Security Onion

Network Security Monitoring in Minutes

Doug Burks

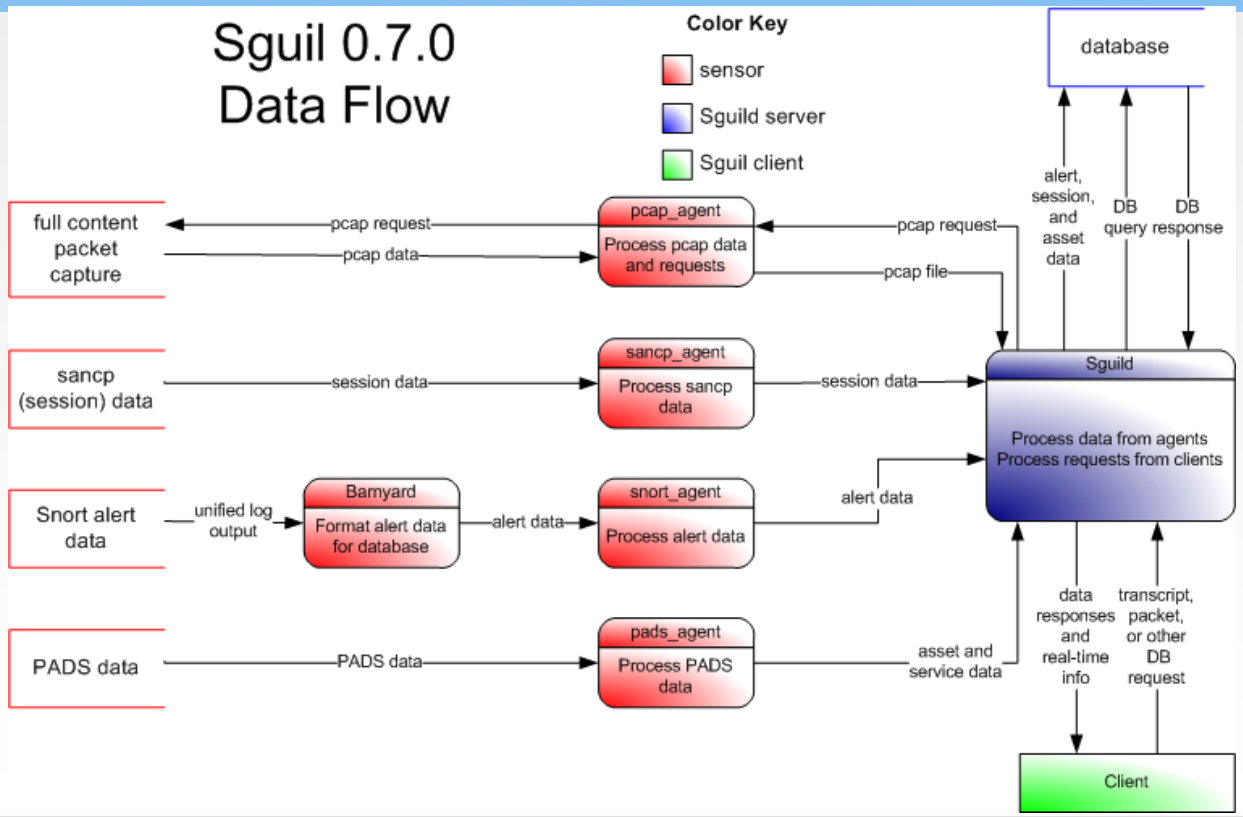
Feel the pain

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)

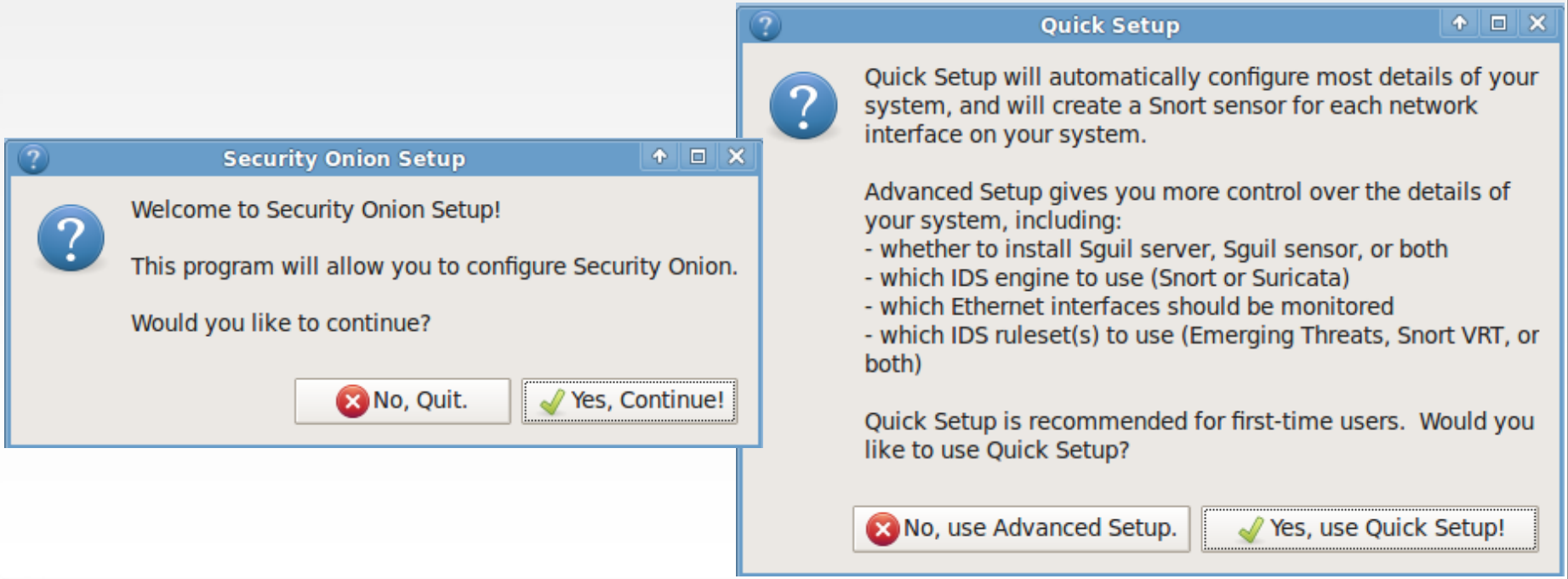
Lots of pieces in the jigsaw puzzle



http://nsmwiki.org/images/e/ea/Sguil-0.7.dfd.png

Setup wizard puts the jigsaw puzzle together for you!

Takes only 2 minutes!

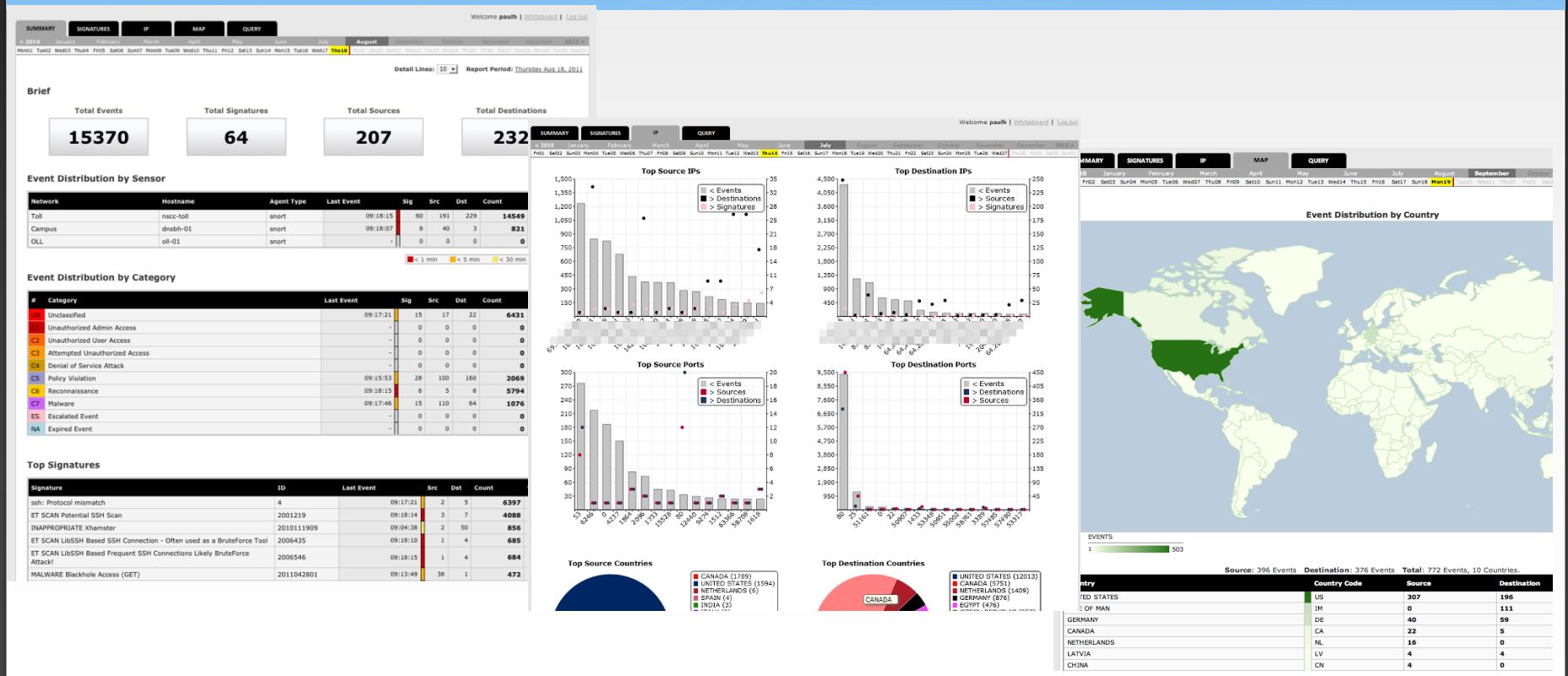


Snorby

Web interface

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

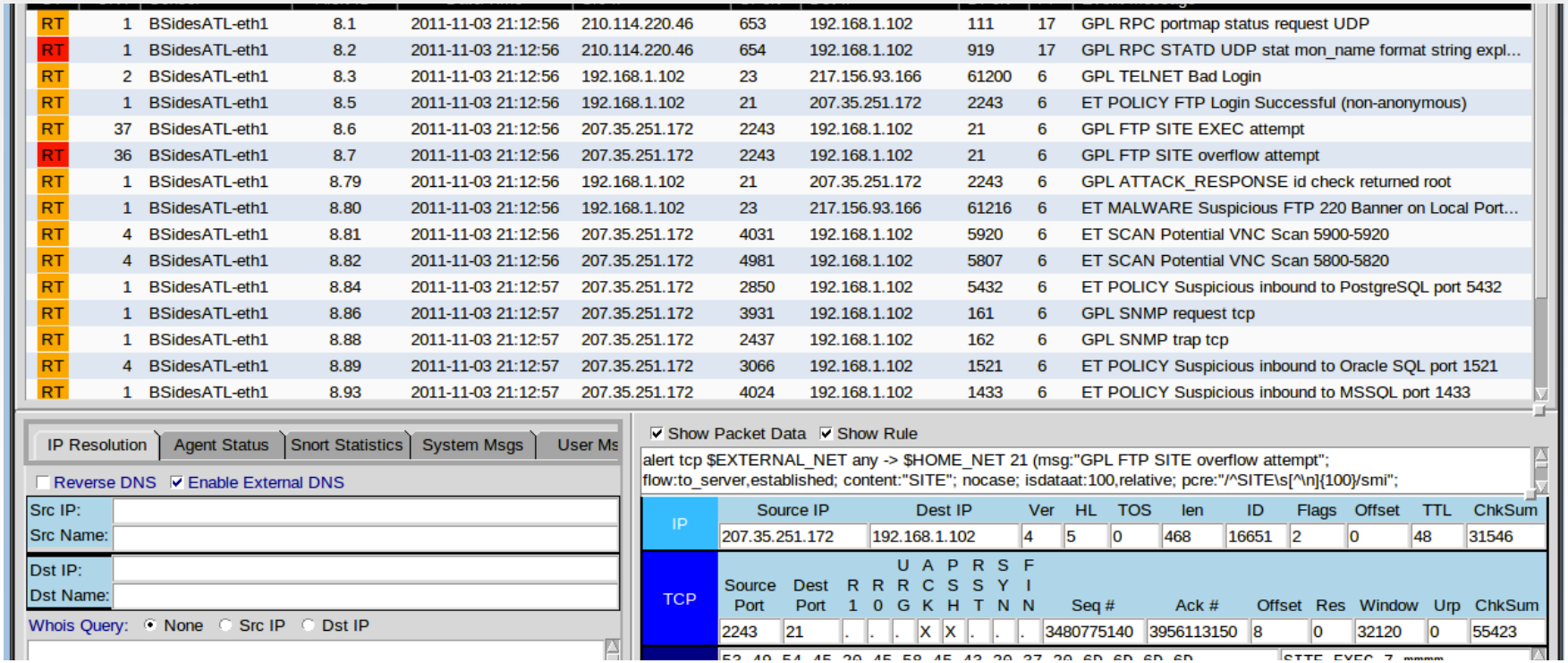
Squert web interface



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 Ms

Reverse DNS | Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: None | Src IP | Dst IP

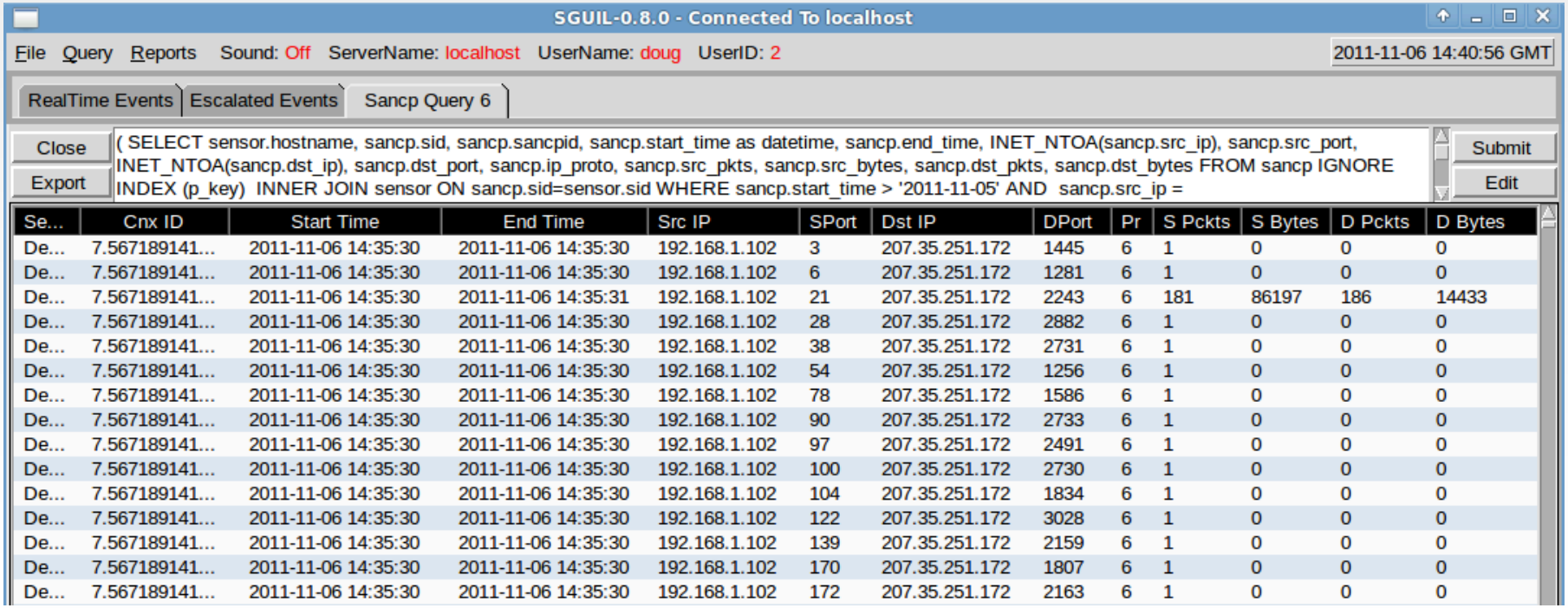
Show Packet Data | Show Rule

```
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";
```

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

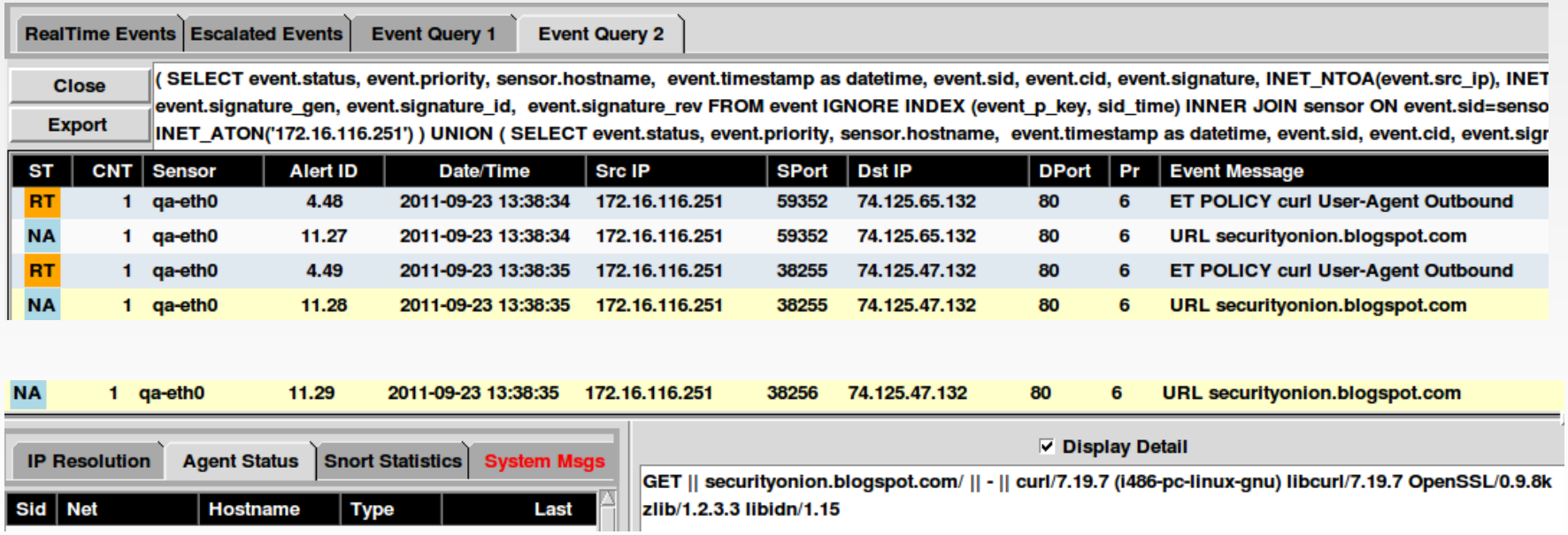
	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	2243	21	.	.	.	X	X	.	.	.	3480775140	3956113150	8	0	32120	0	55423

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

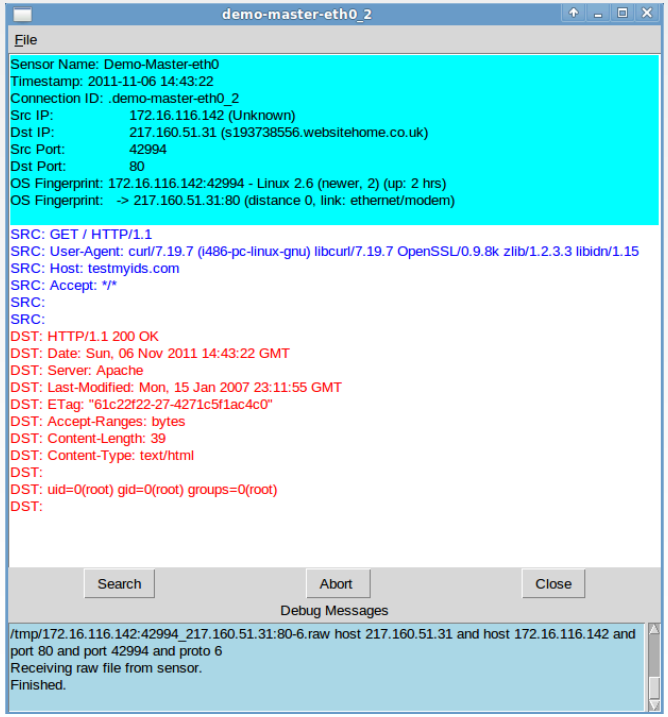


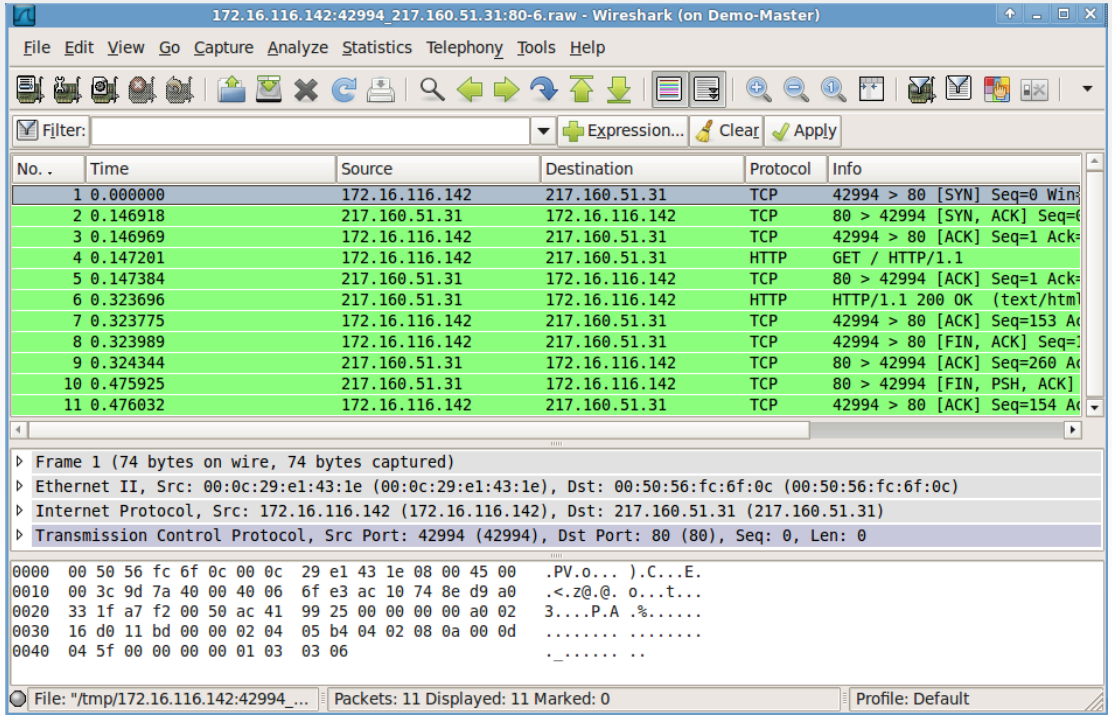
Se...	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	3	207.35.251.172	1445	6	1	0	0	0
De...	7.567189141...	2011-11-06 14:35:30	2011-11-06 14:35:30	192.168.1.102	6	207.35.251.172	1281	6	1	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)



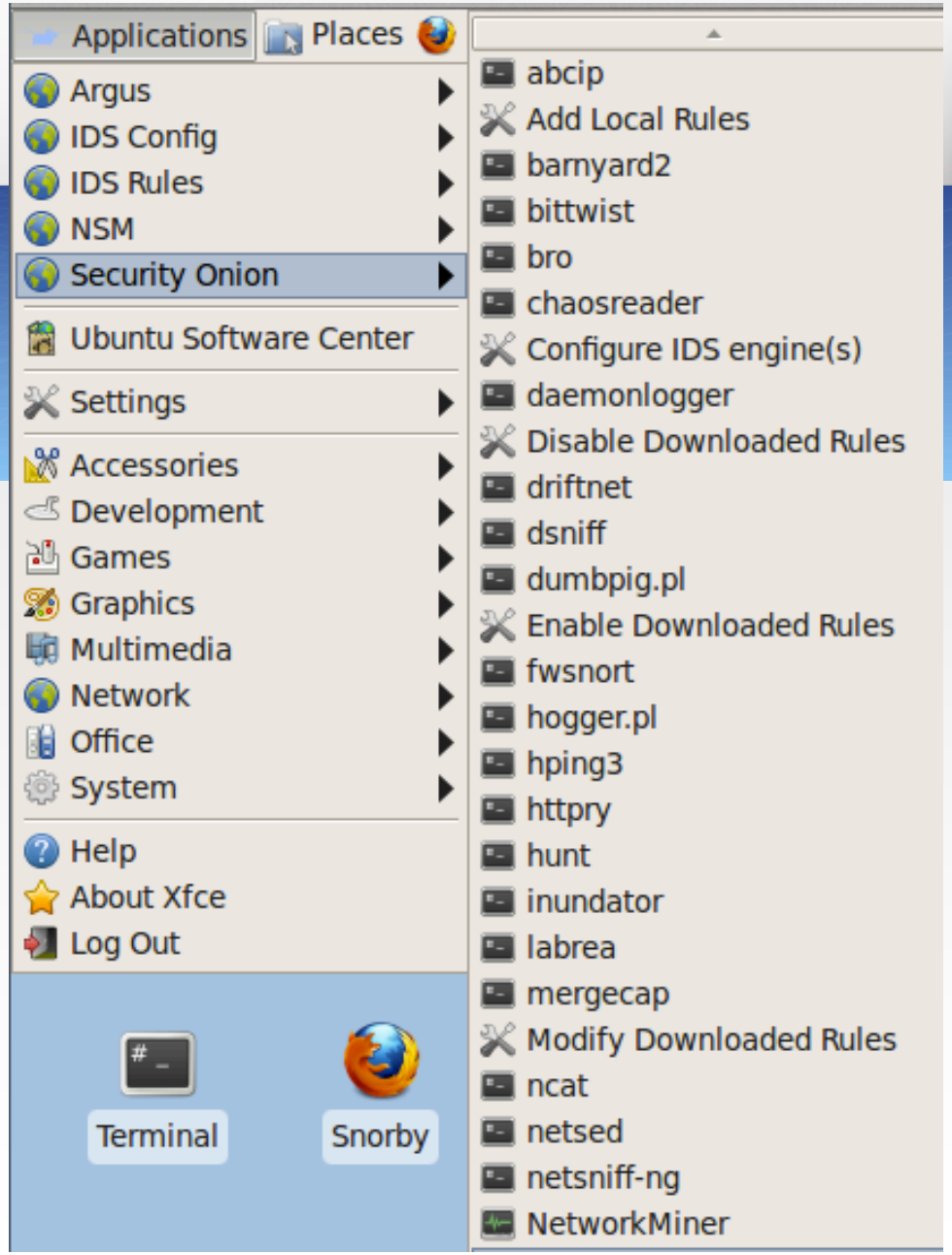
Right-click Alert ID to pivot to Full Content (transcript in Sguil or pcap in Wireshark)





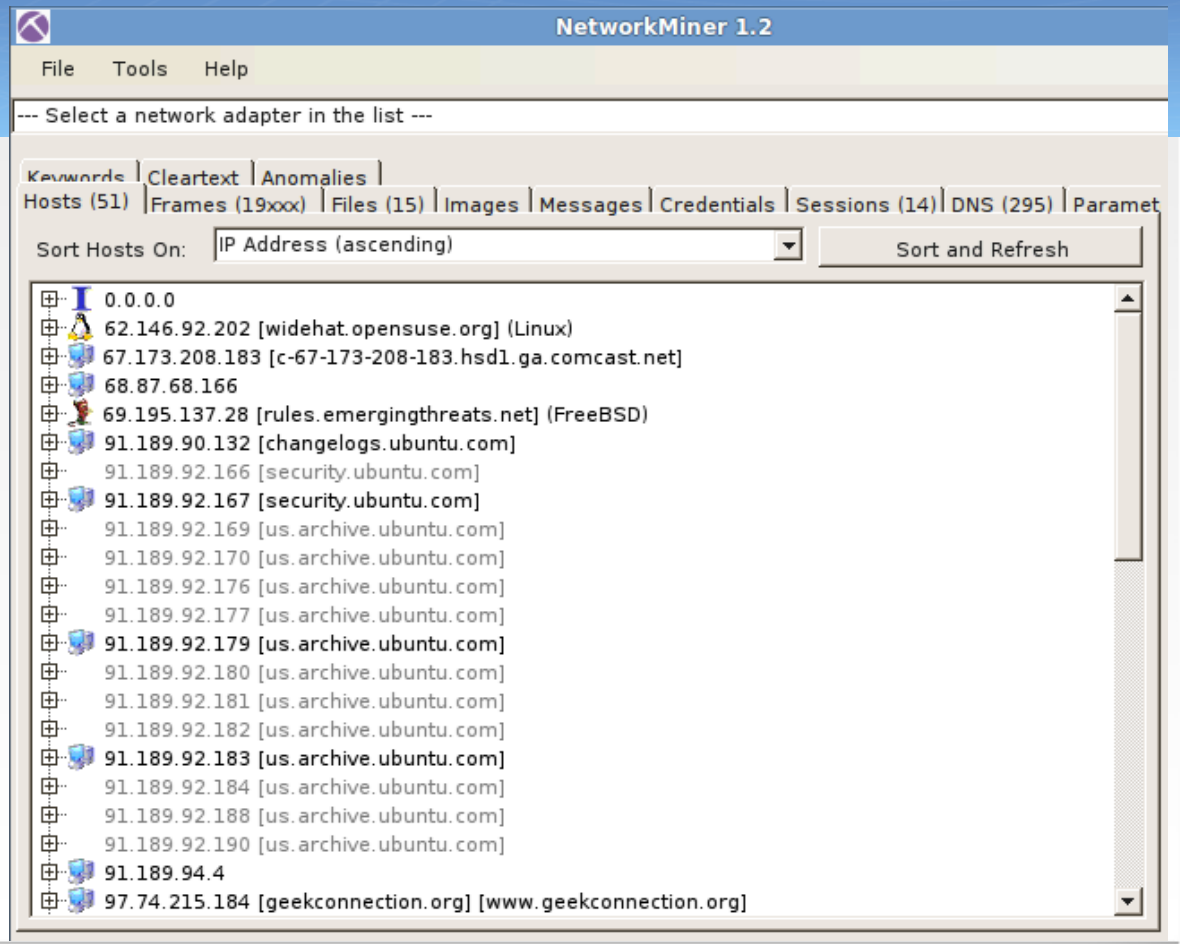
PCAP Tools

We haz them

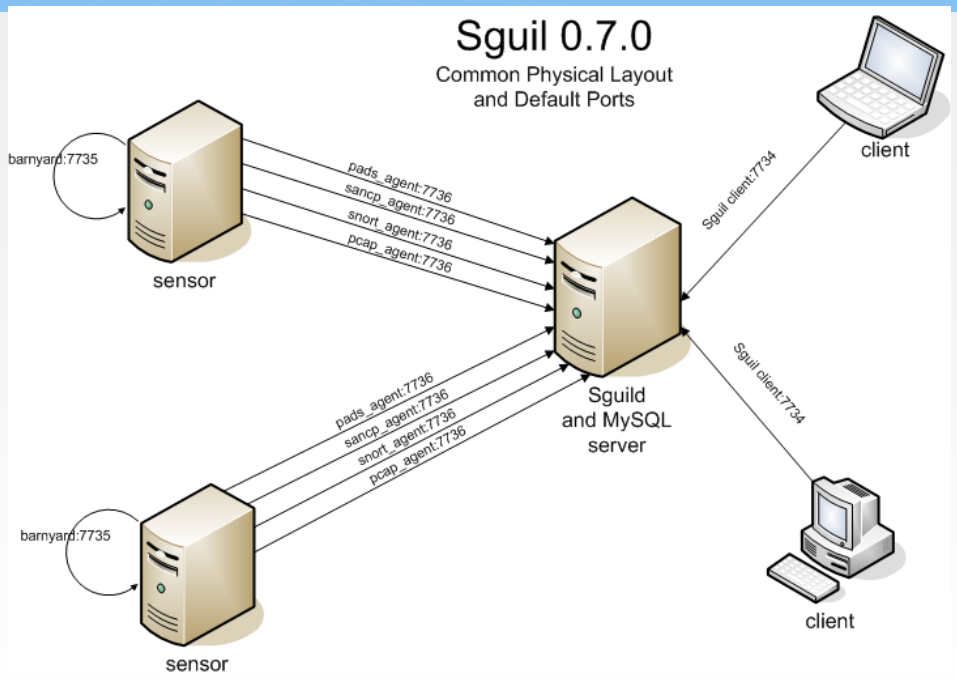


NetworkMiner

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

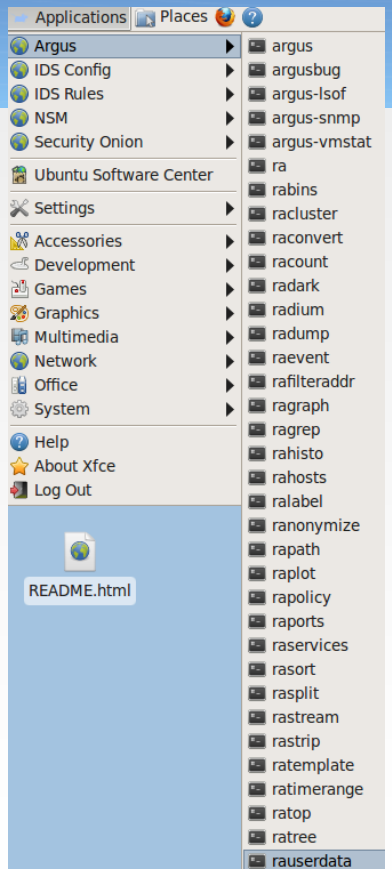
or just outdated and vulnerable software like:
zcat /nsm/bro/logs/*/soft* |bro-cut -d name version.major |grep Firefox |grep -v 12 |sort |uniq -c |sort –nr

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        102   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