1.15681	2004-04-10 21	:48:05	.13.1	196 14	133 1-	47.83.170.157	2984	6	MS-SQL	sa log	jin failed				
<mark>C3</mark> 1	-sensor-v	a 1.15682	2004-04-10 21	:48:05	.13.1	195 14	433 1	47.83.170.157	2987	6	MS-SQL	. sa log	jin failed				
C3 1	-sensor-v	a 1.15683	2004-04-10 21	:48:05	.13.1	195 14	433 I [.]	47.83.170.157	2996	6	MS-SQL	. sa log	jin failed				
<mark>C3</mark> 1	-sensor-v	a 1.15684	2004-04-10 21	:48:05	.13.1	195 14	133 I-	47.83.170.157	3035	6	MS-SQL	. sa log	jin failed				- 1
C3 1	-sensor-v	a 1.15685	2004-04-10 21	:48:05	.13.1	196 14	433 1·	47.83.170.157	3028	6	MS-SQL	. sa log	jin failed				
C3 1	-sensor-v	a 1.15686	2004-04-10 21	:48:05	.13.1	195 14	433 1 [.]	47.83.170.157	3026	6	MS-SQL	. sa log	jin failed				
C3 1	-sensor-v	a 1.15687	2004-04-10 21	:48:05	.13.1	196 14	433 1·	47.83.170.157	3032	6	MS-SQL	. sa log	jin failed				
C3 1	-sensor-v	a 1.15688	2004-04-10 21	:48:05	.13.1	196 14	433 1·	47.83.170.157	3023	6	MS-SQL	. sa log	jin failed				
C3 1	-sensor-v	a 1.15689	2004-04-10 21	:48:06	.13.1	195 14	433 1·	47.83.170.157	3079	6	MS-SQL	. sa log	in failed				
C3 1	-sensor-v	a 1.15690	2004-04-10 21	:48:06	.13.1	196 14	433 1·	47.83.170.157	2949	6	MS-SQL	. sa log	jin failed				
C3 1	-sensor-v	a 1.15691	2004-04-10 21	:48:06	.13.1	196 14	433 1 [.]	47.83.170.157	2737	6	MS-SQL	. sa log	in failed				
	-sensor-v	a 1.15692	2004-04-10 21	:48:06	.13.1	195 14	433 1·	47.83.170.157	3000	6	MS-SQL	. sa log	in failed				
	-sensor-v	a 1.15693	2004-04-10 21	:48:06	.13.1	195 14	433 1·	47.83.170.157	2955	6	MS-SQL	. sa log	in failed				- 1
	-sensor-v	a 1.15694	2004-04-10 21	:48:07	.13.1	195 14	433 1·	47.83.170.157	3495	6	MS-SQL	sa log	jin failed				
-3 I	-sensor-v	a 1.15695	2004-04-10 21	:48:08	.13.1	195 14	433 I	47.83.170.157	3496	6	MS-SQL	. sa log	jin failed				
ا ت-	-sensor-v	a 1.15697	2004-04-10 21	:48:11	.13.	196 14	133	47.83.170.157	4693	ь	M2-201	. sa log	jin lalled				
																	— ï
Src IP:	.13.19	6				📕 Show	Packet	Data 🔳 Show	v Rule	www	.snort.or	g					
Src Name	.13.196	6				alert top	\$SQL	SERVERS 143	3 -> \$EXI	ERN	AL NET a	anv (m	sa:"MS-S	QL sa logir	n failed": c	ontent: "Lo	oain f
Dst IP:	147.83.170.1	157				N	+		- +				- 3	j			3
Dst Name	: ma3.euetib.	upc.es				10	S	ource IP	Dest	t IP	Ver	HL TO)S len	ID Fla	igs Offset	TTL Chk	«Sum
Revers	e DNS	Whois Query	y: 💠 None 💠 S	Src IP 🔶	Dst IP	IP	· · ·	13.196 1	47.83.17	0.157	4	5 0	99	44617 2	0	128 0	
inetnum:	147.83.0.0	- 147.83.255.2	55						UAP	RS	F						
netname:	UPCNET				- EI	TOD	Sourc	e Dest R R	RCS	SΥ	1						
descr:	Universitat I	Politecnica de	Catalunya			TCP	Port	Port 1 0	GКН	ΤN	N Sec	#	Ack #	Offset Ro	es Windov	v Urp Chk	ເSum
country:	FS						1433	4693	. X X		. 36368	6995 5	5400 2976 (650	64952	159 0	
admin-c:	XCT1-RIPE				- 11		04 0	00 3B 00	00 01 (00 A	A 27 00	18 4	8 00 00	01		1	
tech-c:	UNOC4-RIP	Έ			- 11		0E 1	3 00 4C 6F	67 69 6	6E 20	0 66 61	69 6	C 65 64	20Lo	gin fai	led	- 11
status:	ASSIGNED	PI	- O II-1				66 6	72 20 75	73 65 7	72 20	0 27 73	61 2	7 2E 00	00 for ι	iser 'sa	•••	- 11
remarks:	mail spam	reports: abus	e@realris.es		X.		00 0		00 00 (0 0	0 00 00			• • • • •	••••		- 11
					T												- 11
System	Messages) l	Jser Message	s			DATA							ا: م		طهر م ا	_	שו ר
_								M2-20	JL S	5 a	100	JIN	lall	eu a	iert	S	
[2004-04-	28 18 17 261 4	auild: Llear e	nuil is monitoring	coneare	. 11		:.	adica		ЛС	c cř	Ń	hru	to fo	rcin		
-sens	or-fl -sens	igunu. Oser si sor-va	yan is monitoring	1 2012012	·			iuica	le l	12)-JC-0	7	มาน			IY	
[2004-04-2	28 18:24:09]	-sensor-fl:	/snort_data 10%		.											-	- 4
1	-		_		- IV		J.										- Part

13.196_1433-147.83.170.157_4693-6.raw - Ethereal

File Edit View Go Capture Analyze Statistics Help

💫 🛧 🖢 [Q, Q, Q, [📭 🕼 🛣 [🗭 × 🕲 📇 (a) ↓ ↓

No	Time	Source	Destination	Protocol	Info
1	0.000000	147.83.170.157	.13.196	ТСР	4693 > 1433 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
2	0.000166	.13.196	147.83.170.157	ТСР	[TCP ZeroWindow] 1433 > 4693 [RST, ACK] Seq=0 Ack=0 Win=0 L(
3	0.671743	147.83.170.157	.13.196	ТСР	4693 > 1433 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
4	0.671892	.13.196	147.83.170.157	TCP	[TCP ZeroWindow] 1433 > 4693 [RST, ACK] Seq=3681655747 Ack=:
5	1.328130	147.83.170.157	.13.196	ТСР	4693 > 1433 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
6	1.328304	.13.196	147.83.170.157	TCP	1433 > 4693 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7	1.462238	147.83.170.157	.13.196	ТСР	4693 > 1433 [ACK] Seq=1 Ack=1 Win=65535 Len=0
8	1.465914	147.83.170.157	.13.196	TDS	Login Packet (Not last buffer)
9	1.600320	.13.196	147.83.170.157	ТСР	1433 > 4693 [ACK] Seq=1 Ack=513 Win=65023 Len=0
10	1.735437	147.83.170.157	.13.196	TDS	Login Packet
11	1.737302	.13.196	147.83.170.157	TDS	Response Packet
12	1.737334	.13.196	147.83.170.157	TCP	1433 > 4693 [FIN, ACK] Seq=60 Ack=584 Win=64952 Len=0
13	1.871827	147.83.170.157	.13.196	TCP	[TCP Dup ACK 7#1] 4693 > 1433 [ACK] Seq=584 Ack=1 Win=65535
14	1.872572	147.83.170.157	.13.196	ТСР	4693 > 1433 [FIN, ACK] Seq=584 Ack=61 Win=65476 Len=0
15	1.872675	147.83.170.157	.13.196	TCP	[TCP Keep-Alive] 4693 > 1433 [ACK] Seq=584 Ack=61 Win=65476
16	1.872739	.13.196	147.83.170.157	ТСР	1433 > 4693 [ACK] Seq=61 Ack=585 Win=64952 Len=0

⊽ Tabular Data Stream

Type: Response Packet (0x04)

Status: Last buffer in request or response (1)

Size: 59

B

Channel: 0

Packet Number: 1

Window: 0

▽ Token Oxaa Error Message

Length: 39

SQL Error Number: 18456

State: 1

Level: 14

Error length: 27 characters

Integration with Ethereal facilitates understanding binary protocols like TDS, SMB, RPC, etc.

Full content data retrieved from sensor is archived locally for forensic and investigative purposes

	Err	or:	Lo	gin	fai	lec	1 fc	or us	ser	'sa									-	
														-						
040	00	18	48	00	00	01	0e	1b	00	4c	6f	67	69	6e	20	66	<mark>H</mark> Login f			
050	61	69	6c	65	64	20	66	6f -	72	20	75	73	65	72	20	27	ailed fo r user '			
060	- 73	61	27	2e	00	00	00	00	fd	02	00	00	00	00	00	00	sa'			-
070	00																•			1
Ъf	ilter:														•	4	Expression ∑ <u>C</u> lear <u>✓ A</u> pply	P: 16 D: 16 M: 0		

🗖 SG	UIL-0.3.1															>
<u>F</u> ile	Query R	eports	<u>D</u> atabase	Sound: Off			<u> </u>								20	04-04-28 19:11:54 GMT
Real	Time Event	te Ì Feca	lated Events	.)			La	IS	e 4							
Tiea		La Laca		3												
ST C	CNT Sens	or	sid.cid	Date/Time	S	rc IP	S	Port I	Dst IP	DPort	Pr	Eve	nt Message	9		
	C		il na	rtccon	data		into	nar	atod a	nd	C	•h		targo	tc	
		gu	ii po	itstaii	uald	2 IS	IIICE	<u>-</u>	aleu				0005	Larye	LS	
				and p	orts	SCa	anne	ed.	blus ⁻	ТСР) f	fla	as			
				<u> </u>				/		<u> </u>	_		3-			N
ST C	CNT Sens	or	sid.cid	Date/Time	S	rc IP	S	Port [Dst IP	DPort	Pr	Eve	nt Message	2		
																<u> </u>
ST C	CNT Sens	or	sid.cid	Date/Time	S	rc IP	S	Port [Dst IP	DPort	Pr	Eve	nt Message	9		Δ
RT 1	-5	ensor-v	a 1.31257	2004-04-28 (07:05:17 19	95.240.20	1.196 38	848	.13.198	135	6	spp	_portscan:	Portscan Deteo	cted	
RT 1	-5	ensor-v	a 1.31261	2004-04-28 (07:31:49 12	2.222.100	0.193 27	97	.13.201	2745	6	spp	_portscan:	Portscan Deteo	cted	f
RI 1	-5	ensor-v	a <u>1.3126</u> 2	2004-04-28 (07:34:47 21	<mark>13.93.11</mark> 8	.183 25	575	. <mark>13.198</mark>	443	6	spp	_portscan:	Portscan Deteo	sted	
RI 1	-5	ensor-v	a 1.31263		07:35:19 66	6.203.163	6.140 Z3	345	.13.200	135	6	spp	_portscan:	Portscan Detec	cted	
	-5	sensor-v	a 11.31260	0 2004-04-28 (07:54:32 ZT	19.165.5.	178 4	133	.13.199	445	6	SDD	Dortscan:	Portscan Detec	ctea	مرز ا
Src IF	P: 213.9	93.118.18	83						F	Display F	or	tscan	Data 2	00 Max Rows	s	
Src N	ame: e118	183.upc	-e.chello.nl				Sensor		TimeStamp	S	rcli	•	SrcPort	DstlP	DstP	Port Scan Info 🏻 🎽
Dst IF	»:	.13.198					senso	or-2004	1-04-28 07:34:50	213.93.1	118	.183	2571	13.194	443	SYN *****S*
Dst N	ame:	13 198					-senso	or-2004	1-04-28 07:34:50	213.93.1	118	.183	3012	13.195	443	SYN *****S*
- D-	DNC		WE		e ID 🛆 I		senso	or-2004	1-04-28 07:34:50	213.93.1	118	.183	3013	13.196	443	SYN *****S*
- Re	verse Diva	`	whois Que	ry: 🗸 None 🔶			senso	or-2004	1-04-28 07:34:47	213.93.	118	.183	2574	13.197	443	SYN *****S*
inetn	um: 213	.93.116.0) - 213.93.11	9.255			senso	or-2004	1-04-28 07:34:51	213.93.	118	.183	3014	13.198	443	SYN *****S*
descr	ume: IK- '' Chell	INIJ-CAE	SLE)				senso	or-2004	1-04-28 07:34:50	213.93.	118	.183	25/6	13.199	443	SYN *****S*
count	trv: NL						senso	or-2004	1-04-28 07:34:50	213.93.	118	.183	23//	13.200	443	5 Y N 5
admir	1-c: LG4	ю-RIPE					·senso	or-2004	1-04-28 07:34:50	213.93.	118	.183	29/8 9570	13.201	443	5 Y N 5
tech-	c: RC48	32-RIPE					senso	n-2004	1 04 20 07:34:30	213.93.	110 110	100	23/9	13.202	443	31N 3 QVN *****Q*
tech-	C: HMC ₂· ∧⊂⊂i	BI-RIPE	: • A				sense	n-2004	1-04-20 07 :34:36	213.83.	110	103	23/8	13.202	443	SVN ******
remai	s. Assi ks: Cor	itact abi	use@chello.	nl concernina cri	minal		.coner	n-2004	1-04-28 07-34-30 1-04-28 07-34-56	213.33.	110	183	2577	13.201	443	SVN ****** S*
rema	ks: acti	vities lik	e spam, had	ks, portscans			senso	n- 2004	1-04-28 07 34 56	213.93	118	183	2576	13 199	443	SVN *****S*
notify	r: hostn	naster@	chello.at			X	senso	or-2004	1-04-28 07:34:56	213.93.	118	.183	2571	13.194	443	SYN *****S*

System Messages User Messages

-sensor-fl -sensor-va [2004-04-28 18:24:09] -sensor-fl: /snort_data 10% [2004-04-28 18:46:51] -sensor-va: /snort_data 80% [2004-04-28 18:50:54] -sensor-fl: /snort_data 10%

<u>F</u> ile <u>Q</u> uery <u>R</u> ep	oorts <u>D</u> atabase	Sound: Off							2	004-04- <mark>28</mark> 1	9:13:21 GMT
RealTime Events	Escalated Events	Ssn Query 5)								
Close Expor	t WHERE session	ns.start_time > '2	004-04-21' AND (s	sessions.src_ip	= INET_ATON('21	13.93.118.183') OR	sessions.c	lst_ip = INE	T_ATON('	213.93.118.	Submit
Sensor	Ssn ID Start	t Time	End Time	Src IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes 🔺
-sensor-va	10831376912(2004	1-04-28 07:34:50	2004-04-28 07:34	l:51 213.93.11	8.183 3012	.13.195	443	10	102	5	0
-sensor-va	1083137691522004	1-04-28 07:34:47	2004-04-28 07:34	1:51 213.93.11	8.183 2572	.13.195	443	7	0	6	0
-sensor-va	1083137691642004	1-04-28 07:34:50	2004-04-28 07:34	1:51 213.93.11	8.183 3013	. <mark>13.196</mark>	443	14	510	7	1994
-sensor-va	1083137691642004	1-04-28 07:34:51	2004-04-28 07:34	1:51 213.93.11	8.183 3014	.13.198	443	10	102	5	0
-sensor-va	10831376917:2004	1-04-28 07:34:47	2004-04-28 07:34	1:51 213.93.11	8.183 2573	.13.196	443	7	0	6	0
-sensor-va	10831376917:2004	1-04-28 07:34:47	2004-04-28 07:34	1:51 213.93.11	8.183 2575	.13.198	443	7	0	6	0
-sensor-va	10831377244:2004	1-04-28 07:34:51	2004-04-28 07:34	1:51 .13.	195 443	213.93.118.183	3012	1	0	0	0
-sensor-va	10831377244 2004	1-04-28 07:34:51	2004-04-28 07:34	1:51 .13.	196 443	213.93.118.183	3013	1	0	0	0
-sensor-va	10831377244 2004	1-04-28 07:34:51	2004-04-28 07:34	1:51 .13.	198 443	213.93.118.183	3014	1	0	0	0
-sensor-va	10831377244 2004	1-04-28 07:34:51	2004-04-28 07:34	1:51 213.93.11	8.183 2572	.13.195	443	1	0	0	0
-sensor-va	108313//244 2004	1-04-28 07:34:51	2004-04-28 07:34	1:51 213.93.11	8.183 25/3	.13.196	443	1	0	0	0
-sensor-va	10831377244 2004	1-04-28 07:34:4/	2004-04-28 07:34	1:52 213.93.11	8.183 25/4	.13.197	443	2	0	4	10
-sensor-va	10831377244 2004	104-28 07:34:51	2004-04-28 07:34	EST 213.93.1	8.183 25/5	13.198	443	1	0	0	0
-sensor-va	10831377613t2004	H04-28 07:34:47	2004-04-28 07:34	1:56 213.93.1	8.183 2571	.13.194	443	6	0	0	0
-sensor-va	1083137761382004	HU4-28 U7:34:47	2004-04-28 07:34	1.56 Z13.93.1	0.103 2575	13,199	443	6	0	0	0
-sensor-va	10831377613(2004	HU4-28 U7:34:47	2004-04-28 07:34	1.56 213.93.1	0.103 23/7	13.200	443	6	0	0	0
-sensor-va	1083137761382004	HU4-28 U7:34:47	2004-04-28 07:34	1.36 ZI3.93.1	0.103 23/0	13.201	443	6	0	0	0
-sensor-va	10031377013(2004	104-20 07.34.47	2004-04-20 07.34	1.50 213.33.1	0.103 2373	.13.202	440	0	U	U	7
Src IP: 213.93	.118.183					Display Portscan	Data 20	0 Max R	ows		_
Src Name: e11818	33.upc-e.chello.nl			Sensor	TimeStamp	SrclP	SrcPort	DstlP	Dst	Port Sc	an Info 🛛 🔺
Dst IP: .1	13.196				<u> </u>			• •		ר	
Dst Name: .1	13.196			Ouer	'v for t	rattic tr	om	Intru	lder		
Reverse DNS	Whois Query	y: 🔷 None 🔶 S	Grc IP 🔷 Dst IP	ÌP ch	, NNS a	t least i	one	lena	thv		
% This is the RIPE	Whois server.							icity	city		
% The objects are	in RPSL format.			l int	eractio	on with	a ta	arget	-		
% Rights restricte	ed by copyright.			Cinco		ontont	ماله	- -	n + c		
% See http://www.	ripe.net/ripencc/pul	b-services/db/coj	pyright.html			Untent	COIIE	ECLIO			
instrum: 212.0	9 1 1 6 0 9 19 09 1 10	255		n	rt 1/1	2 ic dic	ahla	d na	`		
netname: TK-N	3.116.0 - 213.93.119. IJ-CARLE	.233		P	UIL 44.	2 12 UI20	anie	u, nc	J		
descr: Chello	DHCP			•	rancer	inte av	ailal	hla			
country: NI			X	Ľ	lansci	ipts av	anai				
Suctom Maccaa		c)									
	es Oser Messages	3									
-sensor-fl [2004-04-28 18:24	-sensor-va :09] -sensor-fl: <i>l</i>	/snort data 10%									
2004-04-28 18:46	:51] -sensor-va:	: /snort_data 80%									
[2004-04-28 18:50	:54] -sensor-fl: /	/snort_data 10%									7
			T							'	

×

□ SGUIL-0.3.1

Still query for session data around the time of the attack to see if target system suddenly initiated an outbound connection, or if a new party connected to the victim on another port. Essentially, look for anything suspicious. Nothing happened here, so our estimate is all is well.

Close	Export WHERE sessions.sta	art_time between '2004-0	4-28 07:34' and	1 2004-04-28	07:40' AND	(sessions.src_ip	= INET_ATC	DNC .	13.196') (OR sessic	Submit
ensor	Ssn ID Start Time	End Time	Src	: IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes
-sensor-va	108313769252004-04-28	07:34:00 2004-04-28	07:34:00 216	6.99.65.10	40480	.13.196	443	12	1404	8	612
-sensor-va	1083137646(2004-04-28	07:34:05 2004-04-28	07:34:06 164	4.159.185.74	4671	.13.196	443	3	0	4	0
-sensor-va	1083137646(2004-04-28	07:34:05 2004-04-28	07:34:06 164	4.159.185.74	4672	.13.196	443	3	0	4	0
-sensor-va	108313769232004-04-28	07:34:05 2004-04-28	07:34:06 164	1.159.185.74	4673	.13.196	443	16	2532	12	3200
-sensor-va	108313769232004-04-28	07:34:06 2004-04-28	07:34:06 164	4.159.185.74	4671	.13.196	443	1	0	0	0
-sensor-va	108313769232004-04-28	07:34:06 2004-04-28	07:34:06 164	1.159.185.74	4672	.13.196	443	1	0	0	0
-sensor-va	108313769232004-04-28	07:34:06 2004-04-28	07:34:07 164	1.159.185.74	4674	.13.196	443	12	1340	8	612
-sensor-va	108313768172004-04-28	07:34:41 2004-04-28	07:34:41 165	5.83.9.71	3505	.13.196	443	3	0	4	0
-sensor-va	108313768172004-04-28	07:34:41 2004-04-28	07:34:41 165	5.83.9.71	3506	.13.196	443	3	0	4	0
-sensor-va	108313772442004-04-28	07:34:41 2004-04-28	07:34:41 165	5.83.9.71	3505	.13.196	443	1	0	0	0
-sensor-va	108313772442004-04-28	07:34:41 2004-04-28	07:34:41 165	5.83.9.71	3506	.13.196	443	1	0	0	0
-sensor-va	108313772442004-04-28	07:34:41 2004-04-28	07:34:43 165	5.83.9.71	3509	.13.196	443	16	2620	12	5128
-sensor-va	108313772442004-04-28	07:34:43 2004-04-28	07:34:44 165	5.83.9.71	3510	.13.196	443	12	1302	8	612
-sensor-va	108313769172004-04-28	07:34:47 2004-04-28	07:34:51 213	8.93.118.183	2573	.13.196	443	7	0	6	0
-sensor-va	108313769162004-04-28	07:34:50 2004-04-28	07:34:51 213	3.93.118.183	3013	13.196	443	14	510	7	1994
-sensor-va	108313772442004-04-28	07:34:51 2004-04-28	07:34:51	.13,196	443	213.93.118.183	3013	1	0	0	0
-sensor-va	108313772442004-04-28	07:34:51 2004-04-28	07:34:51 213	8.93.118.183	2573	.13.196	443	1	0	0	0
-sensor-va	108313770072004-04-28	07:35:00 2004-04-28	07:35:00 216	6.99.65.10	40477	.13.196	443	3	0	4	0
-sensor-va	108313770072004-04-28	07:35:00 2004-04-28	07:35:00 216	6.99.65.10	40480	.13.196	443	3	0	4	0
-sensor-va	108313776132004-04-28	07:35:00 2004-04-28	07:35:00 216	6.99.65.10	40477	.13.196	443	1	0	0	0
-sensor-va	108313776132004-04-28	07:35:00 2004-04-28	07:35:00 216	6.99.65.10	40480	.13.196	443	1	0	0	0
-sensor-va	108313776142004-04-28	07:35:00 2004-04-28	07:36:01 216	6.99.65.10	40675	.13.196	443	19	2666	16	3200
-sensor-va	108313776102004-04-28	07:35:01 2004-04-28	07:35:01 216	6.99.65.10	40677	.13.196	443	12	1404	8	612
-sensor-va	1083137707(2004-04-28	07:35:06 2004-04-28	07:35:07 164	1.159.185.74	4674	.13.196	443	3	0	4	0
-sensor-va	108313776132004-04-28	07:35:06 2004-04-28	07:35:07 164	1.159.185.74	4675	.13.196	443	16	2532	12	3200
-sensor-va	108313776132004-04-28	07:35:07 2004-04-28	07:35:07 164	1.159.185.74	4674	.13.196	443	1	0	0	0
-sensor-va	108313776132004-04-28	07:35:07 2004-04-28	07:35:08 164	1.159.185.74	4676	.13.196	443	12	1340	8	612
-sensor-va	108313770872004-04-28	07:35:08 2004-04-28	07:35:08 164	1.159.185.74	4673	.13.196	443	3	0	4	0
-sensor-va	108313776132004-04-28	07:35:08 2004-04-28	07:35:08 164	1.159.185.74	4673	.13.196	443	1	0	0	0
-sensor-va	108313771672004-04-28	07:35:16 2004-04-28	07:35:16 24.3	210.223.71	2781	.13.196	443	3	0	4	0

SGUIL-0	.3.1						in an									×
<u>F</u> ile <u>Q</u> ue	ry <u>R</u> eports	<u>D</u> atabase	Sound: Off											2	2004-04-28 1	8:18:23 GMT
D IT'							35	e 5								
Reallime	Events Esc	alated Events														
ST CNT	Sensor	sid.cid	Date/Time		Src IP		SPort D)st IP	DPort	Pr Ev	ent Mess	sage				\square
RT 1	-sensor-v	/a 1.30889	2004-04-27	16:26:22	200.148.	108.200	3604	<mark>13.196</mark>	80	6 WE	EB-PHP a	.dmin.ph	p access	;		
RT 1	-sensor-\	/a 1.30896	2004-04-27	16:44:48	67.234.73	3.114	0	13.199	8080	6 SC	CAN Prox	y Port 80	80 atterr	npt		
RT 2	Concors	A 1 20004	2004 04 27	17.19.49	165 02 //	150	1000	12 106	00	C 14/			uti hini	200000		
		Alert	Indica	ates	ad	min	.pn	p acc	cess	Tro	m I	Brai	ZIIIā	an i	Ρ	
	-sensor-v	/a 1 30963	2004-04-27	19.40.41	67 18 11	7 150	50361	13 196	8080	6 50	AN Prov	v Port 80	R∩ atterr	Int		
	301301	74 1.50505	2004 04 27	10011	07.10.11		00001	10.100	0000	0 00		y i vitu	ov utten	ip:		
ST CNT	Sensor	sid.cid	Date/Time		Src IP		SPort D)st IP	DPort	Pr Ev	ent Mess	sage		6 7		
	-sensor-\	/a 1.31468	2004-04-28	12:40:57	216.148.	246.132	53	13.194	0	17 BA		-IC udp p ⊐IC udp p	ort 0 tra	ffic		
	-sensor-v	/a 1.314/7	2004-04-28	12:41:06	170.224.	224.100	53 59	13.194	0	17 BA		-iC uap p EIC uap i	ort O tra	unc		
BT 10	-sensor-v	/a 1.314/8	2004-04-28	12:41:00	216 148 2	244.152	53	13 194	0	17 BA	D-TRAFI	FIC udp i	ort 0 tra	unc		
RT 1	-sensor-v	/a 1.31589	2004-04-28	14:16:52	209.61.1	38.248	80	13.194	32771	6 SD	p rpc de	ecode: In	complet	e RPC s	eament	
															.	7
ST ONT	Sansor	sid oid	Date/Time		Sec IP		SPort D)et IP	DPort	Dr Ev	ont Mac	200				
BT 2	-sensor-v	/a 1.31645	2004-04-28	17:38:16	12.43.23	3.212	3108	13,198	135	6 sp	n nortse	an: Port	scan Det	ected		
RT 1	-sensor-v	/a 1.31649	2004-04-28	17:49:52	80.35.17	3.206	2668	.13.202	135	6 SD	p_portse	an: Port	scan Det	ected		
RT 1 RT 1 RT 1	Pa	cket	data ç	give	s de	etai	S: (ddA	uth	۱ <mark>۵۲</mark> ,	id	kieg	ger	а	 7
See ID:	200 140 100	200									1					
SFC IP : See Mamor	200.148.108	.200				📕 Shov	w Packet	Data 🔳 Sho	w Rule w	ww.sno	rt.org					
Src Name:	200-148-108	-200.dsl.teles	p.net.br			alert to	p \$EXTER	NAL_NET an	y -> \$HTTP	SERVE	RS \$HT	P_PORT	S (msg:	WEB-P	HP admin.p	hp access";
Dst IP:	.13.196	3				<u>M</u>										×
Dst Name:	.13.196	3				ID	So	ource IP	Dest I	P '	Ver HL	TOS I	en ID) Flag:	s Offset T	FL ChkSum
Revers	e DNS	Whois Query	y: 🔷 None 🔶	Src IP 🔍	> Dst IP	117	200.14	8.108.200	.13.19	6	4 5	0 42	7 6503	38 2	0 10	8 0
inetnum: status: owner: ownerid: responsib	200.128/9 allocated Comite Gest BR-CGIN-L/ le: Frederico	or da Internet ACNIC A C Neves	t no Brasil			тср	Sourc Port 3604	e Dest R F Port 1 (80	U A P R R C S S G K H T . X X .	SF YI NN	Seq # 2948810:	Ack 5 250565	# Off	set Res 0	Window U 64800 2	Irp ChkSum 72 0
address: address: country:	Av. das Nag 04578-000 - BR	ções Unidas, " São Paulo - S —	11541, 7° andar SP			DATA	50 4F 6F 70 5F 61 5F 6E 77 64	53 54 20 3D 41 64 69 64 3D 61 6D 65 3D 70 6C	2F 61 64 64 41 75 6B 69 65 3D 47 6F 61 79 62	6D 69 74 68 67 65 64 61 64 61 2 6F 79	9 6E 2E 3 6F 72 5 72 61 1 26 61 9 61 26	70 68 26 61 26 61 64 64 61 64	70 3F 64 64 - 64 64 - 5F 70 - 64 5F -	POST / op=Add _aid=k _name= wd=pla	admin.php Author&ad iegera&ad Goda&add_ yboya&add	י? ∆ Id Id .p
System N [2004-04-2 -senso	лessages U 8 18:17:26] s r-fl -sens	guild: User se or-va	s guil is monitorir	ng sensor	s:		65 6D 6D 40 61 64 69 6E 30 56 48 54	61 69 6C 68 75 73 6D 69 6E 3D 65 43 4D 52 55 54 50 2F	3D 72 30 68 2E 63 73 75 70 63 67 56 4E 55 49 31 2F 30	0 30 74 3 6F 6E 0 65 72 3 55 35 0 44 45 0 0D 04	+ 5F 53) 26 61 2 3D 31 5 4A 54 5 76 4B A 41 63	79 73 64 64 26 61 30 34 6A 6F 63 65	74 65 5F 72 64 6D 67 55 78 20 70 74	email= m@hush admins in=eCc 0VMRUN HTTP/1	r00t_Syst .com&add_ uper=1&ad gVU5JT04g UIDEvKjox .0Accen	.e .r lm (U :. .t. ∡

-sei	180	r-va	30	889
			_	

Transcript captures Web server reply showing 405 error

Sensor Name:	-sensor-va	
Timestamp:	2004-04-27 16:26	:22
Connection ID:	-sensor-va 3	0889
Src IP:	200.148.108.200	(200-148-108-200.dsl.telesp.net.br)
Dst IP:	.13.196	(13.196)
Src Port:	3604	, ,
Dst Port:	80	

SRC: POST

/admin.php?op=AddAuthor&add_aid=kiegera&add_name=Goda&add_pwd=playboya&add_email= r00t_System@hush.com&add_radminsuper=1&admin=eCcgVU5JT04gU0VMRUNUIDEvKjox HTTP/1.0 SRC: Accept: */*

SRC: Accept-Language: en-us

SRC: Content-Encoding: gzip, deflate

SRC: Content-Type: application/x-www-form-urlencoded

SRC: Host: com

SRC: User-Agent: Mozilla 4.0 (Linux)

SRC: Content-Length:0

SRC: Connection: Close

SRC:

SRC:

DST: HTTP/1.1 405 Method not allowed

DST: Server: Microsoft-IIS/5.0

DST: Date: Tue, 27 Apr 2004 16:35:51 GMT

DST: Allow: OPTIONS, TRACE, GET, HEAD

DST: Content-Length: 3923

DST: Content-Type: text/html

DST:

Debug Messages

Your request has been sent to the server. Please be patient as this can take some time. Using archived data: /snort_data/archive/2004-04-27/ -sensor-va/200.148.108.200:3604_

.13.196:80-6.raw



×

Did intruder do anything else? Query session data.

Query Builder

×

—Select Query Type Events Sessions





SGUIL-0.	.3.1												×
<u>F</u> ile <u>Q</u> uer	ry <u>R</u> eports <u>I</u>	<u>D</u> atabase	Sound: Off								2	2004-04-28	18:20:48 GMT
RealTime	Events Escala	ated Events	Ssn Query 1)									
Close	Export WH	ERE sessio	ns.start_time > '2	004-04-21'AND (s	essions.s	rc_ip = INET_a	ATON('200	0.148.108.200') O	R sessions.	dst_ip = II	NET_ATON	('200.148.1	0 Submit
Sensor	Ssn ID) Star	t Time	End Time	Src	IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes 🔺
-sensor	r-va 108308	331832(2004	-04-27 16:26:22	2004-04-27 16:26	:23 200	.148.108.200	3604	.13.196	80	12	774	9	8206
-sensor	-va 108308	32261:2004	HU4-27 16:26:23	2004-04-27 16:26	:23	13.196	80	200.148.108.200	3604		U	U	U
		-	•	•			-					7	
	l Se	SSIO	n data	shows	only	v one	tra	nsacti	on, a	and	it		
		corr	acnon	ds to n	ack	, ot wh	ich	Calico	ما مُاد	rt			
		COII	CSPOI	us to p	acr			cause					
				<u>.</u>	• •			_					
			Can als	o launo	ch ti	ransc	ript	s from	this				
			windo	M Or OV		ito a i		auary	v hv				
			windu					query	IJу				
			m	odityin	g qu	iery k	bar a	at top					
								•					
													Y
Src IP:	200.148.108.20	00			Show I	Packet Data 🛽	Show R	ule www.snort	ora				_
Src Name:	200-148-108-2	00.dsl.teles	p.net.br		alert top \$	EXTERNAL N	IET anv ->	SHTTP SERVER	S \$HTTP P	ORTS (ms	a:"WEB-PI	HP admin.p	hp access":
Dst IP:	.13.196				A	·					3		
Dst Name:	.13.196				ID	Source I	Þ	Dest IP V	er HL TOS	i len	ID Flags	s Offset T	TL ChkSum

Reverse DNS Whois Query: \diamondsuit None \blacklozenge Src IP \diamondsuit Dst IP

inetnum: 200.128/9 status: allocated owner: Comite Gestor da Internet no Brasil ownerid: BR-CGIN-LACNIC responsible: Frederico A C Neves address: Av. das Nações Unidas, 11541, 7° andar address: 04578-000 - São Paulo - SP country: BR

System Messages User Messages

[2004-04-28 18:17:26] sguild: User sguil is monitoring sensors: -sensor-fl -sensor-va

	5																							
_		IP	200.	Sou .148	irce .108	IP .200	5		De:	st IP .196) i	V 4	/er	HL 5	TOS 0	i 42	en 7	ID 650) 38	Flags 2	Offset 0	TTL 108	ChkS 0	um
I	T	СР	Sou Po 360	rce ort 4	De Po	est ort	R P 1 0	U R G	AF CS KF	PR SS TT	SF YI NN	32	Seq	#	25	Ack	#	Off	set	Res '	Window 64800	/ Urp	ChkS	um
	D	ата	50 6F 5F 5F 77 65 6D 61 69 30 48	4F 70 61 64 60 40 64 65 56 54	53 3D 69 61 3D 61 68 6D 3D 4D 54	54 41 60 70 69 75 69 65 52 50	20 64 3D 65 6C 73 6E 43 55 2F	2F 64 6B 3D 61 3D 68 73 63 4E 31	61 41 69 47 79 72 75 67 55 2F	64 75 65 67 62 30 63 70 56 49 30	6D 74 67 64 6F 30 6F 65 55 44 0D	69 68 65 61 79 74 6D 72 35 45 0A	6E 6F 72 26 5F 26 3D 4A 76 41	2E 72 61 26 53 61 31 54 4B 63	70 26 26 64 61 79 64 26 30 6A 63	68 61 64 64 73 64 61 34 65	70 64 5F 64 74 5F 64 67 78 70	3F 64 64 70 5F 65 72 6D 55 20 74	POS op= _ai _na wd= ema m@h adm in= oVM HTT	iT /a AddA d=ki play ill=r ush. insu eCcg RUNU P/1.	dmin.p uthor8 egera8 oda∾ boya∾ 00t_Sy com∾ per=18 VUSJTC IDEvK 0Acc	hp? add id_p add_ jste id_r adm 04gU jox cept.	<u> *</u>	

□ SGUIL-0.3.1	an setting	and the states of the second				ue de la										×
<u>File Query R</u>	eports <u>D</u> atab	ase Sound: Off			C -		- 6							200	4-04-28 18	:26:41 GMT
RealTime Ever	nts Escalated	d Events) Event Que				156										
Close Exp	ort WHERE	event.timestamp > '2(004-04-01	AND eve	ent.status =	=13 and (event.siar	nature n	ot like 'l	MS-SQL	%' LIMII	Г 1500				Submit
ST CNT Sense	or sid	.cid Date/Time		Src IP	S	Port Dst	:IP	DP	ort Pr	Event N	Messad	9				
C3 1 -s	ensor-va 1.8	452 2004-04-08	22:55:03	12.44.103	.112 30	631	.13.196	445	56	NETBIC	S SMB	Data Se	ervice Ses	sion Se	etup AndX	request u
C3 1 -s	ensor-va 1.1	1822 2004-04-09	16:07:26	12.44.103	.112 33	504	.13.195	445	56	NETBIC	S SMB	Data Se	ervice Ses	sion Se	etup AndX	request u
C3 1 -s	ensor-va 1.1	2538 2004-04-09	17:24:08	12.44.103	.112 44	199	.13.195	443	56	NETBIC	S SMB	Data Se	ervice Ses	ision Se	etup AndX	request u
C3 1 -s	ensor-va 1.1	2685 2004-04-09	17:51:45	12.44.103	.112 43	322	.13.195	443	56	NETBIC	S SMB	Data Se	ervice Ses	sion Se	etup AndX	request u
C3 1 -SI	ensor-va 1.1	2/59 2004-04-09	18:06:22	12.44.103	112 4	/28	.13.195	445	5 6	NETRIC	IS SWR	Data Se	ervice Ses	ision Se	etup AndX	request u
	ensor-va 1.1	2903 2004-04-09 2912 2004-04-09	18:32:00	12.44.103	112 20	118	13,195	445	5 6	NETBIC	DS SMB	Data Se	rvice Ses	sion Se	tup AndX	request u
			TO LOE IVV							THE TERM		L'atta d'u				7
Src IP: 12.4	4.103.112				Show	Packet Da	ata 🔳 Sh	ow Rule	e www	.snort.o	ra					
Src Name: wire	less103-112.aw	cable.com			alart tan	¢EVTEDN					meau"N	ETDIOS	SMD Dat	o Comi	no Socoion	Sotup And
Dst IP:	.13.195				alert top	AEVIEUN	AL_NET a	шу-> әг		101 445 (msg: N	етвюз	SIME Dat	a Servio	Se Session	i Setup Anc
Dst Name:	13.195					Sou	ree IP	D	iaet ID	Vor		nal 20	ID	Elage (Offect TT	ChkSum
Reverse DNS	Nonoc Whois	Quenc 🛆 None 🔶	Src IP	Dist IP	IP	12 44 10	3 112		13 105	401		/5 IEII	4500	nays v		
AT&T WorldNet	Services ATT (NET_12_0_0_0_1)				12.77.10	J.112		0.100	T		107	-500		, 113	V
ATEL WORldiver	12.0.0.0 - 12	2.255.255.255				Source	Dest R	RRC	SSY	г I						
ALASKA WIREL	ESS CABLE AL	ASKA-W74-102 (NET-	-12-44-102-	0-1)	TCP	Port	Port 1	0 G K	НΤΝ	N Se	eq #	Ack #	Offset	Res W	/indow Ur	p ChkSum
	12.44.102.0	- 12.44.103.255			2018	445 .	X	Χ	. 3305	10870 1	15128929	93 5	0 17	7122 59:	5 0	
# ARIN WHOIS	database, last u	updated 2004-04-27 1	9:15			00 00	01 68 FF	F 53 4	D 42 7	3 00 00	0 00 0	0 18 0	7 C8	h.SMB	s	
# Enter ? for ad	ditional hints o	n searching ARIN's V	VHOIS dat	abas		00 00	00 00 00	0 00 0	0 00 0	0 00 00	0 00 0	0 00 FF	F FE	 b	•••••	
e.						00 00	00 E4 00	0 00 0	0 00 0	0 D4 00	0008	0 2D 03	1 4E	n 	нz 	
						54 4C	4D 53 53	3 50 0	0 03 0	0 00 00			0 A4 TLI	1SSP		
Querying R	eassigned Bloc	CK: ALASKA WIRELES	SS CABLE	ALAS		00 00	00 18 00	0 18 0	0 BC 0 0 5E 0	0 00 00	0 1E 0	0 1E 00	0 40	:::::	••••••••	
104 107 102						00 00	00 10 00	0 10 0	0 D4 0	0 00 00	0 15 8	2 88 E	0 55		ų	
0				- 11		00 53	00 45 00 00 38 00	0520	02D0 0430	0 04500	o 41 o	0 74 00	033.5. 052.9	.E.R .8.6.C	3 .E.A.t.R	
Orginame: ALA	ASKA WIRELES -20	SS CABLE				00 32	00 32 00	0 7A 0	0 32 0	0 32 00	62 0	0 6F 00	0 61 .2	2.z.2	.2.b.o.a	
Address: 3055	BRADDOCK S	STREET				00 74 00 50	00 68 00 00 26 00	0 4C 0 0 55 0	0240 0530	0 74 00 0 45 00	0680 0520	0 69 00 0 20 00	041.t. 0.P	.h.L.\$.&.U.S	.t.h.i.A .E.R	
City: FAIRB/	ANKS				DATA		00	0 33 0	o 39 o	0 38 00	36 0	0 43 00	0 45	.3.9	.8.6.C.E	
Stateriov. AK						00 41	00 1C D4 00 00 00	4 61 43 0 00 0	2860 0000	1 52 E0 0 00 00	6 00 04 0 57 E	0 00 00 8 43 D4	000.A	aB.	.R	
	or in <i>l</i>	Alaska ig	: trv	ina	to	D4 FD	8A 65 18	8 25 2	1 93 5	9 35 74	4 90 E	3 9C 3E	B F0	.e.%!.	Y5t;.	
			5 CI Y	ii ig		41 C8 56 9A	3F 5B 50 10 00 51	02851 70063	BA26 9006	9 BD 73 F 00 64	3903° 4006	7 F6 49 F 00 7	9 DC A.' 7 00 V	۲LP(L. ⊌ i	i.s.7.I. n d о ш	
la esta	blish	SMB coi	nneo	ctio	ns 🛛	73 00	20 00 32	2 00 3	0 00 3	0 00 30	00 2	0 00 32	2 00 s.	.2.0.	0.02.	
				+ la : a		31 00 0 6F 00	39 00 39 77 00 71	5000	0005 0003	7 00 69 2 00 30	9006 003	E 00 64 0 00 30	4 00 1.9	9.5 . s	W.i.n.d. 2000	
[2 LO	port 4	445 ICP	. IS	this	5	20 00	35 00 21	E 00 3	ŏŏŏŏ	$\tilde{0}$ $\tilde{0}$ $\tilde{0}$ $\tilde{0}$	ŏ ŏŏ ŏ	õ õõ õ	0 31 .	50.		
	· Io	aitimate	רב			FF 53	4D 42 2E	B 00 04	0 00 0	0 18 43 F FF FF	3 CO 04	0 00 00 0 00 E	0 00 .SI F FF	1B+	c	
	IC	giunate	51			01 01	õõ õč õõ	0 4A 6	č 4A 6	D 49 68	8 43 6	č 42 73	3 72	jij	mIhClBsr	-
				ЫX ,		00							•			A

13.195_445-12.44.103.112_2018-6.raw - Ethereal

10

<u>File Edit View Go Capture Analyze Statistics Help</u>

No 1	n Source	Destination	Protocol	Info	1
1	(12.44.103.112	.13.195	ТСР	2018 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460	
2	(.13.195	12.44.103.112	TCP	445 > 2018 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460	
3 :	112.44.103.112	.13.195	ТСР	2018 > 445 [ACK] Seq=1 Ack=1 Win=17520 Len=0	
4	212.44.103.112	.13.195	SMB	Negotiate Protocol Request	
5	2.13.195	12.44.103.112	SMB	Negotiate Protocol Response	L
6	2.13.195	12.44.103.112	SMB	[TCP Retransmission] Negotiate Protocol Response	
7	212.44.103.112	.13.195	TCP	[TCP Previous segment lost] 2018 > 445 [ACK] Seq=306 Ack=90 Win=17431 Len=0	
8	412.44.103.112	.13.195	SMB	[TCP Retransmission] Session Setup AndX Request, NTLMSSP_NEGOTIATE	
9	4 .13.195	12.44.103.112	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED	
10	5.13.195	12.44.103.112	SMB	[TCP Retransmission] Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE	
11	512.44.103.112	.13.195	TCP	[TCP Previous segment lost] 2018 > 445 [ACK] Seq=670 Ack=399 Win=17122 Len=0	
12	\$ 12.44.103.112	.13.195	SMB	Echo Request	
13	.13.195	12.44.103.112	TCP	445 > 2018 [ACK] Seq=399 Ack=306 Win=65230 Len=0 SLE=544608682 SRE=544608735	
14	\$ 12.44.103.112	.13.195	SMB	[TCP Retransmission] Echo Request	
15	<u>.13.195</u>	12.44.103.112	SMB	Echo Response	
16	.13.195	12.44.103.112	SMB	Session Setup AndX Response, Error: STATUS_ACCOUNT_LOCKED_OUT	
17	\$ 12.44.103.112	.13.195	TCP	2018 > 445 [ACK] Seq=723 Ack=491 Win=17030 Len=0	•
⊳ Et	hernet II, Src: •	00:06:b1:80:01:	10, Dst	: 00:0e:84:61:0e:e0	
⊳ In	iternet Protocol,	Src Addr:	.13.19	5 (.13.195), Dst Addr: 12.44.103.112 (12.44.103.112)	
⊳ Tr	ansmission Contr	ol Protocol, Sro	c Port:	445 (445), Dst Port: 2018 (2018), Seq: 452, Ack: 723, Len: 39	
⊳ Ne	etBIOS Session Se	rvice		Etheraal follows the entire session	
⊽ Sľ	1B (Server Messag	e Block Protoco	1)		
∇	SMB Header			and shows this is part of a brute	H
	Server Componen	t: SMB		forcing attempt. The target	
	Response to: 14				
	Time from reque	st: 0.002257000	second	account is locked out.	
	SMB Command: Se	ssion Setup And	X (0x73		
	NT Status: STAT	US_ACCOUNT_LOCK	ED_OVT	(0xc0000234)	•
0010) 00 4f 6a 52 40	00 80 06 02 c	C	0d c3 0c 2c .0jR@,	
0020) 67 70 01 bd 07	e2 5a 2c ea 3	c c4 ff	f6 82 50 <u>18</u> gpZ, . <p.< td=""><td></td></p.<>	
0030) <u>fd 2d 0f</u> 7c 00	00 00 00 00 2	3 ff 53	4d 42 73 <u>34</u> #.SMBs <mark>4</mark>	
0040	02 00 c0 98 07	c8 00 00 00 00	0 00 00	00 00 00 00	
0050	00 00 00 00 ff	fe 01 98 80 0	0 00 00	00	L
₩.	_ilter:			T The Expression The Apply NT Status code (smb.nt_status), P: 53 D: 53 M: 0	//

SGUIL-0.3.1			on and	uus alla an alla							×
<u>F</u> ile <u>Q</u> uery <u>R</u> ep	orts <u>D</u> atabase Sound: Off								20	04-04-28 1	8:30:27 GMT
RealTime Events	Escalated Events Event Query	Cat III Ssn G	Query 4								
Close Export	t WHERE sessions.start_time > '20	004-04-01' AND	(sessions.s	src_ip = INET_AT	ON('12.44	4.103.112') OR ses	sions.dst	_ip = INET	_ATON('12	.44.103.11	Submit
Sensor	Ssn ID Start Time	End Time	Sr	c IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes 🛛 🛓
-sensor-va	1081438831522004-04-08 15:40:31	2004-04-08 15:4	10:31 12.	44.103.112	2065	.13.195	445	7	0	4	0
-sensor-va	10814388813(2004-04-08 15:40:55	2004-04-08 15:4	41:21 12.	44.103.112	2609	.13.195	445	159	21406	126	15658
-sensor-va	10814388850 2004-04-08 15:40:31	2004-04-08 15:4	40:31 12.	44.103.112	2065	.13.195	445	1	0	0	0
-sensor-va	10814388850 2004-04-08 15:40:31	2004-04-08 15:4	10:34 12.	44.103.112	2073	.13.195	445	38	4152	36	5062
-sensor-va	10814389160 2004-04-08 15:40:34	2004-04-08 15:4	40:56 12.	44.103.112	2091	.13.195	445	114	14444	86	10240
-sensor-va	10814389160 2004-04-08 15:41:21	2004-04-08 15:4	41:21 12.	44.103.112	2609	.13.195	445	1	0	0	0
-sensor-va	10814390090{2004-04-08 15:41:21	2004-04-08 15:4	12:58 12.	44.103.112	3182	.13.195	445	1118	153546	866	110938
-sensor-va	1081439040022004-04-08 15:42:58	2004-04-08 15:4	43:27 12.	44.103.112	1415	.13.195	445	86	11174	66	7996
-sensor-va	10814391330(2004-04-08 15:44:02	2004-04-08 15:4	14:35 12.	44.103.112	2744	.13.195	445	154	20316	122	15502
-sensor-va	10814391330(2004-04-08 15:44:43	2004-04-08 15:4	14:43 12.	44.103.112	3663	13.200	445	2	0	0	0
-sensor-va	10814391950(2004-04-08 15:45:45	2004-04-08 15:4	15:48 12.	44.103.112	1224	13.198	445	4	0	0	0
-sensor-va	1081439344382004-04-08 15:44:41	2004-04-08 15:4	49:04 12.	44.103.112	3714	13.195	445	2555	348654	1970	253510
-sensor-va	1081439381042004-04-08 15:49:04	2004-04-08 15:4	19:04 12.	44.103.112	3714	.13.195	445	1	0	0	0
-sensor-va	10814394431(2004-04-08 15:49:23	2004-04-08 15:4	19:44 12.	44.103.112	1967	.13.195	445	218	28718	168	21772
-sensor-va	10814394502:2004-04-08 15:49:45	2004-04-08 15:	50:50 12.	44.103.112	3161	13.195	445	53	7174	46	5518
-sensor-va	10814395050(2004-04-08 15:50:50	2004-04-08 15:	50:50 12.	44.103.112	3161	.13.195	445	1	0	0	0
-sensor-va	10814395360:2004-04-08 15:50:50	2004-04-08 15:	51:15 12.	44.103.112	2504	.13.195	445	86	10456	68	7840
-sensor-va	10814395980;2004-04-08 15:51:14	2004-04-08 15:	52:40 12.	44.103.112	3648	.13.195	445	24	1810	18	2188
-sensor-va	10814396910:2004-04-08 15:53:34	2004-04-08 15:	53:55 12.	44.103.112	2567	.13.195	445	60	6838	42	4822
Src IP: 12.44.1	03.112		- Show	Bosket Data 🗔 🤅	Chau Du		~ [
Src Name: wireles	s103-112.awcable.com				SHOW RU		y				
Dst IP: .1	3.195										(5)
Dst Name: .1	3.195			Source IP		Dest IP Ver	HL TOS	len l	D Flags	Offset T	L ChkSum
Reverse DNS	Whois Query: 🔷 None 🔶 S	rc IP 🔷 Dst IP	IP								
AT&T WorldNet Se	ervices ATT (NET-12-0-0-0-1)	4			U A	PRSF					
	12.0.0.0 - 12.255.255.255			Source Dest	RRRC	CSSYI					
ALASKA WIRELES	S CABLE ALASKA-W74-102 (NET-12	-44-102-0-1)	TCP	Port Port	10GK	(HTNN <mark>Se</mark> q	# A	.ck # Of	ffset Res V	Window U	rp ChkSum
	12.44.102.0 - 12.44.103.255										
# ABIN WHOIS dat	tabase last undated 2004-04-27 19:1	15									
# Enter ? for addit	ional hints on searching ARIN's WH	OIS databas				_				_	—
е.	Ū				<u></u> <u> </u>	for seg	scini	n da	ita c	how	/C
				Qu	Ċŗÿ				icu J		י ט
1.		<u>مر</u> ار	-	l hu	ndr	ods of	sim	ilar	SAS	sion	S
Svetem Messade	e) Heer Message		DATA		····		5	IIMI .	505.		
System Message	3 Oser Messages				tc) multir)e <	svsta	ems		
								·			
[2004-04-28 18:17:	26] sguild: User sguil is monitoring	sensors:									
-sensor-fi -	Sensor-Va 091 -concor-fl: lenort data 109										
2004-04-20 10.24	ooj -sensor-n. /snort_uata 10%	2	-								<u>X</u>

□ 13.195_445-61.223.233.125_4571-6.raw - Ethereal ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp
$\textcircled{\begin{tabular}{lllllllllllllllllllllllllllllllllll$
Io. Time Source Destination Protoco Info
1 0.000000 61.223.233.125 .13.195 TCP 4571 > 445 [SYN] Seq=0 Ack=0 Win=32320 Len=0 MSS=1414 WS=3
2 0.000299 .13.195 61.223.233.125 TCP 445 > 4571 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=0
4 0.390924 61.223.233.125 .13.195 ICP 4571 > 445 [ACK] Seq=1 ACK=1 WIN=S60000 Len=0
5 0.494917 61.223.233.125 .13.195 SMB Negotiate Protocol Request
6 0.495121 .13.195 61.223.233.125 TCP [TCP ZeroWindow] 445 > 4571 [RST] Seq=1 Ack=3192247225 Win=0 Len=0
7 0.534161 61.223.233.125 .13.195 TCP [TCP ZeroWindow] 4571 > 445 [RST, ACK] Seq=1 Ack=138 Win=0 Len=0
▷ Frame 4 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: 00:0e:84:61:0e:e0, Dst: 00:06:b1:80:01:10
▷ Internet Protocol, Src Addr: 61.223.233.125 (61.223.233.125), Dst Addr: .13.195 (.13.195)
⊽ Transmission Control Protocol, Src Port: 4571 (4571), Dst Port: 445 (445), Seq: 1, Ack: 1, Len: 0
Source port: 4571 (4571)
Destination port: 445 (445) Adding a Sport rule to knock down
Sequence number: 1
Acknowledgement number: 1 CONNECTIONS WITH ICP RSIS FOILS A SIMILAR
Header length: 20 bytes hruto forcing attack
▷ Flags: 0x0014 (RST, ACK)
Window size: 0
Checksum: 0x5c2a (correct)
▼ SEQ/ACK analysis
⊽ TCP Analysis Flags
This is a TCP duplicate ack
This is a ZeroWindow segment
Duplicate ACK #: 1
Duplicate to the ACK in frame: 3
0000 00 06 b1 80 01 10 00 0e 84 61 0e e0 08 00 45 00aE.
0010 00 28 c3 16 00 00 59 06 5d 6e 3d df e9 7d .(Y.]n=}
0020 0d c3 11 db 01 bd 27 6d 31 e3 ed a8 b7 c9 50 14'm 1P.
Filter: ► + Expression So Clear Apply P: 7 D: 7 M: 0

	Del Contra	15 and a strat	A Martin Martin State		a an		SAN STRAL		GANADA.	SI DESTA				BUSIDES.	selling and			
<u>F</u> ile <u>Q</u> ue	ry <u>R</u> epo	rts <u>D</u> atabase	Sound: Off													2004-04-2	8 18:44:	36 GMT
RealTim	e Events	Escalated Even	ts Èvent Qu			Li	35	e /										
Close	Export	WHERE event.	timestamp > '20	004-04-01	AND e	vent.stati	us = 15 L	IMIT 500									Su	ubmit
ST CNT	Sensor	sid.cid	Date/Time		Src IP		SPort	Dst IP		DPo	rt Pr	Event M	lessad	e				7
C5 1	senso	r 1.28845	2004-04-23	15:40:09	66.159.3	219,196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.28846	2004-04-23	15:40:12	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.28847	2004-04-23	15:40:19	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.28859	2004-04-23	18:57:50	66.159.3	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.28860	2004-04-23	18:57:53	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.28861	2004-04-23	18:58:00	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	or 1.28940	2004-04-24	12:15:08	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	[Donoat	tod tr	~ffi/	- fr	om	noi	+ 20) +/	n r		4 7	\cap	vazit	⊦h r	\mathbf{a}		
C5 1	ſ	repea		anno			μυι	ιZU		υþ		ιΖ	υ,	VVI		10		_
C5 1		-	anr	lica	stic	n d	-ta	۱۸/	ha	t i	c t	hic	2					_
CS 1			aht	лсс		n u	ala	. VV	IIa	LI	5 (.1115	1					
	senso	1 1 20004	2004-04-24	14.10.45 21.10.41	66 150	210.100	20	.150).J4) 94	20	6	MISCIS	ource	Port 20	to <102	9 4		-
	senso	r 1.29004	2004-04-24	21.19.41	66 159	219.190	20	150	3.34	20	6	MISC S	ource	Port 20	to <102	4 4		_
C5 1	senso	r 1.23003	2004-04-24	21.13.44	66 159	219.196	20	159	3.34	20	6	MISC S	ource	Port 20	to <102	4		_
C5 1	senso	r 1,29095	2004-04-25	21:58:51	66,159	219,196	20	159	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.29096	2004-04-25	21:58:54	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.29097	2004-04-25	21:59:01	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.29160	2004-04-26	12:30:17	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.29161	2004-04-26	12:30:20	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
C5 1	senso	r 1.29162	2004-04-26	12:30:26	66.159.	219.196	20	.153	3.34	20	6	MISC S	ource	Port 20	to <102	4		
Care ID:	00 450 0												1					
STC IP:	66.159.2	19.196				📕 Shov	v Packet	Data 🔳 Sh	iow Ri	ule	www.s	nort.org						
Src Name	netblock	-66-159-219-196.	totalvelocity.co	m		alert to	sexter	NAL NET 2	20 -> \$	номе	NET	:1023 (m	sa:"M	ISC Sol	urce Por	t 20 to <102	4"; flags	:S.12; :
Dst IP:	-	153.34					+				_		.				, j .	>
Dst Name	:	.coi	n				Sc	urce IP		Dest	IP	Ver H	I TOS	S len	ID	Flags Offse	tΠLC	hkSum
Bevers	e DNS	Whois Query:	📣 None 🔶 🤅	Src IP 📣	Dst IP	IP	66 159	219 196	_	15	 3 34	4 5	0	48	21392	2 0	118 (ווייסמוו
- reters	C DITO	Thios duciy.					00.100	.210.100	<u> </u>		0.04	7	V	10	21002			,
OroName	: Total V	elocity					Sourc	o Doct R	BBI	4 P K 7 S S	SF VI							
OrgID:	TOTAL-9				- H.	TCP	Port	Port 1	0 G I	кнт	ŃŃ	Sea #	А	\ck #	Offset	Res Windov	V Urp Cl	hkSum
Address:	11301 W	. Olympic #552			- H		20	20			X	3004719	33 0		7	0 65535	590 0	
City: L	os Angele	S			- 11			LV -				000 17 10	0		<u> </u>	00000		
PostalCo	de: 90064				- 11		None.											11
Country:	US				- 11													- 11
					<u> </u>													- 11
		Y	>		- 1	DATA												- 11
System	Messages	User Message	s			DATA												- 11
[2004-04-2	28 18:43:19	9] sensor: Da	atabase Server	:														
192.168.1	0.2.	_																
[2004-04-2	28 18:43:19	9] sensor: Da	atabase Next C	ID: 29 744.														
1					IX.	-												14

SGUIL-0.3.1				the fallen en						l'anne the	>
<u>F</u> ile <u>Q</u> uery <u>R</u> ej	ports <u>D</u> atabase Sound: <mark>Off</mark>								200	04-04-28 1	3:48:50 GMT
RealTime Events	s Escalated Events Event Query	Cat V Ssn Qu	ery 1)							
Close Expo	rt WHERE sessions.start_time > 'a	2004-04-21' AND (:	sessions	s.src_ip = INET	_ATON('6	6.159.219.196') OP	l session:	s.dst_ip = l	NET_ATO	N('66.159.	Submit
Sensor	Ssn ID Start Time	End Time	Sr	c IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes 🛛
sensor	10829303880 2004-04-25 21:58:50	2004-04-25 21:59	:14	.153.34	4727	66.159.219.196	21	18	128	16	566
sensor	10829303880 2004-04-25 21:58:50	2004-04-25 21:58	:50	.153.34	4726	66.159.219.196	80	8	520	4	1642
sensor	10829304927 2004-04-25 22:01:32	2004-04-25 22:01	32 66	.159.219.196	80	.153.34	4726	1	0	0	0
sensor	10829304927 2004-04-25 22:01:32	2004-04-25 22:01	32 66	.159.219.196	80	.153.34	4726	1	0	0	0
sensor	10829826583 2004-04-26 12:30:17	2004-04-26 12:30	26 66	.159.219.196	20	.153.34	20	6	0	0	0
sensor	10829826583 2004-04-26 12:30:16	2004-04-26 12:30	:16	153.34	1554	66.159.219.196	80	8	520	4	1642
sensor	10829826899 2004-04-26 12:30:16	2004-04-26 12:30	:40	153.34	1555	66.159.219.196	21	18	124	16	566
sensor	10829836201:2004-04-26 12:46:04	2004-04-26 12:46	:04 66	.159.219.196	21	153.34	1555	4	170	2	0
sensor	10830726290 2004-04-27 13:29:42	2004-04-27 13:29	:52 66	.159.219.196	20	153.34	20	6	0	0	0
sensor	10830726290 2004-04-27 13:29:41	2004-04-27 13:29	:42	.153.34	3319	66.159.219.196	80	8	520	4	1642
sensor	10830726601 2004-04-27 13:29:41	2004-04-27 13:30	:05	.153.34	3320	66.159.219.196	21	18	128	16	566
sensor	10830727108 2004-04-27 13:31:50	2004-04-27 13:31	:50 <mark>66</mark>	.159.219.196	80	.153.34	3319	1	0	0	0
sensor	10830727108 2004-04-27 13:31:50	2004-04-27 13:31	:50 66	.159.219.196	80	.153.34	3319	1	0	0	0
sensor	10830844000:2004-04-27 16:45:59	2004-04-27 16:46	:09 66	.159.219.196	20	.153.34	20	6	0	0	0
sensor	10830844310 2004-04-27 16:45:58	2004-04-27 16:46:	:22	.153.34	3711	66.159.219.196	21	18	128	16	566
sensor	10830848343 2004-04-27 16:53:04	2004-04-27 16:53	:14 66	.159.219.196	20	.153.34	20	6	0	0	0
sensor	10830848655 2004-04-27 16:53:04	2004-04-27 16:53	:27	.153.34	3823	66.159.219.196	21	18	128	16	566
sensor	10830857952 2004-04-27 17:09:13	2004-04-27 17:09	:13 66	.159.219.196	21	.153.34	3823	4	170	4	0
sensor	10831614601 2004-04-28 14:10:04	2004-04-28 14:10:	:14 66	.159.219.196	20	.153.34	20	6	0	0	0
sensor	10831614601 2004-04-28 14:10:04	2004-04-28 14:10	27	.153.34	1148	66.159.219.196	21	18	126	16	566
sensor	10831614601 2004-04-28 14:10:03	2004-04-28 14:10:	:04	.153.34	1147	66.159.219.196	80	8	520	4	1642
Src IP:	.153.34		Show	Packet Data 🗌	Show R	ule www.snort.o	rg				
Src Name:	.com	r									
Dst IP: 66.159	0.219.196	F	(
Dst Name: netblo	ck-66-159-219-196.totalvelocity.com	1	ID	Source IF	,	Dest IP Ver	HL TOS	len l	D Flags	Offset T	TL ChkSum
Reverse DNS	Whois Query: 💠 None 💠 Sr	c IP 🔶 Dst IP	IP								
OrgName: Total OrgID: TOTAL- Address: 11301 City: Los Ange	Velocity 9 W. Olympic #552 eles	X L	тср	Source Dest Port Port	U / R R R 1 0 G	APRSF CSSYI KHTNN Sec	1# A	ck#Off	set Res V	Vindow U	rp ChkSum
StateProv: CA PostalCode: 9006 Country: US	4	¥		Sessi from	ion the	data q local l	uery P oi	y sh	ows	tra to	ffic the
System Messag	es User Messages		DATA	Tota	Ve	locity I	P. U	sinc		rts	80.
[2004-04-28 18:43 192.168.10.2. [2004-04-28 18:43	::19] sensor: Database Server: ::19] sensor: Database Next CID	29744.				20, an	d 21	LTČ	P.		
		図算		1							X

	sensor 1	0831	614	6018	7786
--	----------	------	-----	------	------

<u>F</u>ile

<u> </u>		
Sensor Name: Timestamp: Connection ID: Src IP: Dst IP: Src Port: Dst Port:	sensor 2004-04-28 14:10:04 sensor_108316 .153.34 (66.159.219.196 (1 1148 21	1460187786 com) netblock-66-159-219-196.totalvelocity.com)
DST: 220 web2k0 DST: SRC: user anony SRC: DST: 331 Anonyn DST:	06 Microsoft FTP Ser mous nous access allowed,	vice (Version 5.0). send identity (e-mail name) as password.
SRC: pass SRC: DST: 230 Anonyn DST: SRC: PORT 10,20 SRC: DST: 500 Invalid DST: SRC: RETR SRC: RETR SRC: AddybK.dll	nous user logged in. 00,111, <mark>36,4,125</mark> PORT Command.	Transcript shows local IP failing to retrieve AddybK.dll; probably infected with malware. Research ties DLL to centralmedia.ws, an adware developer. Note the private source IP in the "PORT" command.
SRC: DST: 150 Openin DST: DST: 425 Can't o DST:	g ASCII mode data co pen data connection.	nnection for AddybK.dll(62868 bytes).
		Debug Messages
snort.log.108317: Creating unique Copying the file f	5200 data file on senso rom sensor	or.

Removing file from sensor.



7

×

Bonus Coverage!

As I was preparing this presentation, something changed at a client's site...





<u>File Query F</u>	ile Query Reports Database Sound: Off 2004-05-10 22:45:19 GMT																
RealTime Eve	RealTime Events Escalated Events Ssn Query 26 Ssn Query 27 Ssn Query 28																
ST CNT Sen	sor sensor-va	sid.cid 1.40326	Date/Time 2004-05-10 21:2	27:06	Src IP 80.35.189.20	S 10 1:	Port Ds 204	st IP <mark>.13</mark>	3.210	DPor 135	t Pr 6	Even NETE	it Messa BIOS DCI	ge ERPC IS	yster	nActivat	or pi
RT 2 -	sensor-va sensor-va	1.40331 1.40370	2004-05-10 21:3 2004-05-10 21:4	33:56 14:33	62.101.72.12 12.44.103.10	24 23 00 43	8401 212	.13	3.210 3.210	135 135	6 6	NETE	BIOS DCI BIOS DCI	ERPC IS	yster vster	nActivat nActivat	or p: or p:
	Neve	er-be	fore-se	er	ı (at	this	s sit	e)	Ne	tBl	05	S D	DCE	RPC			
	ISystemActivator path overflow alerts appear!																
ST CNT Sen	sor	sid.cid	Date/Time		Src IP	s	Port Da	st IP		DPor	t Pr	Even	it Messa	ge			Ā
RT 1 -	sensor-va sensor-fl	1.40427 2.3868	2004-05-10 22:3	39:43 10:54	12.101.70.10	0		13	3.194 .152.2		1	LOC	AL Heart AL Heart	tbeat tbeat	-VA -FL		_11
											(LORA)						7
ST CNT Sen	sor sensor-va	sid.cid 1 40335	Date/Time 2004-05-10 21:3	35-33	Src IP	S 4	Port Ds 151	st IP 13	217	DPor 3127	t Pr	Even	it Messa portscar	ge 1: Portsi	can D	etected	Z
RT 1	sensor-va	1.40351	2004-05-10 21:3	38:28	12.45.104.14	19 44	889	.13	3.196	445	6	spp_	portscar	1: Ports	can D	etected	
RT 1 -	sensor-va	1.40369	2004-05-10 21:4	14:29	12.44.103.10	0 4	198	.13	3.196	135	6	spp_	portscar	1: Ports	can D	etected	
RT 1	sensor-va	1.40408	2004-05-10 22:4	43:54	210.125.31.7	'9 21	086	.13	3.199 3.199	4899	6	spp_	portscar	1: Ports	can D	etected	
Src IP: 80.3	35 189 200]] Chavu	Dealest	Data 🔳	0									
Src Name: 200	.red-80-35-18	9.pooles.rim	a-tde.net		alert tcp	SEXTER	NAL NE	T anv	-> \$HOM	ME NET	10rt.0	rg (msa:	"NETBIC	S DCEF	RPC IS	SystemA	ctivate
Dst IP:	.13.210						ſ					(<u></u> g.				.,	×
Dst Name:	.13.210				IP	So	urce IP		Dest	IP	Ver	HL T	OS len	ID	Flag	s Offset	TTL
Reverse DN	IS Whois Que	ery: 🔶 Non	e 🔶 Src IP 🔷	Dst IP		80.35.1	89.200		.13.21	0	4	5 0	1420	41048	2	0	112
netnum: 80 netname: R).32.0.0 - 80.3: IIMA	5.255.255		Ê	Top	Source	Dest I		APR: CSS	SF YI							
descr: TEL	EFONICA DE	E ESPANA Registry		- 1	TCP	Port	Port	100	KHTI	NN	Seq #	1	Ack #	Offset	Res \	Window	Urp <s< td=""></s<>
country: ES		regiony		- 1	-	1204	135		X		93154	47 32	6651377	5	0	16560	132 0
admin-c: AF	986-RIPE			- 1		90 06 0	0 03 10		00 H8 0	6 00 00 0 06 00)0)0		 		
tech-c: FLT	T14-RIPE					74 2C 9	96 D2 60	24 58 5E 00) 00 01 0	5 64 49 0 00 00	BU 7		1E2% DO t,`/	«X.,EdI.	p 		- 11
System Mess	ages) User	Messages			DATA	10 5E 0 10 00 0 AF 6E 3	00 00 02 00 00 80 72 F4 0C	96 F1) 00 7C 8 L F1 2A 4) 00 4D 4	E 00 00 D CE 11 1 52 42	A6 6	0 00 0 A 00 2 O 00 0	20 20 30 .nr	*M	 j.		- 11
[2004-05-10 22	:30:28] -s	ensor-fl: Dat	tabase Next CID): A		00 00 0 20 06 0	00 00 0D 00 00 20	F0 AC) BA 00 0) 00 4D 4	0 00 00 5 4F 57	A8 F 04 0	4 0B 0 0 00 0)0)0		 		- 11
[2004-05-10 22	:34:16] -s	ensor-va: /s	nort_data 87%	V	4	A2 01 (38 03 (00 00 00 00 00 00	00 00) 00 C0 0) 00 C0 0	0 00 00 0 00 00 5 00 00	00 0	0 00 4	16 16 8		F F		X

File Query Reports Database Sound: Off								2004-	05-10 22	:49:04 GMT
RealTime Events) Escalated Events) Sen Query 26) Sen	Query 27	Sen Query 28	2)							
Class Expert WHERE sessions start time > '2004 05 02'		iona aro in - INE	, ET AT	ON(100 25	100 000		accelone o	lot in -	INET A	Submit
Sensor Ssn ID Start Time End Time	AND (Sess	rc IP	SDort	Det ID	109.200		sessions.c	ss_ip = ss Byte	s D Pckt	Submit
-sensor-va 1084224470 2004-05-10 21:27:03 2004-05-10 1	21:27:03 80	35,189,200	1198	13.2	204	135	2	0	0	0
-sensor-va 1084224470 2004-05-10 21:27:04 2004-05-10	21:27:04 80	.35.189.200	1199	13.2	205	135	2	0	0	0
A query for coscion data	- cho		1200	13.2	206	135	2	0	0	0
A query for session data		VVS	1201	13.2	207	135	2	0	0	0
worm/intruder tried conr	nectir	na to 📗	1202	13.2	208	135	2	0	0	0
			1203	13.2	210	135	20	3552	10	120
port 4444 ICP on two t	arge	ts. 🛉	1219	13.2	210	4444	1 6	0	6	0
Naither shows any hyte	s of r	lata 📗	1205	13.2	211	135	22	3552	12	200
			1220	13.2	211	4444	16	0	6	0
sent by the source o	or the		1206	13.2	212	135	4	0	0	0
doctination so the evolution	tnra	hably	1207	13.2	213	135	4	0	0	0
descination, so the exploi	ι μιυ	Dabiy	1209	13.2	215	135	4	õ	0	ŏ
did not succeed Full con	tent	data 📗	1210	13.2	216	135	4	0	0	0
			1211	13.2	217	135	4	0	0	0
reveals SYN - RST ACK S	Sessi	ons. 📋	1212	13.2	218	135	4	0	0	0
sepsor va 108/22//70 200/ 05 10 21/27/05 200/ 05 10	01-07-07 90	25 199 200	1213	13.2	219	135	4	0	0	0
-Selisui-va 1064224470 2004-03-10 21.27.03 2004-03-10	21.27.07 00	.35.183.200	1210	13.2		155		U	v	U I
Src IP: 80.35.189.200	Show I	Packet Data 🔳 S	Show F		w snort	ora	f.			
Src Name: 200.red-80-35-189.pooles.rima-tde.net	mea."NET		Sustan		w.anort.	org	w attempt	little en	dian" - fle	
Dst IP: .13.210		BIOS DEERFC I	System	IACIIVATOI	pantos	ento	wattempt			Jw.lo_selv
Dst Name: .13.210	10	Source IP		Dest IP	Ver	HL	TOS len	ID	Flags O	ffset TTL
📕 Reverse DNS Whois Query: 💸 None 🔶 Src IP 🐟 Dst IP	IP	80.35.189.200		.13.210	4	5	0 1420	41048	2 0	112
inetnum: 80.32.0.0 - 80.35.255.255			U A	APRSF						
netname: RIMA	тср	Source Dest R	RRO		Son		A ale #	0//001	Ree Win	dour Linn (C
descr: Provider Local Registry		1004 125			740215	#	AUK #	F		
country: ES	-	1204 135 .		<u>^ - - - -</u>	749315	447	320051377	5	0 1050	50 132 0
admin-c: AFG2-RIPE		90 06 00 03 10 0 90 06 00 00 01 0)0 00 0 00 04 0)0 A8 06 00)0 05 00 00	0 00 E5 6 00 01	00 00	00 00	 	 	
tech-c: FLT14-RIPE		00 00 00 00 32 2 74 20 96 D2 60 F	24 58 P 5F OD 0	D CC 45 64	4 49 BO	70 DD	AE2\$ OO t`∧	XEdI.p	·	
		70 5E 0D 00 02 0		00 7C 5E 00	0 00 00	00 00	00 p^			
System Messages User Messages	DATA	AF 6E 72 F4 0C 0	96 F1 F D0 00 0	-1 2H 4D C8 D0 4D 41 52	2 42 01	00 00	00 .nr	*№j MARB	·	
[2004-05-10 22:30:28] -sensor-fl: Database Next CID:		00 00 00 00 00 00 F 20 06 00 00 20 f	70 AD E 06 00 r	3A 00 00 00 00 4D 45 40	0 00 A8 F 57 04	F4 08	00		55 55	
3838. [2004.05.10.22:24:16] sensor va: /sport_data.97%		A2 01 00 00 00 0			0 00 00	00 00	46		. F	
									-	

A more complicated session data query tries to discover why these alerts appeared out of nowhere.

By querying for one of the target IPs, with session bytes > 0, and ignoring ports 80 and 443, we see exactly when the outside world began interacting with newly available ports on this target.

t ns.dst_	ip = INET_ATON('	.13.211')) and session	ns.dst_bytes > 0	and ses	sions.dst_port !=	80 and s	essions.	dst_port	!= 443	Submit
Ssn ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes
108421697	3 2004-05-10 19:22:52	2004-05-10 19:22:53	216.38.214.96	62061	.13.210	25	24	262	19	868
108421836	2 2004-05-10 19:45:01	2004-05-10 19:45:01	12.43.223.29	4452	.13.210	445	12	274	4	178
108422447	0 2004-05-10 21:27:04	2004-05-10 21:27:07	80.35.189.200	1204	.13.210	135	20	3552	10	120
108422483	6 2004-05-10 21:33:54	2004-05-10 21:33:56	62.101.72.124	28401	.13.210	135	15	3552	14	200
108422547	9 2004-05-10 21:44:30	2004-05-10 21:44:39	12.44.103.100	4212	.13.210	135	15	3392	14	280
108422574	5 2004-05-10 21:46:06	2004-05-10 21:48:20	81.91.226.43	21048	.13.210	139	14	516	14	8
108422690	4:2004-05-10 22:07:24	2004-05-10 22:07:24	12.37.252.76	2231	.13.210	445	12	274	4	178

Thanks again to session data, we can inform the client when a change was made to the access control at the client site.



Future Developments

- Snort rule and sensor management features
- Sguil 0.4.0 offers SANCP (www.metre.net) to replace Snort keepstats session logging
- Augment database output to include PostgreSQL and Oracle
- Test ability to scale
- Rewrite some components in compiled languages
- Live CD or install CDs to ease installation
- FreeBSD port



Questions?

• Thank you for your time.



