



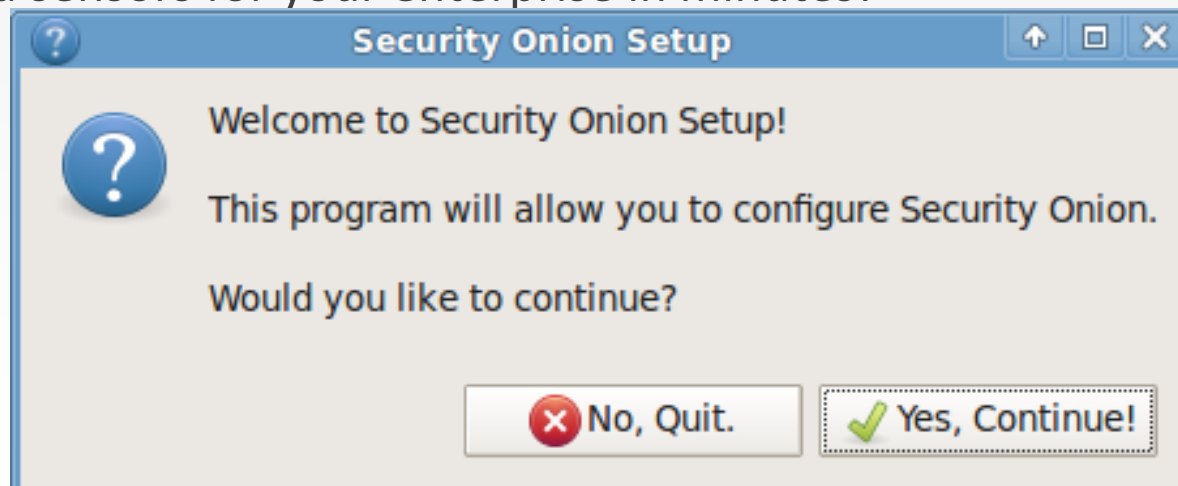
# Security@onion

Peel Back the Layers of Your Network in Minutes

Doug Burks

# What is Security Onion?

Security Onion is a Linux distro for IDS (Intrusion Detection) and NSM (Network Security Monitoring). It's based on Ubuntu and contains Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!



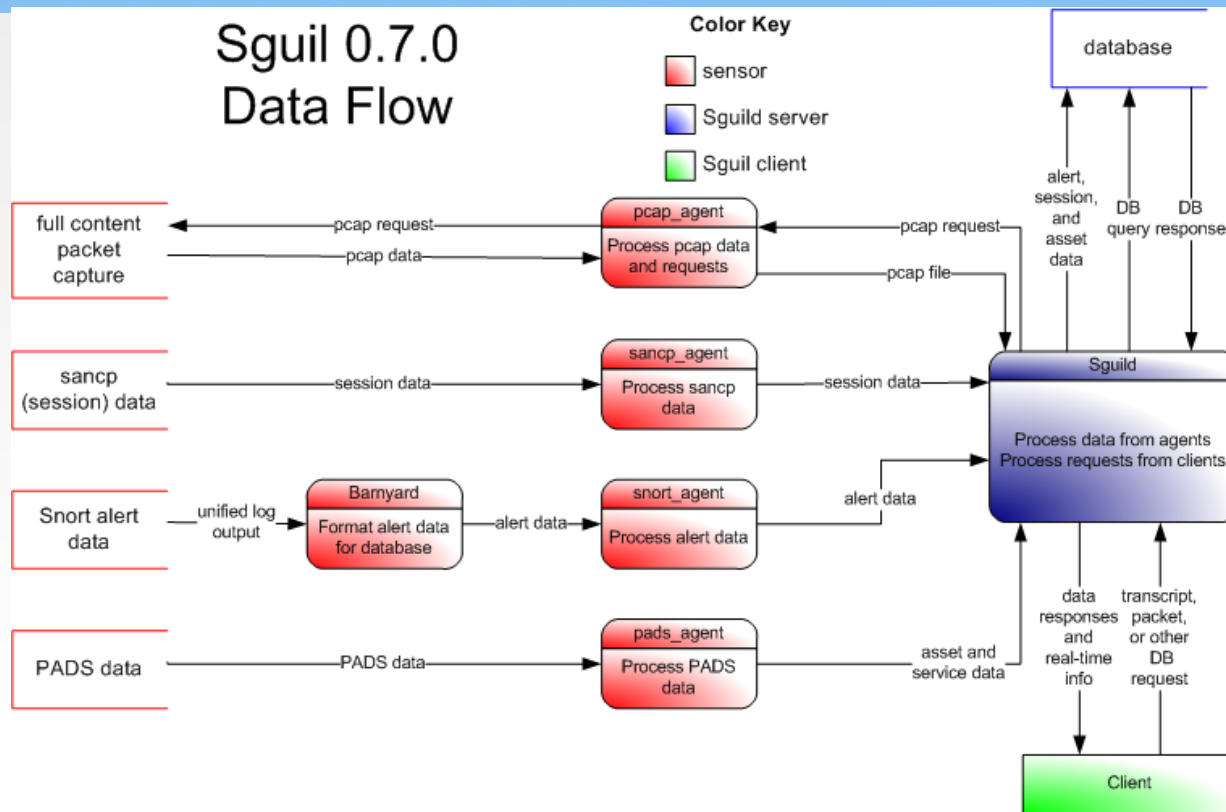
IDS is sub-optimal; need NSM (multiple data types)

S  
Network  
C  
H  
I  
Monitoring  
Y

Sguil is the defacto reference  
implementation of NSM



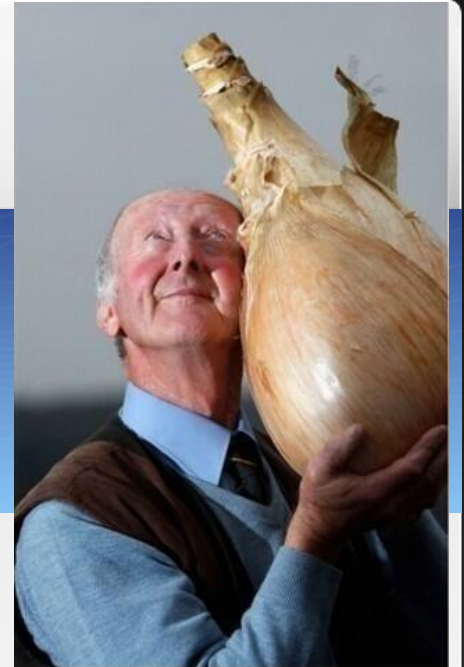
# Lots of pieces in the Sguil jigsaw puzzle





# Big Onions

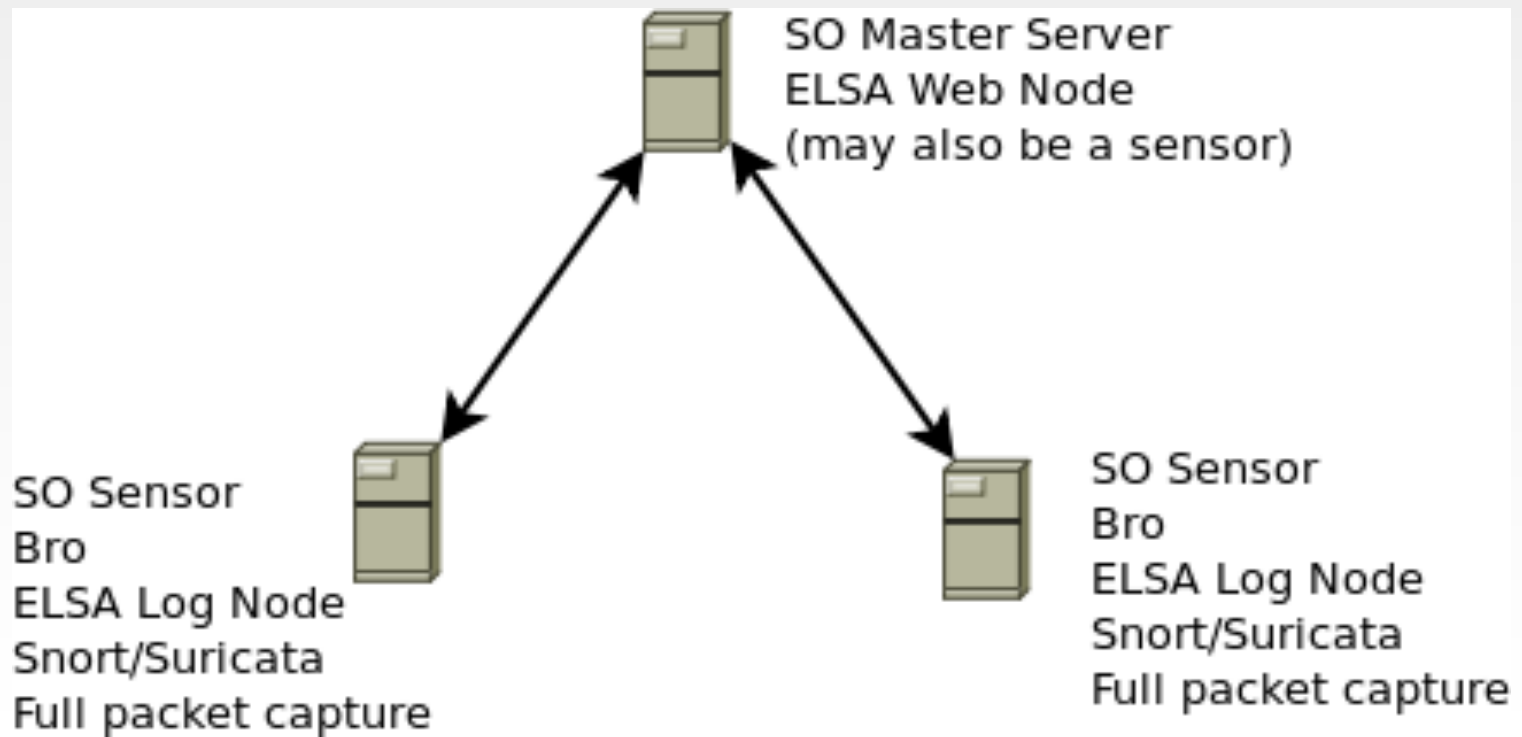
- Use our ISO image (based on Xubuntu 12.04 **64-bit**)  
OR  
Start with your preferred flavor of Ubuntu 12.04 (Ubuntu, Kubuntu, Lubuntu, Xubuntu, or **Ubuntu Server**) 32-bit or **64-bit**, add our PPA and install our packages
- High performance:
  - Snort/Suricata/Bro running on **PF\_RING**
  - Netsniff-ng uses **zero-copy** for high-speed full-packet capture
- ELSA (like a free version of Splunk) – **distributed** database with central web interface



# Data Types

- Alert data
  - NIDS alerts from Snort/Suricata
  - HIDS alerts from OSSEC
- Asset data from Bro and PRADS
- Session data from Argus, Bro, and PRADS
- Transaction data – http/ftp/dns/ssl/other logs from Bro
- Full content data from netsniff-ng

# Distributed Deployment



# Snorby

Snorby "All About Simplicity"

Welcome Dustin Webber | [Settings](#) | [Log out](#)

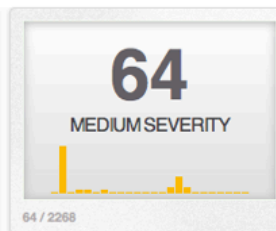
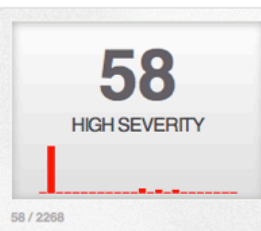
Dashboard My Queue (8) Events Sensors Search Administration

## Dashboard

More Options

TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR

Last Updated: 11/28/10 5:00:00 PM



### TOP 5 SENSOR

Snorby.org	3120
Home Sensor	494

### TOP 5 ACTIVE USERS

Dustin Webber	8
Administrator	0

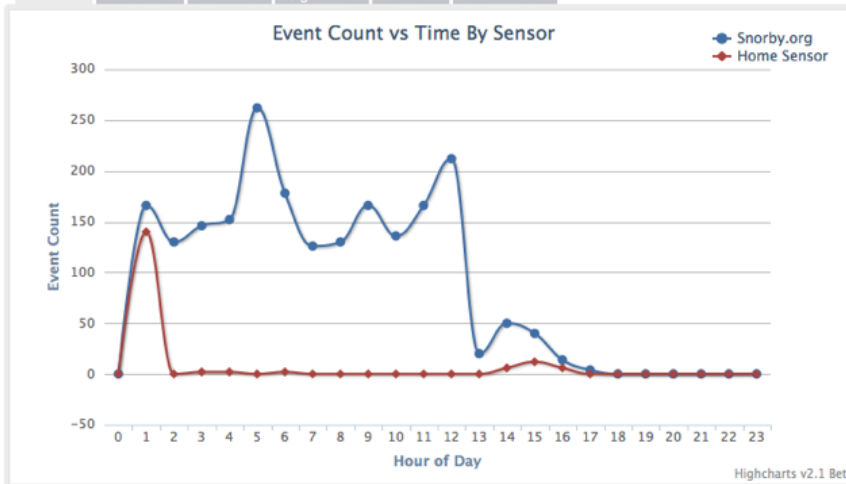
### LAST 5 UNIQUE EVENTS

(http_inspect) CHUNK S...	2
Bad segment, adjusted ...	8
(http_inspect) OVERSIZ...	2
ET WORM Potential MySQ...	4
TCP Timestamp is outsi...	6

### ANALYST CLASSIFIED EVENTS

False Positive	418
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0

Sensors Severities Protocols Signatures Sources Destinations



# Pivot to pcap from Snorby

The screenshot displays the Snorby web interface. At the top, the header reads "Snorby 'All About Simplicity'" and "welcome Administrator". Below the header is a navigation menu with "Administration" selected. The main content area shows a table of events with columns for "Sev.", "Sensor", "Source IP", "Destination IP", "Event Signature", and "Timestamp". Two events are listed, both with a severity of 1 and a sensor of "bdr-beta-eth1.1". The first event is "ET TROJAN Suspicious User-Agent - Possible Trojan Downloader (...)" and the second is "ET TROJAN Tibs/Harnig Downloader Activity".

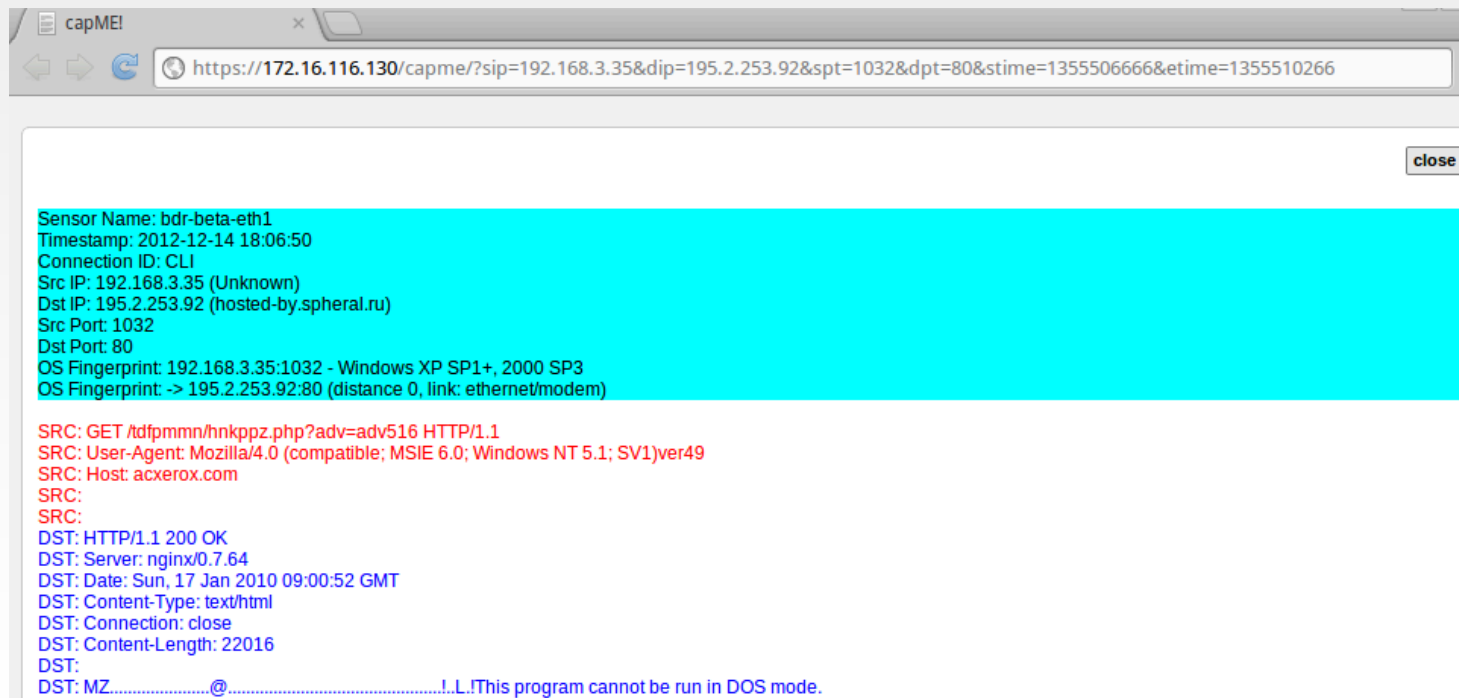
Below the event table, there are sections for "IP Header Information" and "Signature Information". The "IP Header Information" section shows a table with columns for "Source", "Destination", "Ver", "Hlen", "Tos", "Len", "ID", "Flags", "Off", "TTL", "Proto", and "Csum". The values are: Source: 192.168.3.35, Destination: 195.2.253.92, Ver: 4, Hlen: 5, Tos: 0, Len: 180, ID: 58, Flags: 0, Off: 0, TTL: 128, Proto: 6, Csum: 30175.

The "Signature Information" section shows a "Generator ID" of 1. A "Packet Capture Builder" dialog box is open, allowing the user to configure a packet capture. The dialog box has the following fields:

- Source address (Source Address : Source Port): 192.168.3.35 : 1032
- Destination address (Destination Address : Destination Port): 195.2.253.92 : 80
- Protocol: TCP
- Start time (default is 30 minutes before the event start time): 2012 December 14 17:36
- End time (default is 30 minutes after the event end time): 2012 December 14 18:36

At the bottom of the dialog box are "Fetch Packet" and "Cancel" buttons. The background interface also shows a "View Rule" button and a "URP" section with a value of 0.

# CapME



The screenshot shows a web browser window with the following details:

- Tab: capME
- Address Bar: <https://172.16.116.130/capme/?sip=192.168.3.35&dip=195.2.253.92&spt=1032&dpt=80&stime=1355506666&etime=1355510266>
- Close Button: close
- Sensor Name: bdr-beta-eth1
- Timestamp: 2012-12-14 18:06:50
- Connection ID: CLI
- Src IP: 192.168.3.35 (Unknown)
- Dst IP: 195.2.253.92 (hosted-by.spheral.ru)
- Src Port: 1032
- Dst Port: 80
- OS Fingerprint: 192.168.3.35:1032 - Windows XP SP1+, 2000 SP3
- OS Fingerprint -> 195.2.253.92:80 (distance 0, link: ethernet/modem)
- Log Entries:
  - SRC: GET /tdfpmmn/hnkppz.php?adv=adv516 HTTP/1.1
  - SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)ver49
  - SRC: Host: acxerox.com
  - SRC:
  - SRC:
  - DST: HTTP/1.1 200 OK
  - DST: Server: nginx/0.7.64
  - DST: Date: Sun, 17 Jan 2010 09:00:52 GMT
  - DST: Content-Type: text/html
  - DST: Connection: close
  - DST: Content-Length: 22016
  - DST:
  - DST: MZ.....@.....!..!This program cannot be run in DOS mode.

# Squert web interface

Welcome paalk | [Dashboard](#) | [Log out](#)

2010 January February March April May June July August September October November December 2011

Month: Tuesday Wednesday Thursday Friday Saturday Sunday Monday Tuesday Wednesday Thursday Friday Saturday Sunday Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Detail Lines: 10 Report Period: Thursday, Aug 18, 2011

**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	nasc-toll	smart	09:18:15	60	191	229	14549
Campus	dnsh-01	snort	09:18:07	8	40	3	821
OLL	oll-01	snort	-	0	0	0	0

**Event Distribution by Category**

#	Category	Last Event	Sig	Src	Dst	Count
01	Unclassified	09:17:21	15	17	22	6431
02	Unauthorized Admin Access	-	0	0	0	0
03	Unauthorized User Access	-	0	0	0	0
04	Attempted Unauthorized Access	-	0	0	0	0
05	Denial of Service Attack	-	0	0	0	0
06	Policy Violation	09:15:53	28	100	160	2069
07	Reconnaissance	09:18:15	6	5	8	5794
08	Malware	09:17:46	15	110	64	1076
09	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	30	856
ET SCAN LIBSSH Based SSH Connection - Often used as a BruteForce Tool	2006435	09:18:10	1	4	685
ET SCAN LIBSSH 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**

**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
UNITED KINGDOM	GB	0	111
GERMANY	DE	40	59
CANADA	CA	22	5
NETHERLANDS	NL	16	0
LATVIA	LV	4	4
CHINA	CN	4	0

**Top Source Countries**

- CANADA (1789)
- UNITED STATES (1594)
- NETHERLANDS (6)
- SPAIN (4)
- INDIA (2)

**Top Destination Countries**

- UNITED STATES (12013)
- CANADA (5751)
- NETHERLANDS (4409)
- GERMANY (276)
- EGYPT (478)

# Sguil client

RT	Count	Interface	Time	Date	Time	Source IP	Source Port	Dest IP	Dest Port	Protocol	Event
RT	1	BSidesATL-eth1	8.1	2011-11-03 21:12:56	210.114.220.46	653	192.168.1.102	111	17	UDP	GPL RPC portmap status request
RT	1	BSidesATL-eth1	8.2	2011-11-03 21:12:56	210.114.220.46	654	192.168.1.102	919	17	UDP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	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	TCP	ET POLICY Suspicious inbound to MSSOL 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{0,100}/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	Source Port	Dest Port	R	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	2243	21	.	.	.	X	X	.	.	.	3480775140	3956113150	8	0	32120	0	55423

# Pivot to pcap from Sguil

Sensor Name: qa-eth0  
Timestamp: 2011-09-23 13:38:35  
Connection ID: .qa-eth0\_29  
Src IP: 172.16.116.251 (Unknown)  
Dst IP: 74.125.47.132 (yw-in-f132.1e100.net)  
Src Port: 38256  
Dst Port: 80  
OS Fingerprint: 172.16.116.251:38256 - Linux 2.6 (newer, 1) (up: 1 hrs)  
OS Fingerprint: -> 74.125.47.132:80 (distance 0, link: ethernet/modem)

SRC: GET / HTTP/1.1  
SRC: User-Agent: curl/7.19.7 (i486-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15  
SRC: Host: securityonion.blogspot.com  
SRC: Accept: /\*  
SRC:  
SRC:  
DST: HTTP/1.1 200 OK  
DST: Content-Type: text/html; charset=UTF-8  
DST: Expires: Fri, 23 Sep 2011 13:38:35 GMT  
DST: Date: Fri, 23 Sep 2011 13:38:35 GMT  
DST: Cache-Control: private, max-age=0  
DST: Last-Modified: Fri, 23 Sep 2011 13:37:45 GMT  
DST: ETag: "3114913c-e7b3-4f2c-8dea-5797108fce8"  
DST: X-Content-Type-Options: nosniff  
DST: X-XSS-Protection: 1; mode=block  
DST: Server: GSE  
DST: Transfer-Encoding: chunked  
DST:  
DST: 1000

Search Abort Close

Debug Messages

/tmp/172.16.116.251:38256\_74.125.47.132:80-6.raw host 172.16.116.251 and host 74.125.47.132 and port 38256 and port 80 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

Fjfilter: 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=
2	0.146918	217.160.51.31	172.16.116.142	TCP	80 > 42994 [SYN, ACK] Seq=
3	0.146969	172.16.116.142	217.160.51.31	TCP	42994 > 80 [ACK] Seq=1 Ack=
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=
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 Ac
8	0.323989	172.16.116.142	217.160.51.31	TCP	42994 > 80 [FIN, ACK] Seq=
9	0.324344	217.160.51.31	172.16.116.142	TCP	80 > 42994 [ACK] Seq=260 Ac
10	0.475925	217.160.51.31	172.16.116.142	TCP	80 > 42994 [FIN, PSH, ACK]
11	0.476032	172.16.116.142	217.160.51.31	TCP	42994 > 80 [ACK] Seq=154 Ac

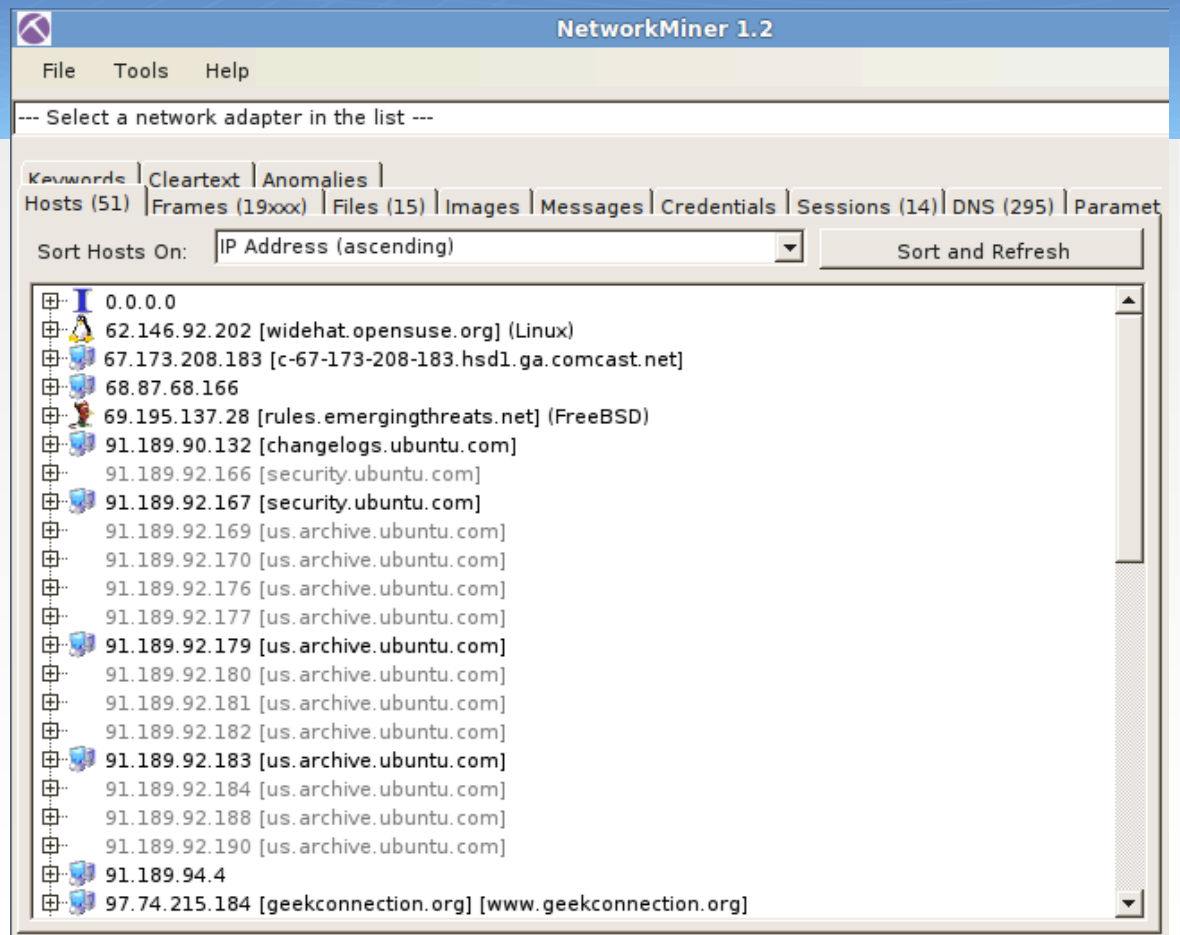
Frame 1 (74 bytes on wire, 74 bytes captured)  
Ethernet II, Src: 00:0c:29:e1:43:1e (00:0c:29:e1:43:1e), Dst: 00:50:56:fc:6f:0c (00:50:56:fc:6f:0c)  
Internet Protocol, Src: 172.16.116.142 (172.16.116.142), Dst: 217.160.51.31 (217.160.51.31)  
Transmission Control Protocol, Src Port: 42994 (42994), Dst 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 00 01 03 03 06 .....

File: "/tmp/172.16.116.142:42994\_..." Packets: 11 Displayed: 11 Marked: 0 Profile: Default

# NetworkMiner

There's gold in them  
thar PCAPs!



The screenshot shows the NetworkMiner 1.2 application window. The title bar reads "NetworkMiner 1.2". The menu bar includes "File", "Tools", and "Help". Below the menu bar, there is a prompt: "--- Select a network adapter in the list ---". The main interface features a navigation bar with tabs: "Keywords", "Cleartext", "Anomalies", "Hosts (51)", "Frames (19xxx)", "Files (15)", "Images", "Messages", "Credentials", "Sessions (14)", "DNS (295)", and "Parameters". The "Hosts (51)" tab is active. Below the navigation bar, there is a "Sort Hosts On:" dropdown menu set to "IP Address (ascending)" and a "Sort and Refresh" button. The main display area shows a list of hosts, each with a small icon, an IP address, and a description in brackets. The list is sorted by IP address in ascending order.

IP Address	Description
0.0.0.0	
62.146.92.202	[widehat.opensuse.org] (Linux)
67.173.208.183	[c-67-173-208-183.hsd1.ga.comcast.net]
68.87.68.166	
69.195.137.28	[rules.emergingthreats.net] (FreeBSD)
91.189.90.132	[changelogs.ubuntu.com]
91.189.92.166	[security.ubuntu.com]
91.189.92.167	[security.ubuntu.com]
91.189.92.169	[us.archive.ubuntu.com]
91.189.92.170	[us.archive.ubuntu.com]
91.189.92.176	[us.archive.ubuntu.com]
91.189.92.177	[us.archive.ubuntu.com]
91.189.92.179	[us.archive.ubuntu.com]
91.189.92.180	[us.archive.ubuntu.com]
91.189.92.181	[us.archive.ubuntu.com]
91.189.92.182	[us.archive.ubuntu.com]
91.189.92.183	[us.archive.ubuntu.com]
91.189.92.184	[us.archive.ubuntu.com]
91.189.92.188	[us.archive.ubuntu.com]
91.189.92.190	[us.archive.ubuntu.com]
91.189.94.4	
97.74.215.184	[geekconnection.org] [www.geekconnection.org]

# ELSA

ELSA Admin

Query

From  To      R

[class=BRO\\_HTTP \(602\) \[Grouped by user\\_agent\]](#)

Result Options...

Count	Value
446	<a href="#">Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)</a>
54	-
14	<a href="#">Bob's Evil Clown C&amp;C Agent</a>
14	<a href="#">NSISDL/1.2 (Mozilla)</a>
10	<a href="#">Mozilla/4.0 (compatible; UPnP/1.0; Windows NT/5.1)</a>
10	<a href="#">Mozilla/4.0 (compatible; UPnP/1.0; Windows 9x)</a>
8	<a href="#">Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)</a>
8	<a href="#">Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)ver49</a>
8	<a href="#">Mozilla/4.0 (compatible; MSIE 6.0; Win32)</a>
3	<a href="#">uri</a>
3	<a href="#">string</a>
2	<a href="#">Windows-Update-Agent</a>
2	<a href="#">BTWebClient/2220</a>
2	<a href="#">BTWebClient/6120</a>
1	<a href="#">curl/7.22.0 (x86_64-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23 librtmp/2.3</a>
1	<a href="#">Firefox 1</a>

# Pivot to pcap from ELSA

ELSA Admin 1 node(s) with 10042.0 logs indexed and 19011.0 archived

Query  Submit Query Help

From  To  Add Term Report On Archive  Reuse current tab  Grid display

class=BRO\_NOTICE BRO\_NOTICE.notice\_type='HTTP::Malware\_Hash\_Registry\_Match' (4) X

Result Options... Records: 4 / 4 489 ms 2 < prev 1 next > 15

	Timestamp	host (1)	program (1)	class (1)	srcip (3)	srcport (4)	dstip (3)	dstport (1)	notice_type (1)	notice_msg (4)
Info	Fri Dec 14 18:06:51	<a href="#">127.0.0.1</a>	<a href="#">bro_notice</a>	<a href="#">BRO_NOTICE</a>	<a href="#">192.168.3.35</a>	<a href="#">1032</a>	<a href="#">195.2.253.92</a>	<a href="#">80</a>	<a href="#">HTTP::Malware_Hash_Registry_Match</a>	<a href="#">192.168.3.35</a> <a href="#">38331f62959ad1170d7ca41308dd25de</a> <a href="#">http://acxerox.com/tdfpmmn/hnkppz.php?adv=adv516</a>
Info	Fri Dec 14 18:06:51	<a href="#">127.0.0.1</a>	<a href="#">bro_notice</a>	<a href="#">BRO_NOTICE</a>	<a href="#">192.168.3.35</a>	<a href="#">1033</a>	<a href="#">195.2.253.92</a>	<a href="#">80</a>	<a href="#">HTTP::Malware_Hash_Registry_Match</a>	<a href="#">192.168.3.35</a> <a href="#">9563754c0f76f2bb1eabfa71dad730e1</a> <a href="#">http://acxerox.com/tdfpmmn/hohhveswgc.php?adv=adv516</a>
Info	Fri Dec 14 18:07:05	<a href="#">127.0.0.1</a>	<a href="#">bro_notice</a>	<a href="#">BRO_NOTICE</a>	<a href="#">192.168.3.25</a>	<a href="#">1054</a>	<a href="#">89.187.51.0</a>	<a href="#">80</a>	<a href="#">HTTP::Malware_Hash_Registry_Match</a>	<a href="#">192.168.3.25</a> <a href="#">690eb4a6f24524479c3d3829337c9dd3</a> <a href="#">http://pipiskin.hk/load.exe</a>
Info	Fri Dec 14 18:07:06	<a href="#">127.0.0.1</a>	<a href="#">bro_notice</a>	<a href="#">BRO_NOTICE</a>	<a href="#">192.168.3.65</a>	<a href="#">1035</a>	<a href="#">188.72.243.72</a>	<a href="#">80</a>	<a href="#">HTTP::Malware_Hash_Registry_Match</a>	<a href="#">192.168.3.65</a> <a href="#">9e04a788281c727566873d9df263aec1</a> <a href="#">http://www.hostme.name/ser.exe</a>

Records: 4 / 4 489 ms 2 < prev 1 next > 15

Log Info X

Summary

Links

Plugins

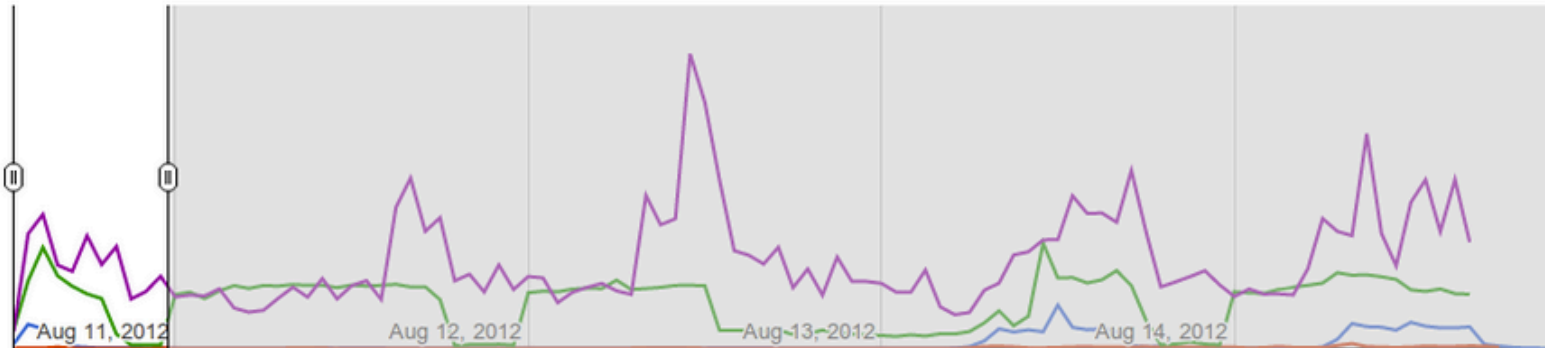
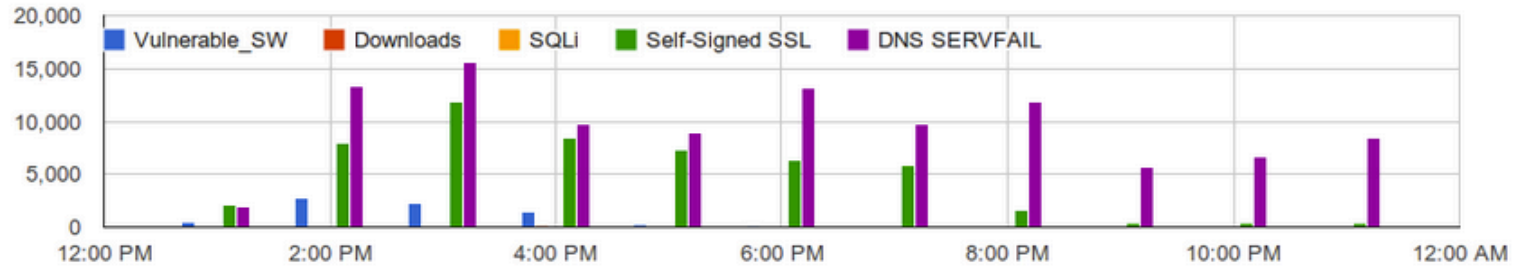
Plugin

getPcap (optional)

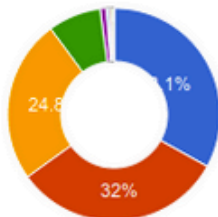
Close

# Bro IDS

## Bro Events



### Self-Signed SSL Destinations



- 69.28.69.85
- 65.197.254.80
- 204.238.52.28
- 210.173.216.40
- 12.230.219.149
- 207.230.34.120
- ▲ 1/2 ▼

### subject

```

emailAddress=admin@wiredsolar.net,CN=secure.wiredsolar.net,OU=IT,O=Wired
Solar,L=Flagler,ST=Florida,C=US
CN=rsip.monitoredsecurity.com,OU=IT Security,O=Symantec Corporation,L=Northern
emailAddress=dhoover@centonline.com,CN=Dean Hoover,OU=Network Admin,O=Ce
Berlin,ST=Wisconsin,C=US
ST=Tokyo,OU=Remote Service,O=RICOH COMPANY,L=Aoyama,C=JP,CN=G
CN=mcs1hkg.live.citrixonline.com,OU=Operations,O=Citrix Online LLC,L=Fort Lauder
C=CA
C=US,CN=mail.tytx.com
CN=TrustedSourceServer_IMQA01
    
```

# Bro Flow

ELSA Admin 1 node(s) with 353.0 logs indexed and 484.0 archived

Query   [Help](#)

From  To      Reuse current tab  Grid display

Result Options... Records: 100 / 471 91 ms ? [< prev](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [next >](#)

	Timestamp	host (1)	program (1)	class (1)	srcip (12)	srcport (83)	dstip (41)	dstport (11)	proto (3)
<a href="#">Info</a>	Mon Dec 24 21:19:29	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">70.55.213.211</a>	<a href="#">31337</a>	<a href="#">192.88.99.1</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:30	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1032</a>	<a href="#">195.2.253.92</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:30	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1033</a>	<a href="#">195.2.253.92</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:30	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1034</a>	<a href="#">195.2.253.92</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:30	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1036</a>	<a href="#">195.2.253.92</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:30	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1037</a>	<a href="#">195.2.253.92</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1035</a>	<a href="#">66.96.224.213</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1040</a>	<a href="#">216.34.181.45</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1041</a>	<a href="#">205.188.156.248</a>	<a href="#">25</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1042</a>	<a href="#">65.54.188.110</a>	<a href="#">25</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1043</a>	<a href="#">64.18.4.11</a>	<a href="#">25</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1044</a>	<a href="#">208.65.153.154</a>	<a href="#">25</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1045</a>	<a href="#">208.48.95.23</a>	<a href="#">25</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1046</a>	<a href="#">96.0.203.90</a>	<a href="#">80</a>	<a href="#">TCP</a>
<a href="#">Info</a>	Mon Dec 24 21:19:31	<a href="#">127.0.0.1</a>	<a href="#">bro_conn</a>	<a href="#">BRO_CONN</a>	<a href="#">192.168.3.35</a>	<a href="#">1047</a>	<a href="#">96.0.203.122</a>	<a href="#">80</a>	<a href="#">TCP</a>

Records: 100 / 471 91 ms ? [< prev](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [next >](#)

# Popular Dst IPs

ELSA Admin

Query class=BRO\_CONN

From 2012-12-22 21:17:02 To Add Term dstip

class=BRO\_CONN (471) class=BRO\_CONN (529) [Grouped by dstip]

Result Options...

Save Chart As...

Count	Value
82	<a href="#">192.168.10.101</a>
69	<a href="#">192.168.10.100</a>
33	<a href="#">192.168.10.128</a>
17	<a href="#">192.168.10.102</a>
17	<a href="#">64.127.109.133</a>
14	<a href="#">192.168.10.125</a>
11	<a href="#">192.168.1.101</a>
11	<a href="#">4.2.2.1</a>
9	<a href="#">66.235.132.121</a>
9	<a href="#">192.168.10.127</a>
5	<a href="#">130.239.18.173</a>
5	<a href="#">195.2.253.92</a>
5	<a href="#">192.168.10.124</a>
5	<a href="#">224.0.0.251</a>
4	<a href="#">192.168.1.102</a>
4	<a href="#">75.101.155.80</a>
3	<a href="#">65.54.188.110</a>
3	<a href="#">208.48.95.23</a>
3	<a href="#">0.0.0.0</a>
3	<a href="#">205.188.156.248</a>
3	<a href="#">64.18.4.11</a>
3	<a href="#">8.18.65.67</a>
3	<a href="#">192.25.206.10</a>
3	<a href="#">80.157.169.154</a>

# Popular Dst Ports

ELSA Admin

Query class=BRO\_CONN

From 2012-12-22 21:17:02 To Add Term dstport

class=BRO\_CONN (471) class=BRO\_CONN (905) [Grouped by dstport]

Result Options... Save Chart As...

Count	Value
138	<a href="#">1900</a>
135	<a href="#">80</a>
109	<a href="#">53</a>
95	<a href="#">2869</a>
31	<a href="#">137</a>
25	<a href="#">2222</a>
22	<a href="#">3</a>
21	<a href="#">445</a>
17	<a href="#">25</a>
15	<a href="#">6881</a>
14	<a href="#">88</a>
13	<a href="#">16001</a>
12	<a href="#">139</a>
11	<a href="#">138</a>
9	<a href="#">0</a>
9	<a href="#">389</a>
7	<a href="#">51413</a>
6	<a href="#">5353</a>
6	<a href="#">6882</a>
5	<a href="#">135</a>
4	<a href="#">1025</a>
3	<a href="#">6969</a>
2	<a href="#">62904</a>
2	<a href="#">16253</a>

# Drilling into an interesting Dst Port

ELSA Admin 1 node(s) with 353.0 logs indexed

Query: class=BRO\_CONN +dstport="6881" Submit Query Help

From: 2012-12-22 21:17:02 To: Add Term Report On Index Reuse current tab Grid display

class=BRO\_CONN (471) class=BRO\_CONN (905) [Grouped by dstport] class=BRO\_CONN +dstport="6881" (15)

Result Options... Records: 15 / 15 50 ms < prev 1 next > 15

	Timestamp	host (1)	program (1)	class (1)	srcip (1)	srcport (5)	dstip (11)	dstport (1)	proto (2)
Info	Mon Dec 24 21:19:43	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	1614	77.243.184.65	6881	TCP
Info	Mon Dec 24 21:19:43	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	1613	78.52.129.97	6881	TCP
Info	Mon Dec 24 21:19:43	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	1630	213.156.52.138	6881	TCP
Info	Mon Dec 24 21:20:30	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	36012	72.20.34.145	6881	UDP
Info	Mon Dec 24 21:20:31	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	213.156.52.138	6881	UDP
Info	Mon Dec 24 21:20:31	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	131.95.100.37	6881	UDP
Info	Mon Dec 24 21:20:32	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	151.14.129.36	6881	UDP
Info	Mon Dec 24 21:20:33	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	90.32.147.198	6881	UDP
Info	Mon Dec 24 21:20:33	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	82.232.190.163	6881	UDP
Info	Mon Dec 24 21:20:33	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	81.52.169.78	6881	UDP
Info	Mon Dec 24 21:20:34	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	77.243.184.65	6881	UDP
Info	Mon Dec 24 21:20:35	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	72.20.34.145	6881	UDP
Info	Mon Dec 24 21:20:35	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	213.17.30.123	6881	UDP
Info	Mon Dec 24 21:20:35	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	203.59.42.71	6881	UDP
Info	Mon Dec 24 21:20:35	127.0.0.1	bro_conn	BRO_CONN	192.168.10.128	37612	78.52.129.97	6881	UDP

Records: 15 / 15 50 ms < prev 1 next > 15

# What is that Dst Port? Pivot 2 Pcap!

ELSA x capMEI x

https://172.16.116.131/capme/?sip=192.168.10.128&dip=77.243.184.65&spt=1614&dpt=6881&stime=1356382183&etime=1356385783

close

Sensor Name: bdr-eth1  
Timestamp: 2012-12-24 21:19:32  
Connection ID: CLI  
Src IP: 77.243.184.65 (mirror.be.gbxs.net)  
Dst IP: 192.168.10.128 (Unknown)  
Src Port: 6881  
Dst Port: 1614  
OS Fingerprint: 192.168.10.128:1614 - Windows XP SP1+, 2000 SP3  
OS Fingerprint -> 77.243.184.65:6881 (distance 0, link: ethernet/modem)

DST: .BitTorrent protocol.....OB\*..l.q.W.1M6-1-2--n4..^..e.T.  
SRC: .BitTorrent protocol.....OB\*..l.q.W.1-t0C40-...z.@x.....F.d1:ei0e1.md6.ut\_pexi0ee1.pi6881e4:reqqi2048e1.v17:libTorrent 0.12.4e....  
DST: .....d1:ei0e1.md11.upload\_onlyi3e11.ut\_metadataal2e6.ut\_pexi1ee4:ipv44:@.d13:metadata\_sizei25951  
SRC: .....  
DST: e1:pi37612e4:reqqi255e1.v16:BitTorrent 6.1.26:yourip4:M.Ae.....@.....  
DST: .....  
SRC: .....

DEBUG: Raw data request sent to bdr-eth1.  
DEBUG: Making a list of local log files.  
DEBUG: Looking in /nsm/sensor\_data/bdr-eth1/dailylogs/2012-12-24.  
DEBUG: Making a list of local log files in /nsm/sensor\_data/bdr-eth1/dailylogs/2012-12-24.  
DEBUG: Available log files:  
DEBUG: 1356383500  
DEBUG: Creating unique data file: /usr/sbin/tcpdump -r /nsm/sensor\_data/bdr-eth1/dailylogs/2012-12-24/snort.log.1356383500 -w /tmp/77.243.184.65:6881\_192.168.10.128:1614-6.raw (ip and host 192.168.10.128 and host 77.243.184.65 and port 1614 and port 6881 and proto 6) or (vlan and host 192.168.10.128 and host 77.243.184.65 and port 1614 and port 6881 and proto 6)  
DEBUG: Receiving raw file from sensor.  
QUERY: SELECT sancp.start\_time, s2.sid, s2.hostname FROM sancp LEFT JOIN sensor ON sancp.sid = sensor.sid LEFT JOIN sensor AS s2 ON sensor.hostname = s2.hostname WHERE sancp.start\_time >= '2012-12-24 20:49:43' AND sancp.end\_time <= '2012-12-24 21:49:43' AND ((src\_ip = INET\_ATON('192.168.10.128') AND src\_port = 1614 AND dst\_ip = INET\_ATON('77.243.184.65') AND dst\_port = 6881) OR (src\_ip = INET\_ATON('77.243.184.65') AND src\_port = 6881 AND dst\_ip = INET\_ATON('192.168.10.128') AND dst\_port = 1614)) AND s2.agent\_type = 'pcap' LIMIT 1

# 2013: The Metrics

- Security Onion 10.04  
37,521
- Security Onion 12.04 (released 12/31/2012)  
34,290 from SourceForge
- Security Onion 12.04.1 (released 6/10/2013)  
6,380 from Sourceforge
- Security Onion 12.04.2 (released 7/25/2013)  
737 from Sourceforge
- ??? From BitTorrent  
??? Ubuntu/Kubuntu/Lubuntu + Security Onion PPA

# Where do we go now?

<http://securityonion.blogspot.com>

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

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