

The Security Onion

Chris Krieger

Security Onion 101

Security Onion is a network security monitoring (NSM) system that provides full-context and forensic visibility into the traffic it monitors

Designed to make deploying complex open source tools simple via a single package (Snort, Suricata, Sguil, Snorby etc.)



Peeling the Onion

Contains a boatload of security tools

Easy setup wizard ... even a Windows Admin can do it!

Has the ability to pivot from one tool to the next to seamlessly

- One of the most effective collection of network security tools available in a single package

Behind the Onion

Created by Doug Burks

Grew out of a SANS Gold Paper

He wanted to make NSM easier to deploy



Before the Onion

Get an alert (firewall, user, etc.)

Look for the alert in some SIEM tool

Try to correlate with other events in SIEM

Oh crap ... We didn't add that server to the SIEM yet – my bad

With NSM & SO

We can take an IDS alert -->

```
alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"GPL SHELLCODE  
x86 inc ebx NOOP";content:"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"; fast_pattern:only; classtype:  
shellcode-detect; sid:2101390; rev:7;)
```

And turn it into something useful:

- Full traffic packet captures
- ASCII transcripts of traffic
- Ability to carve files (or malware) for later analysis
- Build our own alerts

Onion Layers

Over 60 custom tools

- Snort – Signature based IDS
- Sguil – Security analyst console
- Squert -View HIDS/NIDS alerts and HTTP logs
- Snorby -View and annotate IDS alerts
- ELSA - Search logs (IDS, Bro and syslog)
- Bro - Powerful network analysis framework with highly detailed logs
- OSSEC - Monitors local logs, file integrity & rootkits

Onion Links

Project Home

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

Blog

<http://securityonion.blogspot.com>

Mailing Lists

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

Google Group

<https://groups.google.com/forum/?fromgroups#!forum/security-onion>

Wiki

<http://code.google.com/p/security-onion/w/list>

Installing the Onion

Download the ISO from the SO website.

Write/Burn to media

- Do *not* download updates while installing
- Do *not* Install this third-party software
- Create Username & Password
 - Just make sure you remember them.

VMTools/Virtualbox on the Onion

Tools adds features to the VM and helps manage memory better

Updating the Onion

SO has a customized update script

- # sudo soup



Wireshark

The default version of Wireshark (WS) in SO needs updating

Download WS source code from WS's website in SO

```
tar xaf wireshark-<version>.tar.bz2
```

```
cd wireshark-<version>
```

```
sudo apt-get install build-essential qt4-dev-tools libgtk-3-dev libpcap-dev
```

```
sudo ./configure
```

```
sudo make
```

```
sudo make install
```

```
sudo ldconfig
```



Setup the Onion

SO has a Customized Configuration script

- Configuring SO Software
 - Configuration of network
 - Install NSM Software Components
 - Configure storage settings
 - Finalize configuration

SO tool highlights

- SO Data presentation tools
 - Packet Analysis Tools
 - NSM consoles
- SO Data collection tools
- SO Data delivery tools

tcpdump

- Command line tool
 - Available, but does not run by default
- Many uses, capture's live traffic
- Replays already captured traffic
- Can use BPF filters to only capture protocol
 - host, ip, port, etc.
- Available for almost all Linux distributions.

tcpdump switches

- -n doesn't resolve IP's to hosts
- -i specific ethernet adapter
- -c count of packets to capture
- -s specify bytes to capture
- -w <filename> write packets to file
- -r <filename> read packets from filename

** man tcpdump for more details

tcpdump filters

- icmp (only capture icmp traffic)
- port <port #>(only capture specific port)
- tcp (only capture tcp traffic)
- host <host, IP, or net> traffic related to host
- src <host, IP, or net> only capture src traffic
- dst <host, IP, or net> only capture dst traffic
- NOT <any above> to remove

```
ckrieger@wizard ~ $ sudo tcpdump -i wlp4s0 -c 10 not arp and not stp and port 80 or 443
```

```
error : ret -1
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on wlp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
13:53:37.715701 IP sl-ads-default-adcom-mtc.evip.aol.com.http > 192.168.100.149.56137: Flags [.], ack 1592060168, win 1023, length 0
```

```
13:53:38.195830 IP 173.194.204.189.https > 192.168.100.149.59447: Flags [P.], seq 419932806:419932866, ack 3826844911, win 1373, options [nop,nop,TS val 3394942394 ecr 10155631], length 60
```

```
13:53:38.196497 IP 173.194.204.189.https > 192.168.100.149.59447: Flags [P.], seq 60:101, ack 1, win 1373, options [nop,nop,TS val 3394942394 ecr 10155631], length 41
```

```
13:53:38.197513 IP 192.168.100.149.59447 > 173.194.204.189.https: Flags [.], ack 101, win 1424, options [nop,nop,TS val 10167249 ecr 3394942394], length 0
```

```
13:53:38.197681 IP 192.168.100.149.59447 > 173.194.204.189.https: Flags [P.], seq 1:42, ack 101, win 1424, options [nop,nop,TS val 10167249 ecr 3394942394], length 41
```

```
13:53:38.210818 IP 192.168.100.149.59447 > 173.194.204.189.https: Flags [.], seq 42:1460, ack 101, win 1424, options [nop,nop,TS val 10167262 ecr 3394942394], length 1418
```

```
13:53:38.212313 IP 192.168.100.149.52775 > 69-47-66-163.static.try.wideopenwest.com.http: Flags [.], ack 3081155451, win 658, options [nop,nop,TS val 10167264 ecr 1338437134], length 0
```

```
13:53:38.212333 IP 192.168.100.149.32947 > 69-47-66-187.static.try.wideopenwest.com.http: Flags [.], ack 114479976, win 237, options [nop,nop,TS val 10167264 ecr 986702086], length 0
```

```
13:53:38.214733 IP 192.168.100.149.59447 > 173.194.204.189.https: Flags [P.], seq 1460:2586, ack 101, win 1424, options [nop,nop,TS val 10167266 ecr 3394942394], length 1126
```

```
13:53:38.224565 IP 69-47-66-187.static.try.wideopenwest.com.http > 192.168.100.149.32947: Flags [.], ack 1, win 494, options [nop,nop,TS val 986712128 ecr 10147219], length 0
```

```
10 packets captured
```

```
28 packets received by filter
```

```
0 packets dropped by kernel
```

tcpdump in action

dumpcap and tshark

- Part of Wireshark's installation
- dumpcap works similar to tcpdump
 - However, dumps traffic without reading it
- dumpcap uses BPF filters, just like tcpdump
- tshark can use Wireshark Display filters

****** man <command> gives more details

```
secops@Solnx02:/opt/samples$ sudo dumpcap -i eth1 -c 10 -f "not arp and not stp"
Capturing on 'eth1'
File: /tmp/wireshark_pcapng_eth1_20150125000430_yCZ4wV
Packets captured: 10
Packets received/dropped on interface 'eth1': 10/0 (pcap:0/dumpcap:0/flushed:0) (100.0%)
secops@Solnx02:/opt/samples$ sudo tshark -r /tmp/wireshark_pcapng_eth1_20150125000430_yCZ4wV
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
 1 0.000000000 192.168.100.149 -> 216.58.216.195 TLSv1.2 107 Application Data
 2 0.013592000 192.168.100.149 -> 216.58.216.195 TCP 64 47587 > https [PSH, ACK] Seq=3665770321 Ack=1684055694 Win=339[Malformed Packet]
 3 0.014008000 192.168.100.149 -> 216.58.216.195 TCP 64 47587 > https [PSH, ACK] Seq=3665770321 Ack=1684055694 Win=339[Malformed Packet]
 4 0.014269000 192.168.100.149 -> 216.58.216.195 TCP 64 47587 > https [PSH, ACK] Seq=3665770321 Ack=1684055694 Win=339[Malformed Packet]
 5 0.014770000 192.168.100.149 -> 216.58.216.195 TCP 64 47587 > https [PSH, ACK] Seq=3665770321 Ack=1684055694 Win=339[Malformed Packet]
 6 0.044313000 216.58.216.195 -> 192.168.100.149 TLSv1.2 131 Application Data
 7 0.044423000 192.168.100.149 -> 216.58.216.195 TCP 66 47587 > https [ACK] Seq=42 Ack=66 Win=339 Len=0 TSval=28820184 TSecr=134047744
 8 0.044671000 216.58.216.195 -> 192.168.100.149 TLSv1.2 111 Application Data
 9 0.044740000 192.168.100.149 -> 216.58.216.195 TCP 66 47587 > https [ACK] Seq=42 Ack=111 Win=339 Len=0 TSval=28820185 TSecr=134047744
10 0.044751000 216.58.216.195 -> 192.168.100.149 TCP 66 https > 47587 [FIN, ACK] Seq=111 Ack=42 Win=354 Len=0 TSval=134047744 TSecr=28820140
secops@Solnx02:/opt/samples$
```

dumpcap and tshark in action

Argus

- Generates and analyzes Session data
- Saves data in binary
 - Only readable by Argus
- Session data much smaller than full packets
- There are several SO tools that capture session data

```

secops@Solnx02:~$ ra -n -r /nsm/sensor_data/Solnx02-eth1/argus/2015-01-24.log -N 30
  StartTime      Flgs Proto      SrcAddr Sport  Dir      DstAddr  Dport  TotPkts  TotBytes  State
23:20:00.065622 e      udp      192.168.100.10.63038 ->      233.89.188.1.10001 1      60      INT
23:20:00.065986 e      udp      192.168.100.10.63038 ->      255.255.255.255.10001 10     871     INT
23:20:00.351122 e      arp      192.168.100.149 who     192.168.100.230 9      568     CON
23:20:00.577979 *      llc      00:14:69:16:bb:49.170 ->      01:00:0c:cc:cc:cd.170 14     908     INT
23:20:00.578818 e      arp      192.168.100.200 who     192.168.100.19 12     764     INT
23:20:00.783350 e      arp      192.168.100.15 who     192.168.100.19 69     4913    INT
23:20:00.885565 e      arp      192.168.100.138 who     192.168.100.254 82     5240    INT
23:20:01.806091 e      arp      192.168.100.51 who     192.168.100.254 4      252     INT
23:20:05.663844 e      udp      192.168.100.149.39904 <->     192.168.100.2.53 2      576     CON
23:20:05.665277 e      udp      192.168.100.149.38996 <->     192.168.100.2.53 2      552     CON
23:20:05.666853 e *    tcp      192.168.100.149.53350 ->      141.101.114.190.80 10170  8952675 CON
23:20:05.800225 e      arp      192.168.100.15 who     192.168.100.19 2      124     INT
23:20:06.721243 *      llc      00:14:69:16:bb:49.170 ->      01:00:0c:cc:cc:cd.170 12     780     REQ
23:20:07.031672 e      arp      192.168.100.138 who     192.168.100.254 9      564     INT
23:20:07.540879 e      arp      192.168.100.10 who     192.168.100.70 4      252     INT
23:20:10.037811 e      tcp      173.194.68.189.443 <?>     192.168.100.149.57883 2      192     CON
23:20:10.675006 e d    tcp      192.168.100.149.53350 ->      141.101.114.190.80 4141  3772271 FIN
23:20:11.116802 e d    tcp      74.125.29.189.443 <?>     192.168.100.149.45397 14     4831    CON
23:20:12.764684 *      llc      00:14:69:16:bb:49.170 ->      01:00:0c:cc:cc:cd.170 24     1548    REQ
23:20:13.173594 e      arp      192.168.100.138 who     192.168.100.254 24     1524    INT
23:20:13.377028 e      udp      192.168.100.149.59753 <->     192.168.100.2.53 8      960     CON
23:20:13.382383 e      udp      192.168.100.149.48416 <->     192.168.100.2.53 2      552     CON
23:20:13.384236 e d    tcp      192.168.100.149.36953 ->      141.101.115.190.80 558    471383 FIN
23:20:15.016296 e      arp      192.168.100.17 who     192.168.100.19 35     2216    INT
23:20:15.535128 e      udp      192.168.100.149.54471 <->     192.168.100.2.53 5      1083    CON
23:20:15.821214 e s    tcp      192.168.100.149.59464 ->      196.216.2.9.21 62     4768    FIN
23:20:17.476544 e      tcp      192.168.100.149.44360 ->      196.216.2.9.33300 13     938     FIN
23:20:18.379222 e      arp      192.168.100.2 who     192.168.100.149 6      376     CON
23:20:18.497564 e      arp      192.168.100.20 who     192.168.100.19 18     1132    INT
23:20:18.580823 e      udp      192.168.100.149.55761 <->     192.168.100.2.53 2      609     CON
secops@Solnx02:~$ █

```

argus in action

xplico

- Similar to Networkminer, except using a web interface
- Load a pcap file in and it analyses and spits out contents
- Also able to sniff traffic off the wire
 - Powerful analysis tool

For a complete view of html page set your browser to use Proxy, and point it to Web server.

Web URLs: Html Image Flash Video Audio JSON All

Search:

Go

Date	Url	Size	Method	Info
2010-02-26 20:15:14	homesitetoo.com/back11/stat1.php	84	POST	info.xml
2010-02-26 20:15:14	homesitetoo.com/back11/stat1.php	84	POST	info.xml

Previous

1 of 1

Next

Undecoded

Enhance

NSM - Centric look at Network Traffic

- Tools are designed to help paint the bigger picture of overall communication
- Help with analysis to review many forms of data
- Help create an auditable analysis workflow

Sguil

- A Client / server application
- Collects data with deployed agents
- *Only a live tool*
- Key functions
 - Aggregates similar alert data
 - Processes metadata and makes it easy to find
 - Allows for queries and review of alert data
 - Allows for classification and pivot of events

Sguil alerts

- Incorporates 4 types of event data
 - IDS engine data like snort
 - Host based IDS like OSSEC
 - Network profile data from prads
 - Http transaction data from bro
- The interface takes some getting used to
 - NSM book does a decent job explaining it

*We'll explore these other tools later in the course

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: secops UserID: 2 2015-01-25 02:21:02 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	24	Solnx02-e...	3.31	2015-01-25 02:07:00	195.2.253.92	80	192.168.3.35	1032	6	ET MALWARE Possible W...
RT	1	Solnx02-e...	3.57	2015-01-25 02:07:00	192.168.3.35	1035	66.96.224.213	80	6	ET TROJAN Generic .bin ...
RT	1	Solnx02-e...	3.58	2015-01-25 02:07:01	192.168.3.35	1036	195.2.253.92	80	6	ET TROJAN TrojanDownl...
RT	1	Solnx02-e...	3.62	2015-01-25 02:07:01	192.168.1.101	1037	65.32.5.111	53	17	ET INFO DYNAMIC_DNS ...
RT	1	Solnx02-e...	4.35	2015-01-25 02:07:04	192.168.1.10	49174	4.2.2.1	53	17	PADS New Asset - unkno...
RT	1	Solnx02-e...	4.36	2015-01-25 02:07:04	192.168.1.10	49163	8.18.65.67	80	6	PADS New Asset - http A...
RT	1	Solnx02-e...	4.37	2015-01-25 02:07:04	192.168.10.127	1196	192.168.10.101	445	6	PADS New Asset - unkno...
RT	1	Solnx02-e...	4.38	2015-01-25 02:07:04	192.168.10.101	1196	192.168.10.101	445	6	PADS Changed Asset - s...
RT	1	Solnx02-e...	4.39	2015-01-25 02:07:04	192.168.10.128	1088	192.168.10.101	53	17	PADS New Asset - unkno...
RT	1	Solnx02-e...	4.40	2015-01-25 02:07:04	192.168.10.101	1036	216.239.34.10	53	17	PADS New Asset - unkno...
RT	1	Solnx02-e...	4.41	2015-01-25 02:07:04	192.168.10.128	1295	74.125.45.100	80	6	PADS New Asset - http ...
RT	1	Solnx02-e...	4.42	2015-01-25 02:07:04	192.168.10.101	1088	192.168.10.101	53	17	PADS Changed Asset - d...
RT	1	Solnx02-e...	4.43	2015-01-25 02:07:05	192.168.10.103	44880	82.96.64.4	6667	6	PADS New Asset - unkno...

IP Resolution Agent Status Snort Statistics System Ms

Sid	Sensor	Pckt Loss	Avg B/W	Alerts	Pa
3	Solnx02-e...	0.000%	...6Mb/s	0.000/sec	...

Show Packet Data Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hkSu										
TCP	Source Port	Dest Port	U	A	P	R	S	F	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res Window	Urp	hkSu
DATA																					

Search Packet Payload Hex Text NoCase

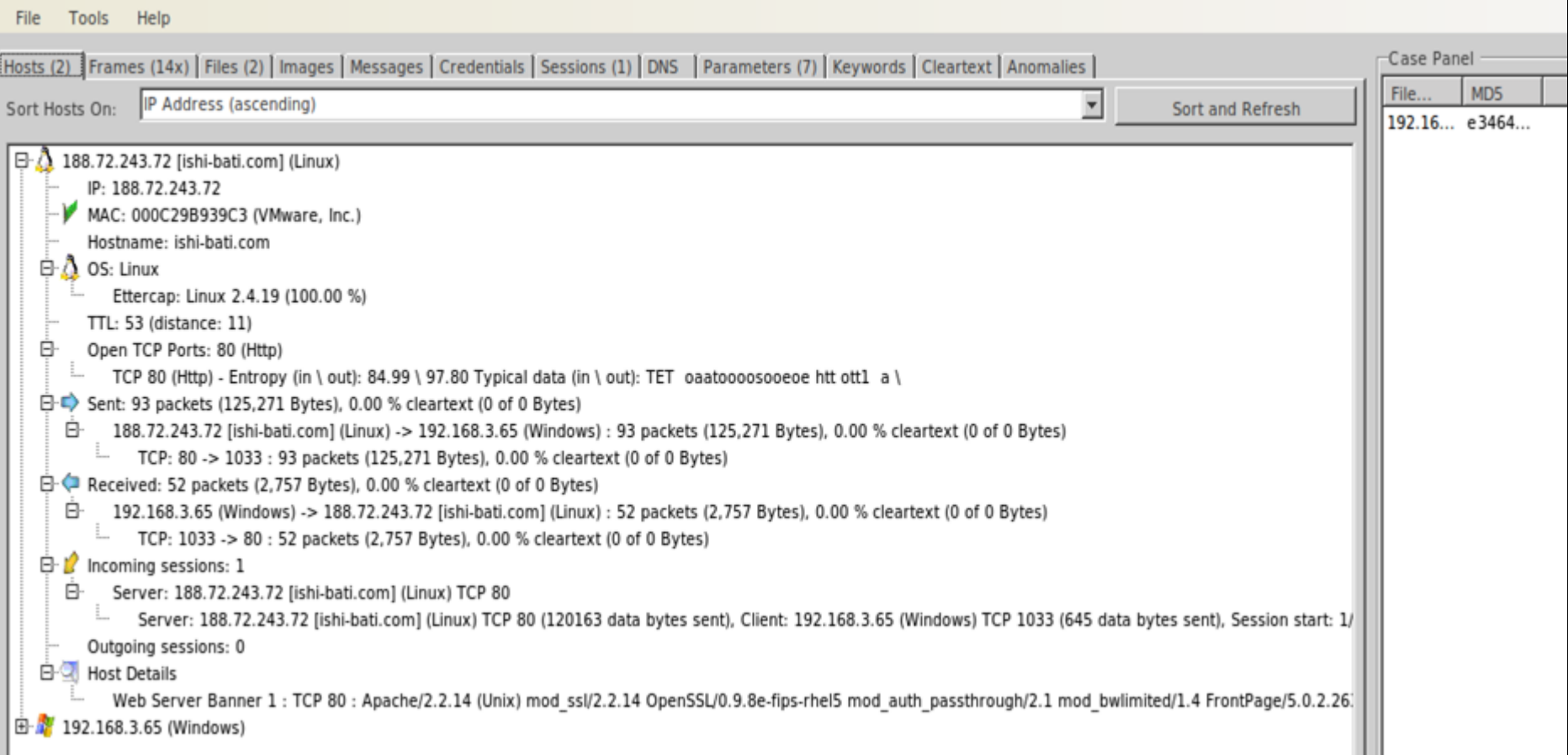
sguil main screen

Network Miner

Windows App, running under Mono in SO

Extracts & organizes host and content data

- Provides good overview of network-based artifacts
- Parsing traces might take time



Network Miner in action

Squert

- Web front-end for Sguil database
- Adds additional features like visualizations and supporting information to events

EVENTS

SUMMARY

VIEWS



19.2%

80.8%

INTERVAL: 2015-01-24 00:00:00 -> 2015-01-24 23:59:59 (+00:00)

FILTERED BY OBJECT: NO

FILTERED BY SENSOR: NO

PRIORITY:

queue only	<input type="checkbox"/>												PADS New Asset - http 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)	1	6	1.038%
grouping	<input type="checkbox"/>	13	5	3	12		23:58:47									
SUMMARY	<input checked="" type="checkbox"/>	2	5	1	1		23:50:20						PADS Changed Asset - domain DNS SQR No Error	2	17	0.160%
queued events	52	10	1	1			23:45:20						GPL ICMP_INFO PING *NIX	2100366	1	0.798%
total events	1253															
total signatures	7	1	7	1	1		23:28:21						[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112	0	0.080%
total sources	-															
total destinations	-	21	7	1	1		23:26:06						[OSSEC] Integrity checksum changed again (2nd time).	551	0	1.676%
COUNT BY PRIORITY	<input checked="" type="checkbox"/>	3	7	1	1		23:25:20						[OSSEC] Integrity checksum changed again (3rd time).	552	0	0.239%
high	-															
medium	-	2	7	1	1		23:24:27						[OSSEC] Integrity checksum changed.	550	0	0.160%
low	-															
10 (19.2%) other																
42 (80.8%)																

squert main screen

Snorby

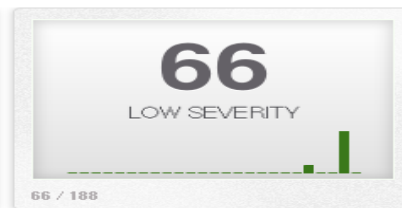
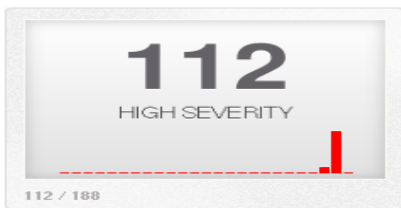
- Web front-end mostly for IDS data (snort)
- Allows for transcript creation
- Allows for classification of data
- Allows for pulling of full packet captures

Dashboard

 More Options

LAST 24 | TODAY | YESTERDAY | THIS WEEK | THIS MONTH | THIS QUARTER | THIS YEAR

Updated: 01/25/15 03:12 AM UTC



TOP 5 SENSOR

Solnx02-eth1:1 188

TOP 5 ACTIVE USERS

 Administrator 0

LAST 5 UNIQUE EVENTS

ET POLICY PE EXE or DLL W... 7

ET CURRENT_EVENTS Zbot Ge... 2

ET TROJAN Zbot POST Reque... 9

ET TROJAN Generic - POST ... 9

ET TROJAN GENERIC Likely ... 3

ANALYST CLASSIFIED EVENTS

Unauthorized Root Access 0

Unauthorized User Access 0

Attempted Unauthorized... 0

Denial of Service Attack 0

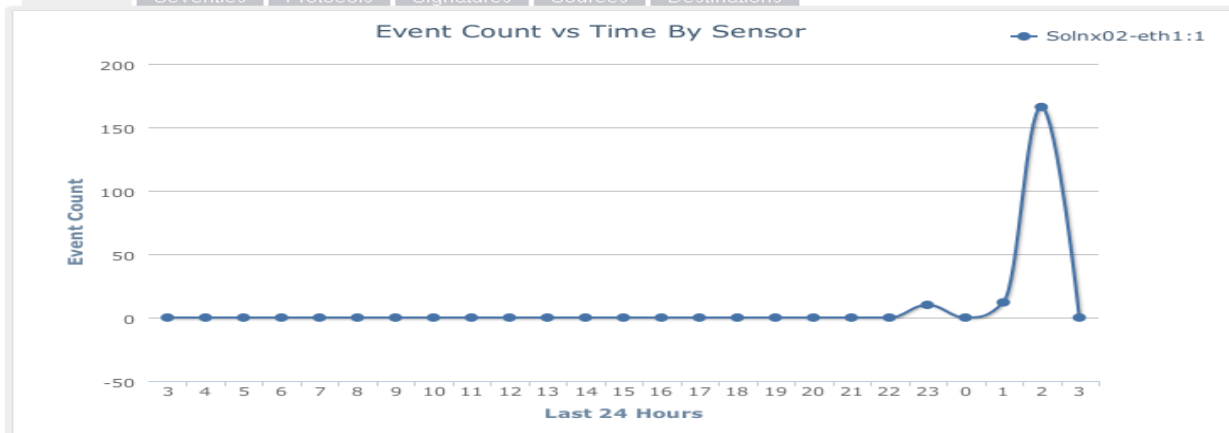
Policy Violation 0

Reconnaissance 0

Virus Infection 0

False Positive 0

Sensors | Severities | Protocols | Signatures | Sources | Destinations



snorby main screen

ELSA

- Web frontend for logs, includes bro logs
- Uses syslog-ng to collect remote events
- Uses mysql to store and query events
- If installed, then just double-click on the link
- Rapidly becoming one of my favorites
 - `https://<host or IP>:3154`
 - Accept SSL cert
- SO side panel has some pre-built queries

- ▼ [Connections](#)
- [Grouped by Node](#)
- [Top SRC IPs](#)
- [Top DST IPs](#)
- [Top DST Ports](#)
- [Top Services](#)
- [Port 53 groupby Service](#)
- [Port 80 groupby Service](#)
- [Port 443 groupby Service](#)
- [Groupby Resp Country](#)
- ▶ [DHCP](#)
- ▼ [DNS](#)
- [Top SRC IPs](#)
- [Top DST IPs](#)
- [Top Requests](#)
- [Top Responses](#)
- [Top nxdomain](#)
- [Zone Transfers](#)

Query [Submit Query](#) [Help](#)

From To [Add Term](#) [Index](#) Reuse current tab Grid display

class=BRO_DNS dstport="53" groupby:hostname (100) [Grouped by hostname] [×](#)

Result Options... ▼

Count ▼	Value
2052	docs.google.com
1336	(empty)
801	0.pfsense.pool.ntp.org
798	0.pfsense.pool.ntp.org.tcgmi.local
304	0.docs.google.com
229	0.drive.google.com
166	3.ubuntu.pool.ntp.org
166	ntp.ubuntu.com
158	2.ubuntu.pool.ntp.org
150	0.ubuntu.pool.ntp.org
150	1.ubuntu.pool.ntp.org
97	id.orig_p
78	drive.google.com
68	www.google.com
61	csi.gstatic.com

Elsa SO interface

Getting pcap data into SO

- Using tcpreplay
 - `sudo tcpreplay -i eth1 -t example.pcap`
- Allows you to run pcap files through all of the live action tools in SO.
- Only catch is, the timestamps on the packets are now system time.

Live Action of SO

Questions

<http://blog.securityonion.net/p/securityonion.html>