

Network Security Monitoring (NSM) Using



James Kirn

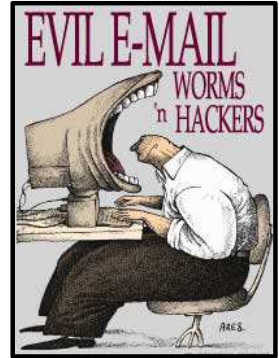
9/20/17

Based on Material from Doug Burks Presentation

2014_017_001_90218

Problem

- All our computers are inter-connected on a local LAN that ultimately connect out to the Internet (usually through a firewall/router).
- The Internet provides many useful services, but it also makes us vulnerable to various unknown malware (good/bad classification).
- Malware often enters our network without our knowing (network visibility).
- End point (host) solutions such as antivirus may miss malware delivery (necessary but not sufficient).



Value

Table 1: Breach Detection Gap Examples

Victim	Reported	Time to Discovery
Michaels Stores	Jan 2014	8 Months
Home Depot	Sept 2014	5 months
PF Chang's	July 2014	11 months ⁴
Sony	Nov 2014	~1 Year
Office of Personnel Management (OPM)	June 2015	~1 Year
Trump Hotels	Sept 2015	~1 Year
Undisclosed Mandiant client	2015	8.5 years



- What if you could see into your network and observe the transactions to better determine what might be malware?
- How do you find bad stuff on the network?
- What if you could stop intruders before they could do extensive damage to your computers/information?
- What if you had a time machine to go back in time to see what happened on your network?

Solution

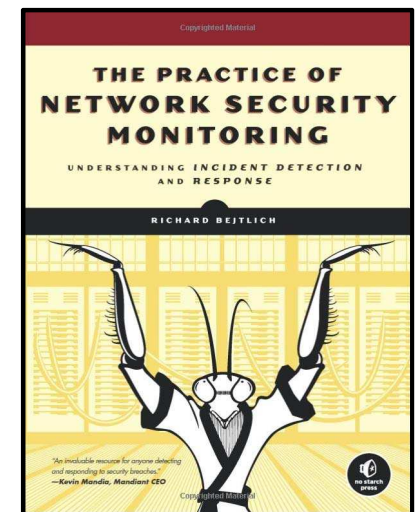
- A **Network Security Monitoring (NSM)** operation is designed to detect adversaries, respond to their activities, and contain them before they can accomplish their (evil) mission.

... (if) NSM doesn't stop adversaries, what's the point?

Time is the key factor in this strategy because intruders rarely execute their entire mission in the course of a few minutes, or even hours. In fact, the most sophisticated intruders seek to gain *persistence* in target networks— that is, hang around for months or years at a time.

---Richard Bejtlich, CSO Mandiant

2013

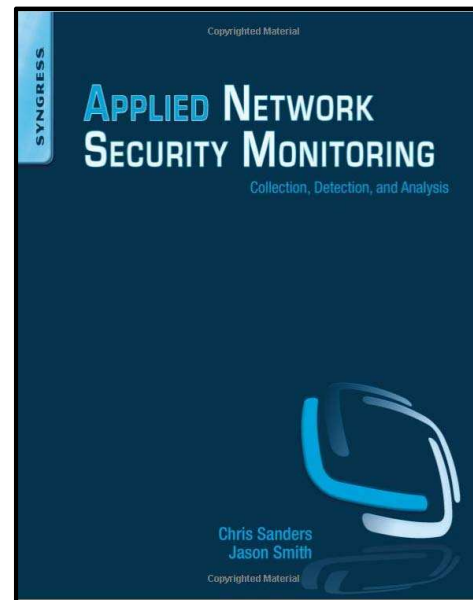


What is Security Onion ?

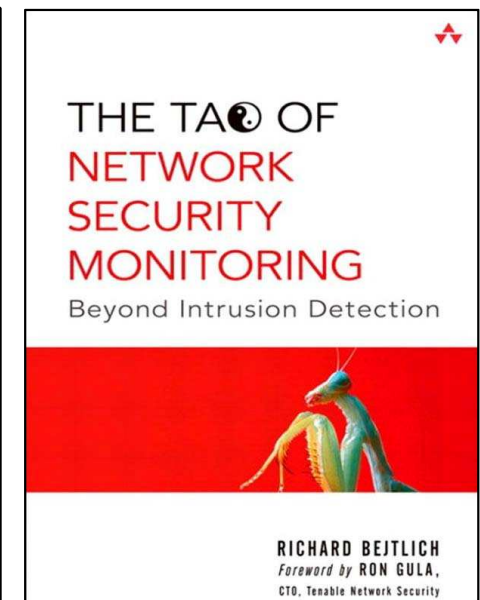
Security Onion is a **FREE** (Ubuntu based) Linux distro for:

- Intrusion Detection
- **Network Security Monitoring**
- Log Management

2014



2005



What Security Tools does SO contain?

Contains:

- Snort
- Suricata
- Bro
- OSSEC
- Sguil
- Squert
- ELSA
- NetworkMiner
- And many other security tools.



These tools will be shown later in the presentation.

What are the Deployment Scenarios?

There are the three Security Onion deployment scenarios:

1. Standalone
2. Sensor/Server
3. Hybrid

The Security Onion setup script allows you to easily configure the best installation scenario to suit your needs.

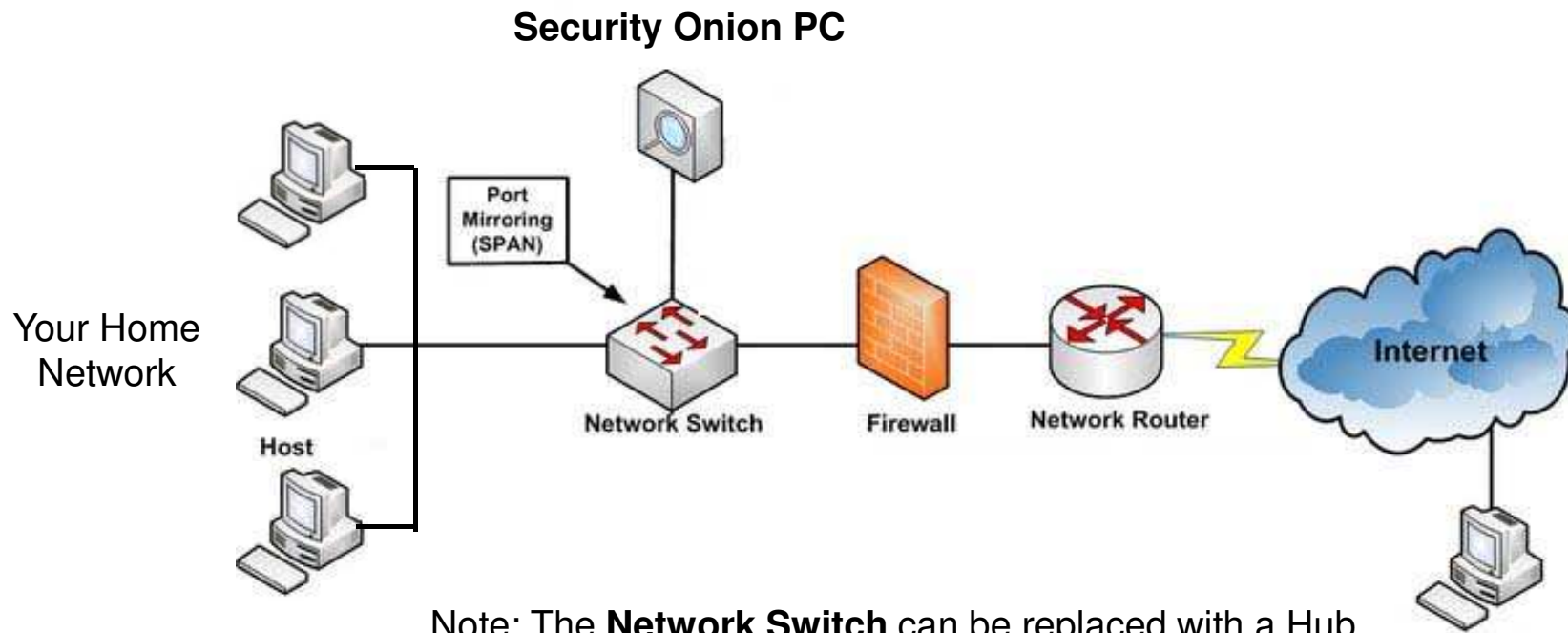
We will be using the Standalone deployment

What is SO's Hardware Requirements?

Assuming a Home based Standalone Install:

- 64 bit Intel based CPU
- At least a 2 core CPU
- RAM – 3 Gigabytes min (more is better)
- Storage – LOTS - it depends on how busy your network is and how much data you want saved. 500 GB would be nice (see web site for calculation)
- Two 1Gbit NICs – one for traffic monitor, one for user management interface
- Some form of Network Tap:
 - ✓ Ethernet switch with Port Mirroring (SPAN port) (this is what I use)
 - ✓ Web site has recommendations for Enterprise Tap Solutions
 - ✓ Hub (slow, but it works)
- Can be a VM

Network Diagram



Note: The **Network Switch** can be replaced with a Hub, but Hubs don't operate a 1 GB.

What Data Does SO Give You?

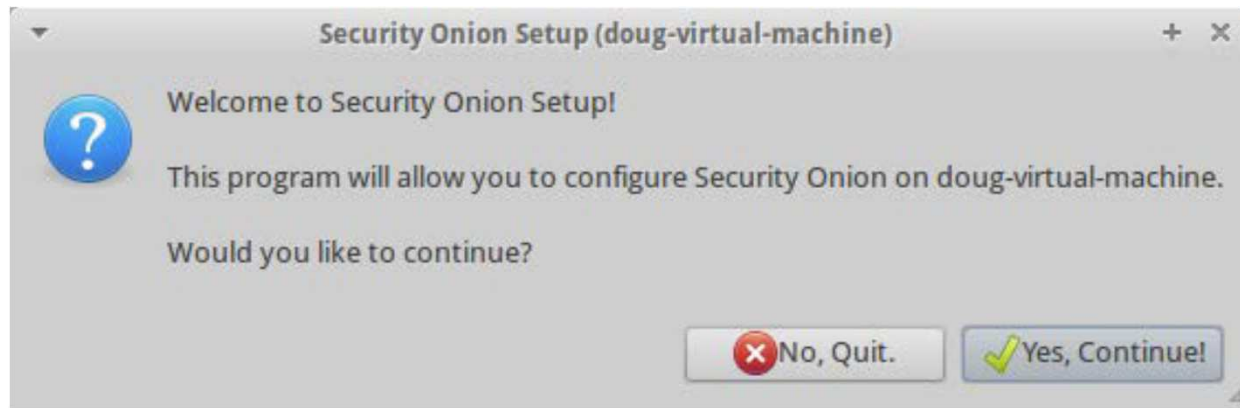
- *Flow Data* from **Argus**, **Bro**, and **PRADS**
- *Alert Data*
 - ✓ **NIDS** alerts from **Snort/Suricata**
 - ✓ **HIDS** alerts from **OSSEC**
- *Syslog Data* received by **syslog-ng** or sniffed by **Bro**
- *Asset Data* from **Bro** and **PRADS**
- *Transaction Data* – HTTP/FTP/DNS/SSL/+Other logs from **Bro**
- *Full Content Data* from **netsniff-ng**

Does SO Scale?

- Big Onions – 64-bit
- Big Traffic – PF_RING
- Big Data – ELSA

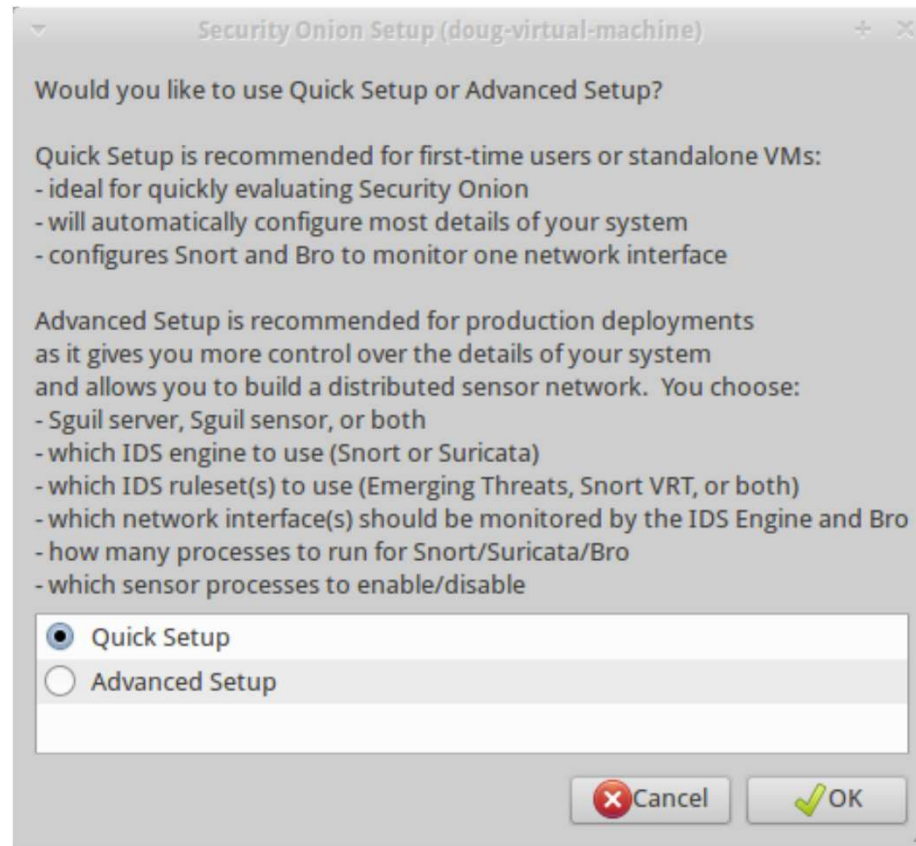


What does SO Look Like?



Answer a Few Simple Questions...

(not all shown - Demo Later)



Snorby

SPONSORED BY **threat stack**
<https://threatstack.com>

Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard My Queue (0) Events Sensors Search Administration

Dashboard

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR Updated: 01/11/14 04:47 PM UTC

396
HIGH SEVERITY
396 / 514

46
MEDIUM SEVERITY
46 / 514

72
LOW SEVERITY
72 / 514

Sensors Severities Protocols Signatures Sources Destinations

Signature	Percentage
ET TROJAN Backdoor family PCRa...	59%
ET INFO EXE - Served Inline HT...	14%
ET SCAN Potential VNC Scan 590...	3%
ET TROJAN Java EXE Download by...	3%
ET POLICY Java EXE Download...	3%
ET POLICY PE EXE or DLL Window...	2%
ET INFO JAVA - Java Archive Do...	2%
GPL SHELLCODE x86 inc ebx NOOP...	2%
ET SCAN Potential VNC Scan 580...	1%
ET POLICY Suspicious inbound t...	1%
ET POLICY Suspicious inbound t...	1%
ET POLICY Suspicious inbound t...	1%
ET POLICY Suspicious inbound t...	1%
ET WEB_CLIENT Possible Intern...	1%
ET POLICY Suspicious inbound t...	1%
ET SHELLCODE Javascript Split ...	1%
ET SHELLCODE Possible Call wt...	1%
ET CURRENT_EVENTS HiMan EK - L...	0%
ET POLICY Vulnerable Java Vers...	0%
ET SCAN Potential SSH Scan OUT...	0%

TOP 5 SENSOR

doug-virtual-machine-eth1:1	514
-----------------------------	-----

TOP 5 ACTIVE USERS

Administrator	0
---------------	---

LAST 5 UNIQUE EVENTS

ET POLICY PE EXE or DLL W...	11
GPL SHELLCODE x86 inc ebx...	10
ET SHELLCODE Possible Cal...	3
ET INFO Exectuable Downlo...	1
ET POLICY SUSPICIOUS *.do...	1

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

Pivot to PCAP from Snorby

The screenshot displays the Snorby web interface. At the top, it says 'Sponsored by threat stack' and 'Welcome Administrator | Settings | Log out'. The navigation bar includes 'Dashboard', 'My Queue (0)', 'Events', 'Sensors', 'Search', and 'Administration'. The main content area is titled 'Listing Sessions (2 unique unclassified sessions)'. It contains a table with the following data:

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions
1	doug-virtual-	172.16.150.20	66.32.119.38	ET INFO Executable Download from dotted-quad Host	4:16 PM	1
2	doug-virtual-	172.16.150.20	66.32.119.38	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL	4:16 PM	1

Below the table, there are several tabs: 'View All Sessions', 'Perform Mass Classification', 'Packet Capture Options', 'Event Export Options', and 'Permalink'. The 'Packet Capture Options' tab is active, and a 'Packet Capture Builder' dialog box is open. The dialog contains the following fields:

- Source address (Source Address : Source Port): 172.16.150.20 : 1294
- Destination address (Destination Address : Destination Port): 66.32.119.38 : 80
- Protocol: TCP
- Start time (default is 30 minutes before the event start time): 2014 January 11 15:46
- End time (default is 30 minutes after the event end time): 2014 January 11 16:46

At the bottom of the dialog, there are two buttons: 'Fetch Packet' (green) and 'Cancel' (red).

Pivot to CapMe to view Packet Contents

```
172.16.150.20:1294_66.32.119.38:80-6-1456675353.pcap
Sensor Name: doug-virtual-machine-eth1
Timestamp: 2014-01-11 16:16:39
Connection ID: CLI
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1294
Dst Port: 80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

SRC: GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda04a8ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.....@.....!L!This program cannot be run in DOS mode.
DST:
DST: $.n..n..n.wq..n..N..n.Rich.n.....PE..L...G.....@.....<.....(.....
.....text..h.....`data..`.....@.....L.....@..j....%..@.D.....Z.....L.....ExitProcess.kernel32.dll
```


Squert Web Interface

The screenshot displays the Squert web interface with the following components:

- Header:** Welcome doug | Logout | comments | sensors | filters
- Calendar:** Navigation for 2013 and 2014, with a timeline from 00:00 to 23:00.
- Left Sidebar (Tools):**
 - Event Grouping: on
 - Event Queue Only: on
 - Map: on
 - Event Summary:**
 - Queued Events: 545
 - Total Events: 736
 - Total Signatures: 35
 - Total Sources: -
 - Total Destinations: -
 - Event Count by Priority:**
 - High: 356 (3.2%)
 - Medium: 46 (0.2%)
 - Low: 72 (1.1%)
 - Other: 50 (0.3%)
 - Event Count by Classification:**
 - Admin Access: -
 - User Access: -
 - Attempted Access: -
 - Denial of Service: -
 - Policy Violation: -
 - Reconnaissance: -
 - Malware: -
 - No Action Req'd: 191 (25.2%)
 - Escalated Event: -
 - History:** 172.16.150.20 | 66.32.119.38
- Main Content Area:**
 - Map:** A world map with the United States highlighted in dark grey.
 - Alert Details:**

16:16:39 ET POLICY SUSPICIOUS *.doc.exe in HTTP URL 2013475 6 0.132%

alert top \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET POLICY SUSPICIOUS *.doc.exe in HTTP URL"; flow.to_server,established; content:".doc.exe"; http_uri; nocase; classtype:bad-unknown; sid:2013475; rev:1;)

file: downloaded.rules:10836
categorize: 0 event(s)
 - Event Table:**

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
1		2014-01-11 16:16:39	172.16.150.20	RFC1918 (RS)	66.32.119.38	UNITED STATES (.us)
 - Signature Details:**

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE	
RT	2014-01-11 16:16:39	3.512	TX	172.16.150.20	1294	66.32.119.38	80	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL
 - Sensor Information:**

Sensor Name: doug-virtual-machine-eth1-1
Timestamp: 2014-01-11 16:16:39
Connection ID: CLI
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1294
Dst Port: 80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seidom 98)
OS Fingerprint -> 66.32.119.38:80 (distance 0, link: ethernet/modem)
 - Request Details:**

SRC: GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-bitmap, image/jpeg, image/pipe, application/x-shockwave-flash, */*
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda04a8ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.....@.....!..L.This program cannot be run in DOS mode.
DST:
DST: \$.....n..n..wq..n..N..n..Rich.n.....PE.L...G.....
DST: ..text..n.....data.....@...L...@...%..@.D..Z.....L.....ExitProcess.kerne32.dll
 - Summary:** 2012088 6 0.397%

Sguil Client



RT	11	doug-...	3.431	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1064	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
RT	2	doug-...	3.442	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1066	6	ET POLICY PE EXE or DLL Windows file download
RT	27	doug-...	3.444	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1067	6	ET INFO EXE - Served Inline HTTP
RT	14	doug-...	3.458	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1067	6	ET POLICY Java EXE Download
RT	14	doug-...	3.472	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1067	6	ET TROJAN Java EXE Download by Vulnerable Version - Likely Driveby
RT	1	doug-...	3.499	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
RT	1	doug-...	3.500	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET TROJAN SpyEye Bot Checkin
RT	1	doug-...	3.501	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET TROJAN SpyEye C&C Check-in URI
RT	1	doug-...	3.502	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET TROJAN Banker PWS/Infostealer HTTP GET Checkin
RT	2	doug-...	3.503	2014-01-11 16:16:37	10.10.10.10	4444	10.10.10.70	1036	6	ET POLICY PE EXE or DLL Windows file download
RT	4	doug-...	3.504	2014-01-11 16:16:37	10.10.10.10	4444	10.10.10.70	1036	6	ET SHELLCODE Possible Call with No Offset TCP Shellcode
RT	2	doug-...	3.505	2014-01-11 16:16:37	10.10.10.10	4444	10.10.10.70	1036	6	GPL SHELLCODE x86 inc ebx NOOP
RT	1	doug-...	3.511	2014-01-11 16:16:39	172.16.150.20	1294	66.32.119.38	80	6	ET INFO Executable Download from dotted-quad Host
RT	1	doug-...	3.512	2014-01-11 16:16:39	172.16.150.20	1294	66.32.119.38	80	6	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL
RT	1	doug-...	3.513	2014-01-11 16:16:39	66.32.119.38	80	172.16.150.20	1294	6	ET POLICY PE EXE or DLL Windows file download
RT	1	doug-...	3.514	2014-01-11 16:16:39	66.32.119.38	80	172.16.150.20	1294	6	ET SHELLCODE Possible Call with No Offset TCP Shellcode

IP Resolution
Agent Status
Snort Statistics
System Msgs
User Msgs

Reverse DNS
 Enable External DNS

Src IP: 172.16.150.20

Src Name: Unknown

Dst IP: 66.32.119.38

Dst Name: static-66-32-119-38.earthlinkbusiness.net

Whois Query: None Src IP Dst IP

#

NetRange: 66.32.0.0 - 66.32.255.255

CIDR: 66.32.0.0/16

OriginAS:

Show Packet Data
 Show Rule

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET POLICY SUSPICIOUS *.doc.exe in HTTP URL"; flow:to_server,established; content:".doc.exe"; http_uri; nocase; classtype:bad-unknown; sid:2013475; rev:1;)

/nsm/server_data/securityonion/rules/doug-virtual-machine-eth1-1/downloaded.rules: Line 10836

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum						
	172.16.150.20	66.32.119.38	4	5	0	378	8716	2	0	128	56326						
TCP	Source Port	Dest Port	R	R	U	A	P	R	S	F							
	1294	80	.	.	.	X	X	.	.	.							
	47	45	54	20	2F	74	69	67	65	72	73	2F	42	72	61	6E	
	64	6F	6E	49	6E	67	65	2F	44	69	61	67	6E	6F	73	74	
	69	63	73	2F	73	77	69	6F	67	2D	6D	65	63	68	61	6F	

Pivot to PCAP from Sguil

doug-virtual-machine-eth1-1_512

File

Sensor Name: doug-virtual-machine-eth1-1
Timestamp: 2014-01-11 16:16:39
Connection ID: .doug-virtual-machine-eth1-1_512
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1294
Dst Port: 80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint: -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

SRC: GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash/*/*
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda04a8ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program

Search Abort Close

Debug Messages

Using archived data:
/nsm/server_data/securityonion/archive/2014-01-11/doug-virtual-machine-eth1-1/172.16.150.20_4.66.32.119.38:80-6.raw
Finished.



172.16.150.20:1294.66.32.119.38:80-6.raw [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.150.20	66.32.119.38	TCP	62	1294 > 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.000272	66.32.119.38	172.16.150.20	TCP	62	80 > 1294 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.000412	172.16.150.20	66.32.119.38	TCP	60	1294 > 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.000923	172.16.150.20	66.32.119.38	HTTP	392	GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
5	0.001160	66.32.119.38	172.16.150.20	TCP	54	80 > 1294 [ACK] Seq=1 Ack=339 Win=6432 Len=0
6	0.002683	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
7	0.003868	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
8	0.005282	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
9	0.005378	172.16.150.20	66.32.119.38	TCP	60	1294 > 80 [ACK] Seq=339 Ack=2921 Win=17520 Len=0
10	0.005461	172.16.150.20	66.32.119.38	TCP	60	1294 > 80 [ACK] Seq=339 Ack=4381 Win=17520 Len=0
11	0.006818	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
12	0.008442	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
13	0.009597	66.32.119.38	172.16.150.20	HTTP	1258	HTTP/1.1 200 OK (application/x-msdos-program)

▶ Frame 4: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits)

▶ Ethernet II, Src: 00:0c:29:61:e7:d5 (00:0c:29:61:e7:d5), Dst: 00:0c:29:5d:b3:ca (00:0c:29:5d:b3:ca)

▶ Internet Protocol Version 4, Src: 172.16.150.20 (172.16.150.20), Dst: 66.32.119.38 (66.32.119.38)

▶ Transmission Control Protocol, Src Port: 1294 (1294), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 338

▶ Hypertext Transfer Protocol

```
0000 00 0c 29 5d b3 ca 00 0c 29 61 e7 d5 08 00 45 00 ..)]....)a...E.
0010 01 7a 22 0c 40 00 80 06 dc 06 ac 10 96 14 42 20 .z".@... ..B
0020 77 26 05 0e 00 50 99 76 be c8 39 be ce e4 50 18 w&...P.v .9...P.
0030 44 70 7b cf 00 00 47 45 54 20 2f 74 69 67 65 72 Dp{...GE T /tiger
0040 73 2f 42 72 61 6e 64 6f 6e 49 6e 67 65 2f 44 69 s/Brando nInge/Di
0050 61 67 6e 6f 73 74 69 63 73 2f 73 77 69 6e 67 2d agnostic s/swing-
0060 6d 65 63 68 61 6e 69 63 73 2e 64 6f 63 2e 65 78 mechanic s.doc.ex
0070 65 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 e HTTP/1 .1..Acce
0080 70 74 3a 20 69 6d 61 67 65 2f 67 69 66 2c 20 69 pt: imag e/gif, i
0090 6d 61 67 65 2f 78 2d 78 62 69 74 6d 61 70 2c 20 mage/x-x bimap,
```

File: /tmp/172.16.150.20:1294.66.32.119.38:80-6.raw Packets: 18 Displayed: 18 Marked: 0 Load time: 0:00.000 Profile: Default

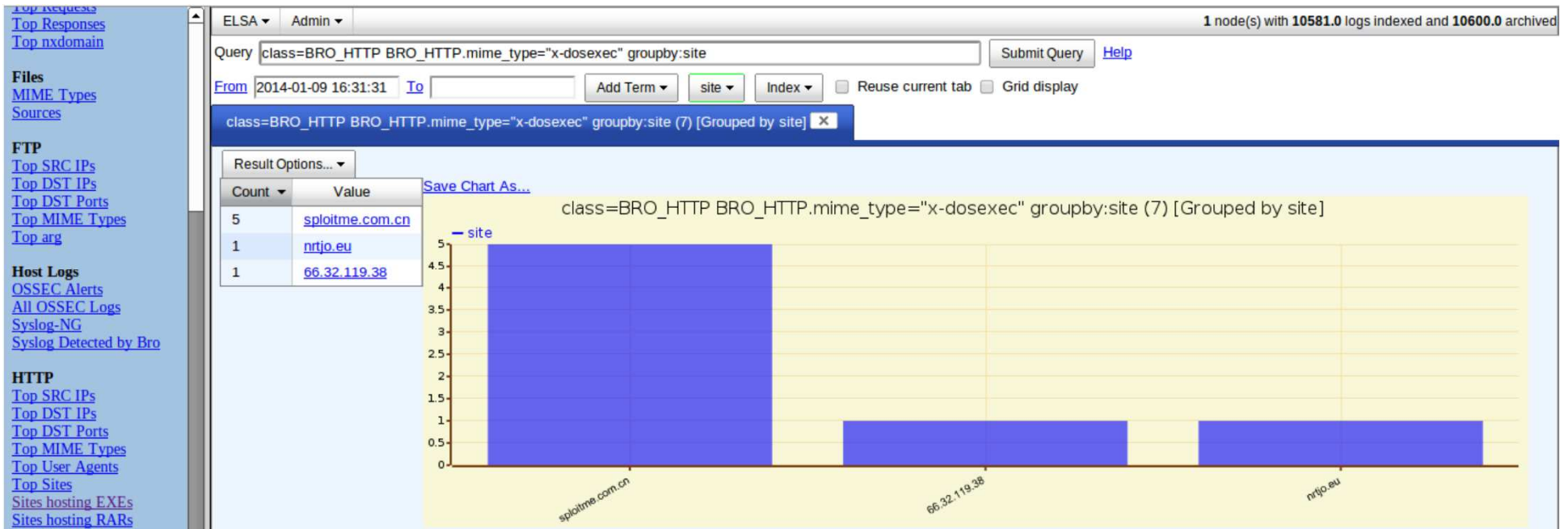
Network Miner



The screenshot displays the NetworkMiner 1.5 application window. The main pane shows a tree view of discovered hosts. The host 172.16.150.20 (Windows) is selected and expanded, showing details such as IP, MAC, OS, TTL, and network statistics. A Case Panel on the right shows a file named '172.16... a6ca...'. Below the main window, a smaller screenshot shows the 'Reconstructed file path' table.

Fram...	Reconstructed file path	Source host	S. port	Destination host	D. port	Protocol	File...	Exten...	Size	Time
4	/opt/networkminer/AssembledFiles/66.32.119.38/HTTP - TCP 80/tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe...	66.32.119.38...	TCP 80	172.16.150.20...	TCP 1294	HttpG...	swing...	x-msd...	8 192 B	1/11/...

ELSA (Enterprise Log Search and Archive)



Pivot to PCAP from ELSA

The screenshot shows the ELSA web interface. At the top, it indicates '1 node(s) with 10586.0 logs indexed and 10606.0 archived'. The search query is 'class=BRO_HTTP "-" site="rapidshare.com.eyu32.ru"'. The results are grouped by site, showing 19 records. The interface includes a sidebar with navigation links for various log types and a main content area displaying a table of log entries. A 'Log Info' popup window is open over the first record, showing details like 'Summary', 'Links', and 'Plugins', with 'getPcap' highlighted as a plugin option.

Info	Timestamp	Fields
Info	Sat Jan 11 16:16:30	1389456989.259525 CideK21NWLaf4Ddssj 10.0.2.15 1063 192.168.56.50 80 1 GET rapidshare.com.eyu32.ru/login.php Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Firefox/3.5.3 0 3005 200 OK ... text/html
Info	Sat Jan 11 16:16:30	1389456989.262719 CideK21NWLaf4Ddssj 10.0.2.15 1063 192.168.56.50 80 2 GET rapidshare.com.eyu32.ru/images/sslstyles.css http://rapidshare.com.eyu32.ru/login.php Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 0 304 Not Modified ... text/html
Info	Sat Jan 11 16:16:30	1389456989.263647 CideK21NWLaf4Ddssj 10.0.2.15 1063 192.168.56.50 80 3 GET rapidshare.com.eyu32.ru/images/images/dot.jpg http://rapidshare.com.eyu32.ru/images/sslstyles.Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 0 347 404 Not Found ... text/html
Info	Sat Jan 11 16:16:30	1389456989.265883 CideK21NWLaf4Ddssj 10.0.2.15 1063 192.168.56.50 80 4 GET rapidshare.com.eyu32.ru/images/rslogo.jpg http://rapidshare.com.eyu32.ru/login.php Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 0 359 404 Not Found ... text/html
Info	Sat Jan 11 16:16:30	1389456989.268045 CJQbug4UwLkPc1kgz 10.0.2.15 1063 192.168.56.50 80 5 GET rapidshare.com.eyu32.ru/images/images/terminator_back.png http://rapidshare.com.eyu32.ru/images/images/terminator_back.png Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 0 359 404 Not Found ... text/html
Info	Sat Jan 11 16:16:30	1389456989.268552 CXMkh151JDizQuzwb 10.0.2.15 1063 192.168.56.50 80 6 GET rapidshare.com.eyu32.ru/images/images/terminator_back.png http://rapidshare.com.eyu32.ru/images/images/terminator_back.png Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 0 359 404 Not Found ... text/html

Install Example

- <https://github.com/Security-Onion-Solutions/security-onion/releases/download/v14.04.5.2/securityonion-14.04.5.2.iso>
- On-line Example:
- <http://blog.securityonion.net/2016/01/security-onion-140431-screenshot-tour.html>

Security Onion – Running Demo

- VPN into KirnNet (Cisco SSL VPN)
- Demo - SO Install on KirnNet vSphere System (about 25 min)
 - 0:00 - Start SO VM Creation
 - 7:30 - File Copies started
 - 10:00 - until Download Complete
 - 12:45 - until Install Complete
 - 15:00 - Security Onion Running – ready for Configuration
 - 17:00 - Reboot after Network Config
 - 20:00 - Configuration
 - 25:00 – Done
- Demo – View Active SO running on KirnNet (about 10 min)

References

- Bro Network Security Monitor (<https://www.bro.org/>)
- ELSA - Enterprise Log Search and Archive (<https://github.com/mcholste/elsa>)
- NetworkMiner (<http://www.netresec.com/?page=NetworkMiner>)
- Netsniff-ng (<http://netsniff-ng.org/>)
- OSSEC (Open Source HIDS SECurity) (<https://ossec.github.io/>)
- Security Onions (<http://blog.securityonion.net/>)
- Sguil (Analyst Console for NSM) (<http://bammv.github.io/sguil/index.html>)
- Snorby (<https://github.com/Snorby/snorby.org>)
- Snort (<http://snort.org/>)
- Squert (<http://www.squertproject.org/>)
- Suricata (<http://suricata-ids.org/>)
- PRADS - Passive Real-time Asset Detection System
(<https://github.com/gamelin/prads>)
- Wireshark/Tshark – (<https://www.wireshark.org/>)

Next Steps

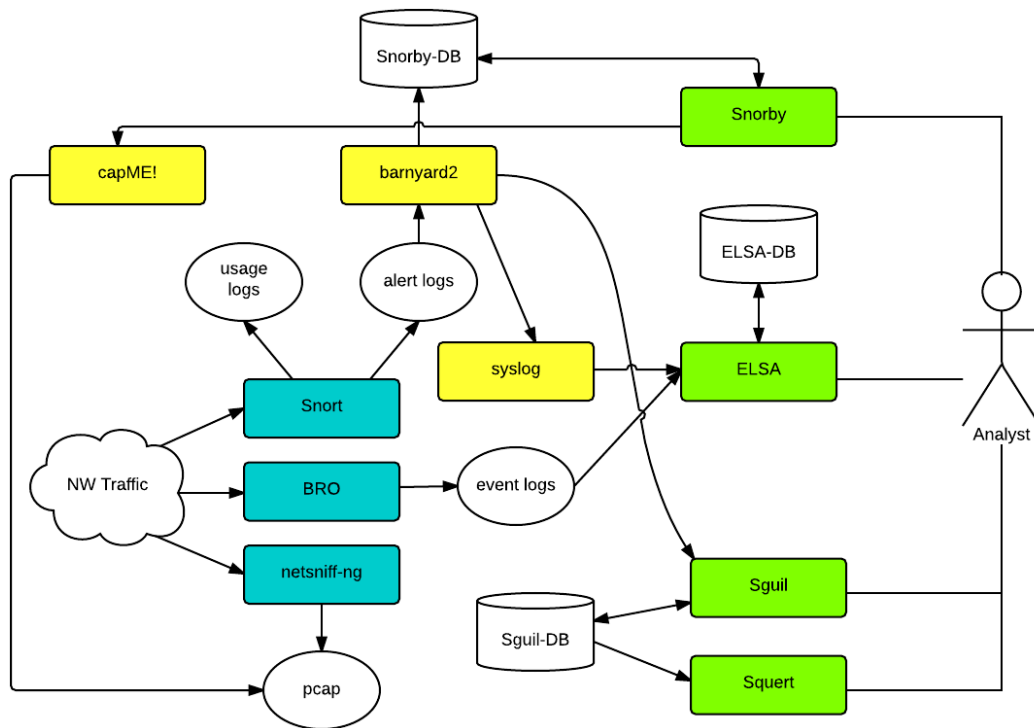
- Download and Install SO on Your System
 - <https://github.com/Security-Onion-Solutions/security-onion/releases/download/v14.04.5.2/securityonion-14.04.5.2.iso>
- Monitor your Network(s)
 - Install it as a Virtual box VM?
 - <http://www.deepimpact.io/blog/installingsecurityoniononvirtualbox>
- Download Chris Sanders - SO Cheat Sheet
 - <https://chrissanders.org/SO-CheatSheet.pdf>
- Follow Security Onion web site for updates
 - <https://securityonion.net/>
- Review the 2017 Security Onion conference presentations?
 - <https://www.youtube.com/playlist?list=PLIjFITO9rB15jhnSfR6shBEskTgGbta2k>

EXTRA CREDIT – A Look Under the Hood



North West Chicagoland Linux User Group (NWCLUG) -10.2017

How Does SO Work?



Blue Boxes – traffic capturing/analysis programs
Green Boxes – user interfaces
Yellow boxes – “intermediate” programs
Circles – data formats
Cylinders – databases

Source: <https://truica-victor.com/security-onion-traffic-to-analyst/>

SO - User Interfaces

- **ELSA** - is a three-tier log receiver, archiver, indexer, and web frontend for incoming syslog (data). It leverages *syslog-ng's pattern-db* parser for efficient log normalization and *Sphinx* full-text indexing for log searching
- **Snorby** – is a web interface built in ruby on rails that shows a nice overview of Snort alerts.
- **Sguil** - is a GUI that provides access to real-time events, session data, and raw packet captures
- **Squert** - is a web application that is used to query and view event data stored in a Sguil database (typically IDS alert data)

SO - Traffic Capturing/Analysis

- **SNORT** –
 - ✓ An open source network-based intrusion detection system (NIDS) that performs real-time traffic analysis and packet logging on IP networks.
 - ✓ In SO, SNORT is set to intrusion detection mode where the program will monitor network traffic and analyze it against rule sets and generate alerts based on those rules.
- **BRO** - processes the network traffic and outputs the result into a set of log files (*/nsm/bro/logs/current/TYPE.log*)
- **netsiff-ng** - is a performant Linux networking toolkit that uses zero-copy mechanisms, so that on packet reception and transmission the kernel does not need to copy packets from kernel space to user space and vice versa.

SO - Intermediate Processors

- **CapME** - is a web interface that allows you to:
 - ✓ view a pcap transcript rendered with tcpflow
 - ✓ view a pcap transcript rendered with Bro (especially helpful for dealing with gzip encoding)
 - ✓ download a pcap
- **Barnyard2** - is an open source-based parsing program designed to retrieve logs written by Snort or Suricata in the *Unified2* format and convert and write them to a database (Snort, MySQL, syslog, etc.).
- **Syslog(-ng)** - collects, parses, classifies, and correlates logs from numerous sources and stores or routes them to log analysis tools.

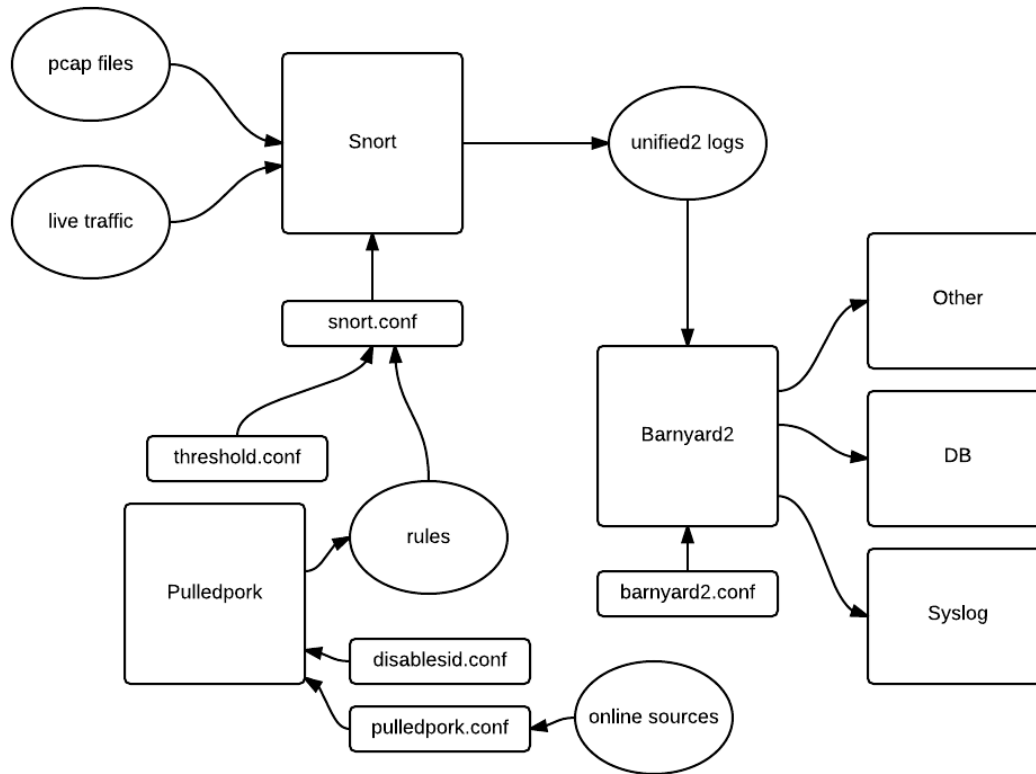
SNORT – Under the Hood



- The purpose of Snort in Security Onion is to provide IDS data and alerts which will be analyzed by the user in one of the user-interfaces available.
- Searches network traffic for pattern matches using rules
- Rules files are updated daily via *Pulledpork*
 - ✓ **Subscription (\$)** - Up-to-date VRT rules available immediately to subscribers
 - ✓ **Registered** - VRT rules freely available to registered users after 30 days
 - ✓ **Community** - rules under GPL. They are a subset of the VRT rules.
 - ✓ **Third-party** rule sets available.
- Uses *Barnyard2* to retrieve logs and place them into databases or other systems



SNORT – Architecture



Source: <https://truica-victor.com/snort-alerts-passing-onion/>

BRO / ELSA



- **Bro** monitors your network traffic and creates event logs, such as:
 - **conn.log**
 - **dhcp.log**
 - **dns.log**
 - **ftp.log**
 - **http.log**
 - **ssl.log**
 - **notice.log**
 - **files.log**
 - **Others...** (see <https://chrissanders.org/SO-CheatSheet.pdf>)
- These logs are linked to **ELSA** where the user can easily perform complex searches

Low Cost SPAN Port (1)

Netgear ProSAFE GS108Ev3 8-Port Gigabit Plus Switch

- (GS108E-300NAS)
- Does port mirroring
- <https://www.newegg.com/Product/Product.aspx?Item=12K-008X-00022>



- <https://www.netgear.com/business/products/switches/web-managed/GS108E.aspx#tab-resources>

Low Cost SPAN Port (2)

- **You'll need a switch capable of port mirroring.** If you do not have this, there's pretty cheap ways to obtain one.
- You can pick up a used Cisco managed switches on Craigslist for next to nothing.

Source:

<https://toastersecurity.blogspot.com/2016/10/setting-up-security-onion-to-enhance.html>



ANY QUESTIONS?