

Security Onion

Network Security Monitoring in Minutes

Doug Burks

Feel the pain

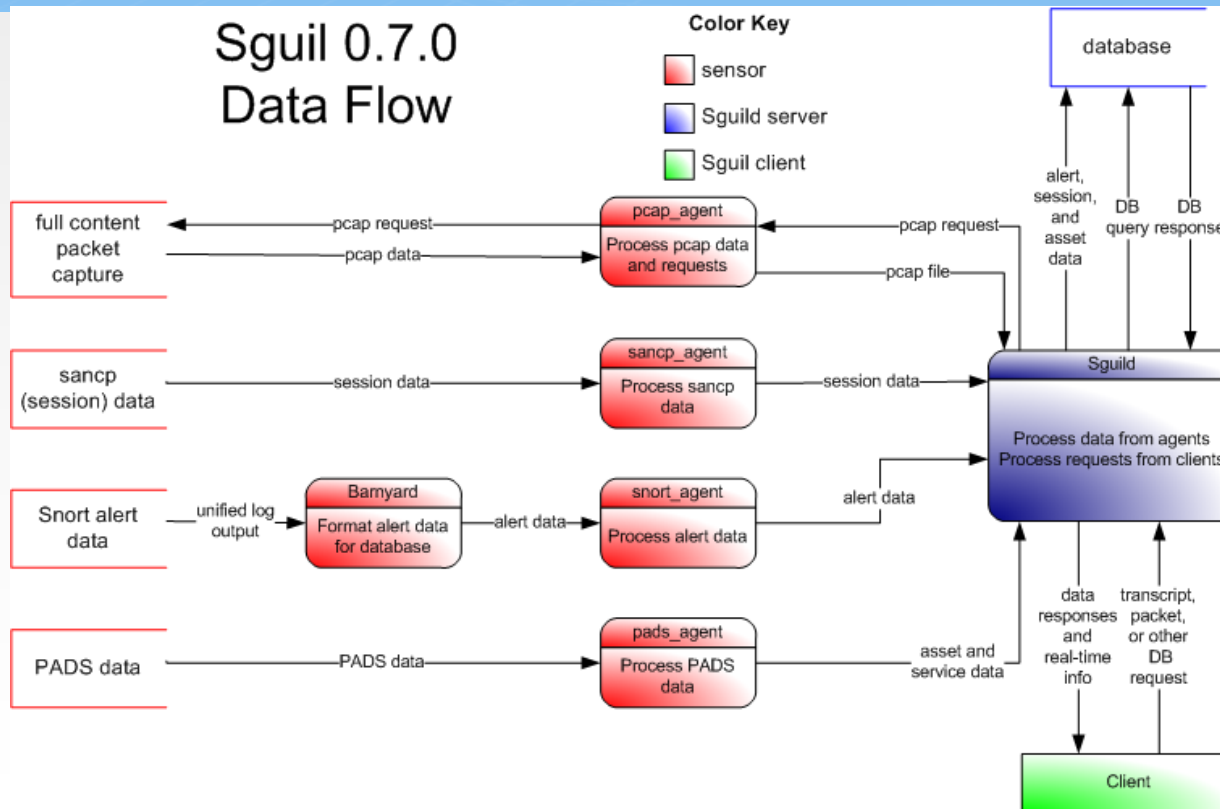
Does your traditional IDS give you all the data you need?



The Beauty of Network Security Monitoring

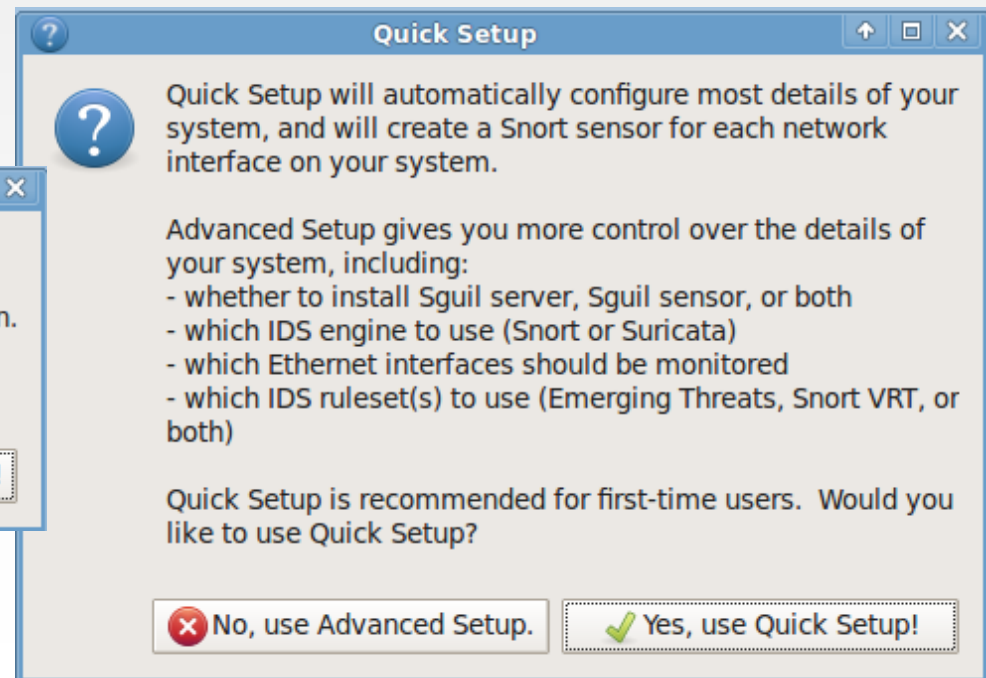
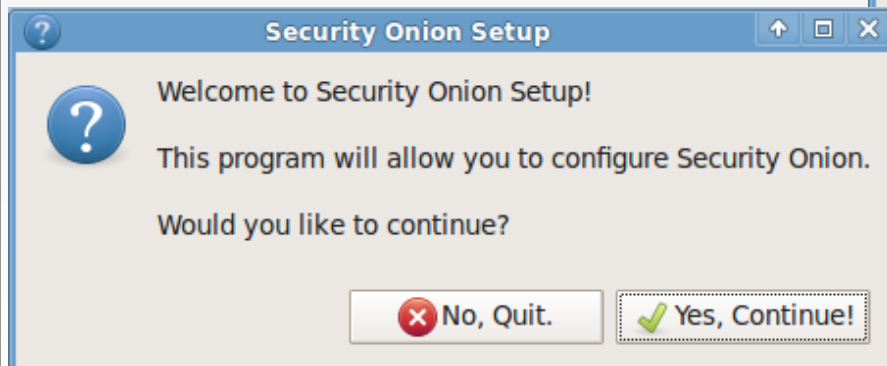
- Multiple data types (not just IDS alerts)
- Sguil is the de facto reference implementation of NSM:
 - Alert data (NIDS alerts from Snort/Suricata and HIDS alerts from OSSEC)
 - Session data (SANCP)
 - Transaction data (HTTP logs from Bro)
 - Full content data (daemonlogger)

Lots of pieces in the jigsaw puzzle



Setup wizard puts the jigsaw puzzle together for you!

Takes only 2 minutes!



Snorby

Web interface

- Web 2.0
- AJAX
- Ruby on Rails
- Buzzword compliant!



Squert web interface



Brief

Total Events

15370

Total Signatures

64

Total Sources

207

Total Destinations

232

Event Distribution by Sensor

Network	Hostname	Agent Type	Last Event	Sig	Src	Dst	Count
Toll	nacc-toll	snort	09:18:15	60	191	229	14549
Campus	dnabb-01	snort	09:18:07	8	40	3	821
OLL	oll-01	snort	-	0	0	0	0

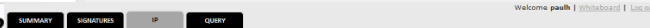
■ < 1 min ■ < 5 min ■ < 30 min

Event Distribution by Category

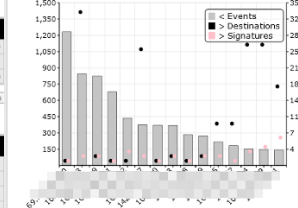
#	Category	Last Event	Sig	Src	Dst	Count
1	Unidentified	09:17:21	13	17	22	6431
2	Unauthorized Admin Access	-	0	0	0	0
3	Unauthorized User Access	-	0	0	0	0
4	Attempted Unauthorized Access	-	0	0	0	0
5	Denial of Service Attack	-	0	0	0	0
6	Policy Violation	09:15:53	28	100	160	2069
7	Reconnaissance	09:18:15	6	5	8	5794
8	Malware	09:17:46	15	110	64	1076
9	Escalated Event	-	0	0	0	0
10	Expired Event	-	0	0	0	0

Top Signatures

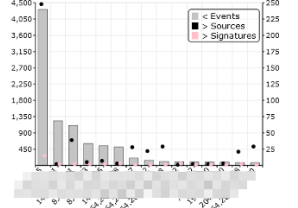
Signature	ID	Last Event	Src	Dst	Count
ssh- Protocol mismatch	4	09:17:21	2	5	6397
ET SCAN Potential SSH Scan	2001219	09:18:14	3	7	4088
INAPPROPRIATE Xhamster	2010111909	09:04:38	2	50	856
ET SCAN LKSSH Based SSH Connection - Often used as a BruteForce Tool	2006435	09:18:10	1	4	685
ET SCAN LKSSH Based Frequent SSH Connections Likely BruteForce Attack	2006546	09:18:15	1	4	684
MALWARE Blackhole Access (GET)	2011042801	09:13:49	38	1	472



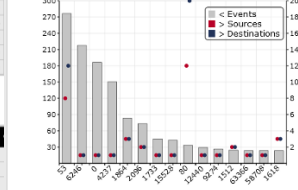
Top Source IPs



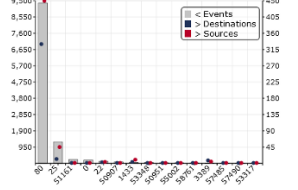
Top Destination IPs



Top Source Ports



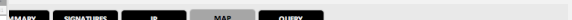
Top Destination Ports



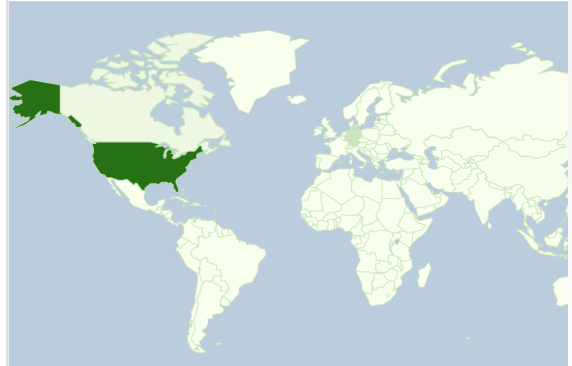
Top Source Countries



Top Destination Countries



Event Distribution by Country



SOURCE: 396 Events
DESTINATION: 376 Events
TOTAL: 772 Events, 10 Countries.

Country	Country Code	Source	Destination
UNITED STATES	US	307	196
INDIA	IN	0	111
GERMANY	DE	40	59
CANADA	CA	22	5
NETHERLANDS	NL	16	0
LATVIA	LV	4	4
CHINA	CN	4	0

The Ultimate Analyst Workstation

- Security Onion in a VM on your Desktop
- Sguil client connects to Sguil server
- Pull pcaps back to your VM for extended analysis

Sguil client designed by analysts for analysts

RT	1	BSidesATL-eth1	8.1	2011-11-03 21:12:56	210.114.220.46	653	192.168.1.102	111	17	GPL RPC portmap status request UDP
RT	1	BSidesATL-eth1	8.2	2011-11-03 21:12:56	210.114.220.46	654	192.168.1.102	919	17	GPL RPC STATD UDP stat mon_name format string expl...
RT	2	BSidesATL-eth1	8.3	2011-11-03 21:12:56	192.168.1.102	23	217.156.93.166	61200	6	GPL TELNET Bad Login
RT	1	BSidesATL-eth1	8.5	2011-11-03 21:12:56	192.168.1.102	21	207.35.251.172	2243	6	ET POLICY FTP Login Successful (non-anonymous)
RT	37	BSidesATL-eth1	8.6	2011-11-03 21:12:56	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE EXEC attempt
RT	36	BSidesATL-eth1	8.7	2011-11-03 21:12:56	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE overflow attempt
RT	1	BSidesATL-eth1	8.79	2011-11-03 21:12:56	192.168.1.102	21	207.35.251.172	2243	6	GPL ATTACK_RESPONSE id check returned root
RT	1	BSidesATL-eth1	8.80	2011-11-03 21:12:56	192.168.1.102	23	217.156.93.166	61216	6	ET MALWARE Suspicious FTP 220 Banner on Local Port...
RT	4	BSidesATL-eth1	8.81	2011-11-03 21:12:56	207.35.251.172	4031	192.168.1.102	5920	6	ET SCAN Potential VNC Scan 5900-5920
RT	4	BSidesATL-eth1	8.82	2011-11-03 21:12:56	207.35.251.172	4981	192.168.1.102	5807	6	ET SCAN Potential VNC Scan 5800-5820
RT	1	BSidesATL-eth1	8.84	2011-11-03 21:12:57	207.35.251.172	2850	192.168.1.102	5432	6	ET POLICY Suspicious inbound to PostgreSQL port 5432
RT	1	BSidesATL-eth1	8.86	2011-11-03 21:12:57	207.35.251.172	3931	192.168.1.102	161	6	GPL SNMP request tcp
RT	1	BSidesATL-eth1	8.88	2011-11-03 21:12:57	207.35.251.172	2437	192.168.1.102	162	6	GPL SNMP trap tcp
RT	4	BSidesATL-eth1	8.89	2011-11-03 21:12:57	207.35.251.172	3066	192.168.1.102	1521	6	ET POLICY Suspicious inbound to Oracle SQL port 1521
RT	1	BSidesATL-eth1	8.93	2011-11-03 21:12:57	207.35.251.172	4024	192.168.1.102	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433

IP Resolution
Agent Status
Snort Statistics
System Msgs
User Msgs

☐ Reverse DNS ☒ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: None Src IP Dst IP

☒ Show Packet Data ☒ Show Rule

alert tcp \$EXTERNAL_NET any -> \$HOME_NET 21 (msg:"GPL FTP SITE overflow attempt"; flow:to_server,established; content:"SITE"; nocase; isdataat:100,relative; pcre:"/^SITE\s{^n}{100}/smi";

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	207.35.251.172	192.168.1.102	4	5	0	468	16651	2	0	48	31546

TCP	U A P R S F										Seq #	Ack #	Offset	Res	Window	Urp	ChkSum	
	Source Port	Dest Port	R 1	A 0	P G	U K	R H	S T	F N	N								
	2243	21	X	X	.	.	.	3480775140	3956113150	8	0	32120	0	55423

Right-click Src/Dst IP and Query SANCP table (Session Data)

SGUIL-0.8.0 - Connected To localhost												
File Query Reports Sound: Off ServerName: localhost UserName: doug UserID: 2 2011-11-06 14:40:56 GMT												
RealTime Events Escalated Events Sancp Query 6												
Close	(SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port, INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX (p_key) INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2011-11-05' AND sancp.src_ip =											Submit
Export	INDEX (p_key) INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2011-11-05' AND sancp.src_ip =											Edit
Se...	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	3	207.35.251.172	1445	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	6	207.35.251.172	1281	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:31	192.168.1.102	21	207.35.251.172	2243	6	181	86197	186	14433
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	28	207.35.251.172	2882	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	38	207.35.251.172	2731	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	54	207.35.251.172	1256	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	78	207.35.251.172	1586	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	90	207.35.251.172	2733	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	97	207.35.251.172	2491	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	100	207.35.251.172	2730	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	104	207.35.251.172	1834	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	122	207.35.251.172	3028	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	139	207.35.251.172	2159	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	170	207.35.251.172	1807	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	172	207.35.251.172	2163	6	1	0	0	0

Right-click Src/Dst IP and query Event table to access HTTP logs (Transaction Data)

RealTime Events

Escalated Events

Event Query 1

Event Query 2

Close

Export

(SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event_p_key, sid_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE (event.src_ip=INET_ATON('172.16.116.251')) UNION (SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event_p_key, sid_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE (event.dst_ip=INET_ATON('74.125.65.132'))))

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	qa-eth0	4.48	2011-09-23 13:38:34	172.16.116.251	59352	74.125.65.132	80	6	ET POLICY curl User-Agent Outbound
NA	1	qa-eth0	11.27	2011-09-23 13:38:34	172.16.116.251	59352	74.125.65.132	80	6	URL securityunion.blogspot.com
RT	1	qa-eth0	4.49	2011-09-23 13:38:35	172.16.116.251	38255	74.125.47.132	80	6	ET POLICY curl User-Agent Outbound
NA	1	qa-eth0	11.28	2011-09-23 13:38:35	172.16.116.251	38255	74.125.47.132	80	6	URL securityunion.blogspot.com

NA

1

qa-eth0

11.29

2011-09-23 13:38:35

172.16.116.251

38256

74.125.47.132

80

6

URL securityunion.blogspot.com

IP Resolution

Agent Status

Snort Statistics

System Msgs

Sid

Net

Hostname

Type

Last

☒ Display Detail

GET || securityunion.blogspot.com/ || - || curl/7.19.7 (i486-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15

Right-click Alert ID to pivot to Full Content (transcript in Sguil or pcap in Wireshark)

demo-master-eth0_2

File

Sensor Name: Demo-Master-eth0
Timestamp: 2011-11-06 14:43:22
Connection ID: .demo-master-eth0_2
Src IP: 172.16.116.142 (Unknown)
Dst IP: 217.160.51.31 (s193738556.websitehome.co.uk)
Src Port: 42994
Dst Port: 80
OS Fingerprint: 172.16.116.142:42994 - Linux 2.6 (newer, 2) (up: 2 hrs)
OS Fingerprint: -> 217.160.51.31:80 (distance 0, link: ethernet/modem)

SRC: GET / HTTP/1.1
SRC: User-Agent: curl/7.19.7 (486-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15
SRC: Host: testmyids.com
SRC: Accept: /*
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Sun, 06 Nov 2011 14:43:22 GMT
DST: Server: Apache
DST: Last-Modified: Mon, 15 Jan 2007 23:11:55 GMT
DST: ETag: "61c22f22-27-4271c5f1ac4c0"
DST: Accept-Ranges: bytes
DST: Content-Length: 39
DST: Content-Type: text/html
DST:
DST: uid=0(root) gid=0(root) groups=0(root)
DST:

Search Abort Close

Debug Messages

/tmp/172.16.116.142:42994_217.160.51.31:80-6.raw host 217.160.51.31 and host 172.16.116.142 and port 80 and port 42994 and proto 6
Receiving raw file from sensor.
Finished.

172.16.116.142:42994_217.160.51.31:80-6.raw - Wireshark (on Demo-Master)

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.116.142	217.160.51.31	TCP	42994 > 80 [SYN] Seq=0 Win=0
2	0.146918	217.160.51.31	172.16.116.142	TCP	80 > 42994 [SYN, ACK] Seq=1
3	0.146969	172.16.116.142	217.160.51.31	TCP	42994 > 80 [ACK] Seq=1 Ack=1
4	0.147201	172.16.116.142	217.160.51.31	HTTP	GET / HTTP/1.1
5	0.147384	217.160.51.31	172.16.116.142	TCP	80 > 42994 [ACK] Seq=1 Ack=1
6	0.323696	217.160.51.31	172.16.116.142	HTTP	HTTP/1.1 200 OK (text/html)
7	0.323775	172.16.116.142	217.160.51.31	TCP	42994 > 80 [ACK] Seq=153 Ack=1
8	0.323989	172.16.116.142	217.160.51.31	TCP	42994 > 80 [FIN, ACK] Seq=153 Ack=1
9	0.324344	217.160.51.31	172.16.116.142	TCP	80 > 42994 [ACK] Seq=260 Ack=153
10	0.475925	217.160.51.31	172.16.116.142	TCP	80 > 42994 [FIN, PSH, ACK] Seq=260 Ack=153
11	0.476032	172.16.116.142	217.160.51.31	TCP	42994 > 80 [ACK] Seq=154 Ack=153

Frame 1 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: 00:0c:29:e1:43:1e (00:0c:29:e1:43:1e), Dst: 00:50:56:fc:6f:0c (00:50:56:fc:6f:0c)

Internet Protocol, Src: 172.16.116.142 (172.16.116.142), Dst: 217.160.51.31 (217.160.51.31)

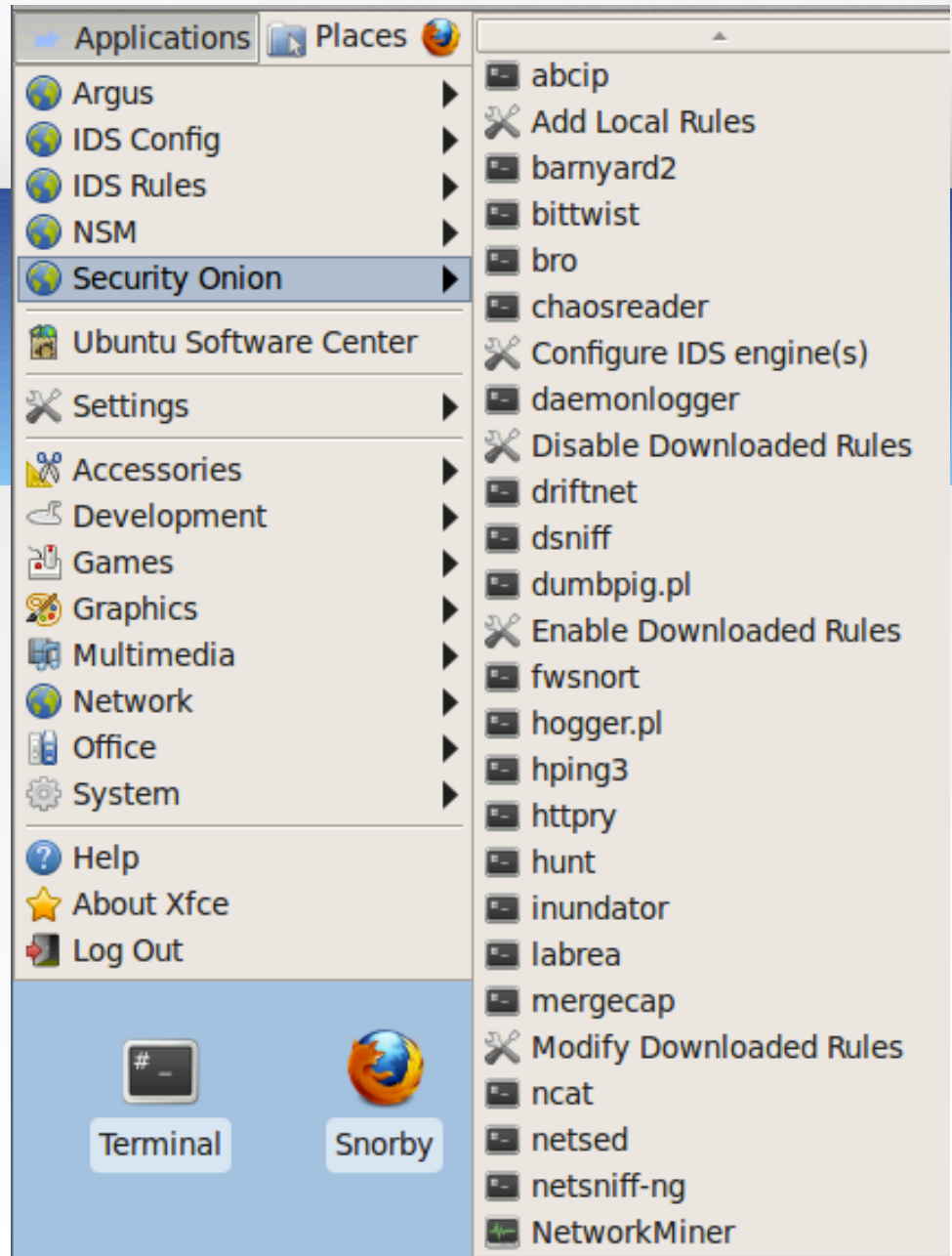
Transmission Control Protocol, Src Port: 42994 (42994), Dst Port: 80 (80), Seq: 0, Len: 0

0000 00 50 56 fc 6f 0c 00 0c 29 e1 43 1e 08 00 45 00 .PV.o...).C...E.
0010 00 3c 9d 7a 40 00 40 06 6f e3 ac 10 74 8e d9 a0 .<.z@.@. o...t...
0020 33 1f a7 f2 00 50 ac 41 99 25 00 00 00 a0 02 3...P.A .%.....
0030 16 d0 11 bd 00 00 02 04 05 b4 04 02 08 0a 00 0d
0040 04 5f 00 00 00 01 03 03 06

File: "/tmp/172.16.116.142:42994_217.160.51.31:80-6.raw" Packets: 11 Displayed: 11 Marked: 0 Profile: Default

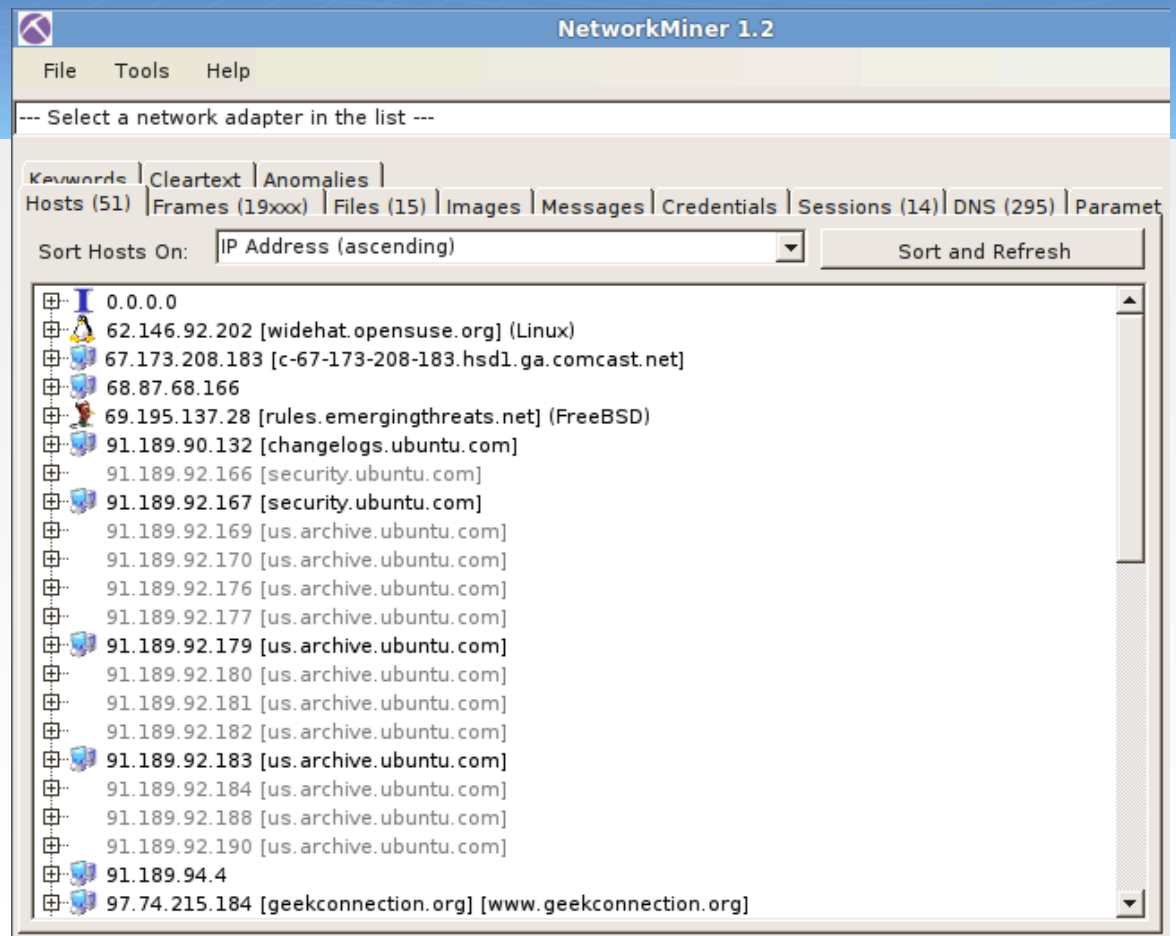
PCAP Tools

We haz them

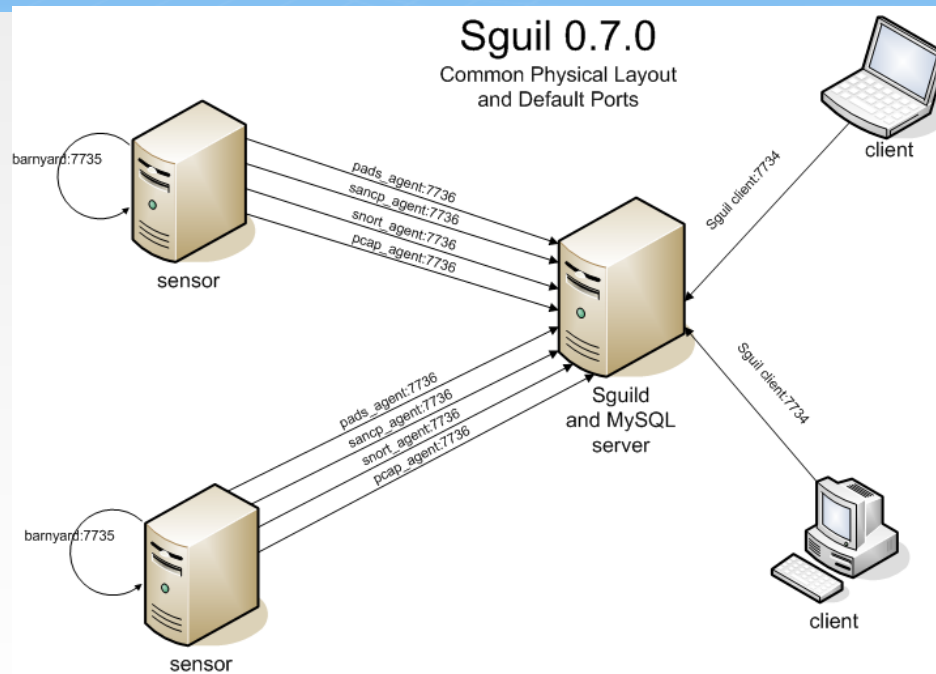


NetworkMiner

There's gold in them
thar PCAPs!



Multiple Sguil sensors



<http://securityonion.blogspot.com/2011/04/security-onion-20110321-distributed.html>

Bro IDS



Bro records a tremendous amount of actionable intelligence about your network traffic. The logs can be found in:
`/nsm/bro/logs`

Hunt for Evil User Agents

```
zcat /nsm/bro/logs/*/http* | bro-cut -d user_agent | sort | uniq -c | sort -nr
```

Look for malicious user agents like:
Bob's Evil Clown C&C Agent

or just outdated and vulnerable software like:

```
zcat /nsm/bro/logs/*/soft* | bro-cut -d name version.major | grep  
Firefox | grep -v 12 | sort | uniq -c | sort -nr
```

```
110 Firefox 3  
71 Firefox 11  
53 Firefox 10
```

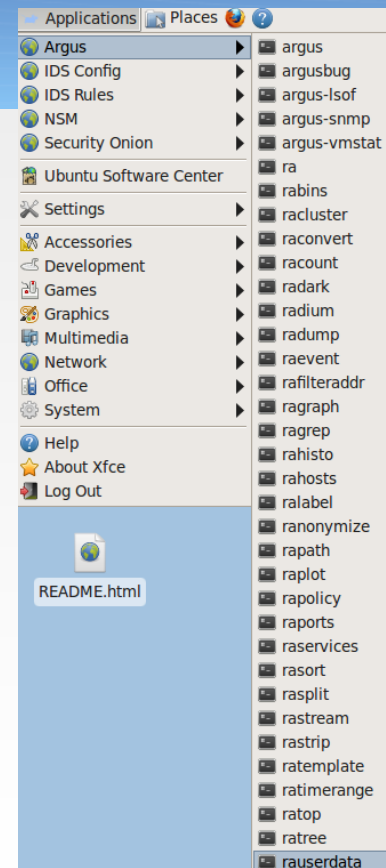
<http://pauldotcom.com/2011/10/in-search-of-evil-user-agents.html>



Argus

```
qa@qa:~$ ranonymize -nr /nsm/sensor_data/*/*argus/*
```

StartTime	Flgs	Proto	SrcAddr	Sport	Dir	DstAddr	Dport	TotPkts	TotBytes	State
15:04:54.445668	e	arp	100.0.1.1		who	100.0.1.2		2	120	CON
15:04:54.791205	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		8	1148	CON
15:04:57.573828	e	udp	fe80::571:1aa8:dc*.546		->	ff02::1:2.547		1	157	INT
15:05:10.079722	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		4	846	CON
15:05:25.080525	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		4	846	CON
15:05:29.574452	e	udp	fe80::571:1aa8:dc*.546		->	ff02::1:2.547		1	157	INT
15:05:33.528292	e	udp	100.0.1.4.123		<->	1.0.2.1.123		2	180	CON
15:05:34.742335	e	tcp	100.0.1.1.6128		<?>	1.0.3.1.80		2	120	CON
15:05:34.914207	e	tcp	100.0.1.1.6129		<?>	1.0.4.1.80		2	120	CON
15:05:38.525547	e	arp	100.0.1.4		who	100.0.1.2		2	182	CON
15:05:39.446526	e	arp	100.0.1.1		who	100.0.1.2		2	120	CON
15:05:40.081400	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		4	846	CON
15:05:42.681708	e	udp	100.0.1.3.123		<->	1.0.2.1.123		2	180	CON
15:05:54.793109	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		8	1148	CON
15:06:04.522112	M	udp	1.0.1.0.68		->	197.0.2.255.67		4	1368	INT
15:06:04.522136	M	icmp	100.0.1.5.8		<->	100.0.1.6.59545		3	186	ECO
15:06:04.522155	M	arp	100.0.1.2		who	100.0.1.6		4	240	CON
15:06:05.522702	e	udp	100.0.1.5.67		->	100.0.1.6.68		2	684	INT
15:06:05.598642	M	icmp	100.0.1.5.8		<->	100.0.1.7.59753		3	186	ECO
15:06:05.598647	M	arp	100.0.1.2		who	100.0.1.7		4	240	CON
15:06:06.522867	e	udp	100.0.1.5.67		->	100.0.1.7.68		2	684	INT
15:06:06.525262	M	arp	100.0.1.6		who	100.0.1.5		2	120	CON
15:06:07.605045	M	arp	100.0.1.7		who	100.0.1.5		2	120	CON
15:06:10.085867	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		4	846	CON
15:06:19.744501	e s	tcp	100.0.1.1.6128		<?>	1.0.3.1.80		2	120	CON
15:06:19.744510	M	arp	100.0.1.2		who	100.0.1.1		2	120	CON
15:06:19.916238	e s	tcp	100.0.1.1.6129		<?>	1.0.4.1.80		2	120	CON
15:06:24.447087	e	arp	100.0.1.1		who	100.0.1.2		2	120	CON
15:06:25.089063	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		4	846	CON
15:06:36.499030	M	udp	100.0.1.4.123		<->	1.0.2.1.123		2	180	CON
15:06:36.599050	M	arp	100.0.1.2		who	100.0.1.4		2	120	CON
15:06:40.090335	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		4	846	CON
15:06:47.684557	e	udp	100.0.1.3.123		<->	1.0.2.1.123		2	180	CON
15:06:54.797327	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		8	1148	CON
15:07:04.760789	e s	tcp	100.0.1.1.6128		<?>	1.0.3.1.80		2	120	CON
15:07:04.917348	e s	tcp	100.0.1.1.6129		<?>	1.0.4.1.80		2	120	CON
15:07:09.447942	e	arp	100.0.1.1		who	100.0.1.2		2	120	CON
15:07:10.096641	e	tcp	100.0.1.3.9247		<?>	197.0.1.1.21627		4	846	CON
15:07:10.096652	M	arp	100.0.1.2		who	100.0.1.3		2	120	CON
15:07:19.728097	e	tcp	100.0.1.1.6128		<?>	1.0.3.1.80		2	120	FIN



NIDS is great, but what about HIDS?

- OSSEC monitors local logs and can receive logs from OSSEC Agents and standard Syslog
- OSSEC alerts are stored in `/var/ossec/logs/alerts/`
- Sguil OSSEC Agent transmits those alerts to the Sguil server

One-man bands make crappy music

Interested in joining an open source project?

Security Onion needs:

- Documentation
- Artwork
- Web interface
- Performance benchmarks
- Package maintainers

<http://code.google.com/p/security-onion/wiki/TeamMembers>

Where do we go now?

<http://securityonion.blogspot.com>

Updates are announced here and it also has the following links:

- Download/Install
- FAQ
- Mailing List
- IRC #securityonion on irc.freenode.net