Network Security Monitoring (NSM) Using

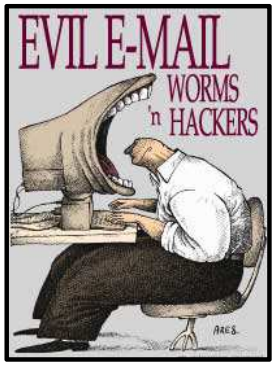
James Kirn

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

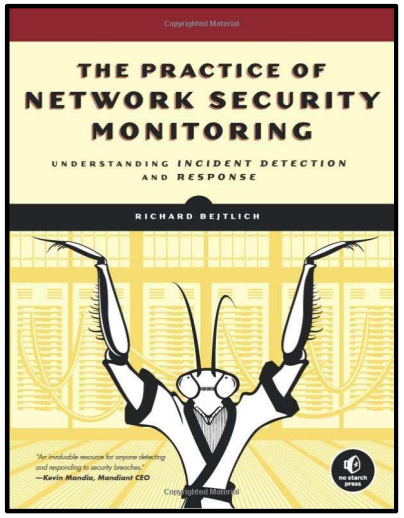
- A **Network Security Monitoring** (**NSM**) operation is designed to detect adversaries, respond to their activities, and contain them before they can accomplish their (evil) mission.

… (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

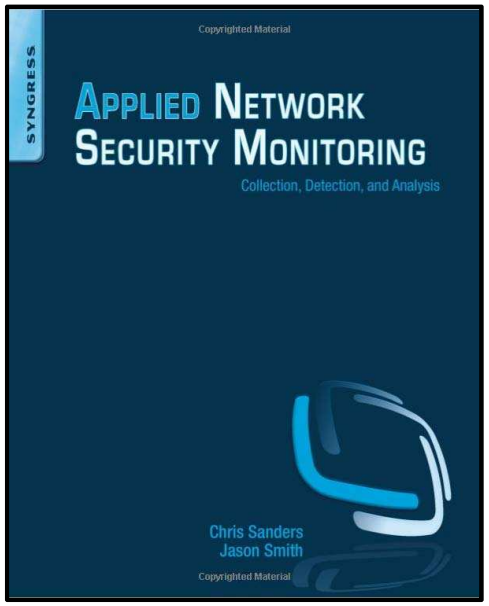


What is Security Onion ?

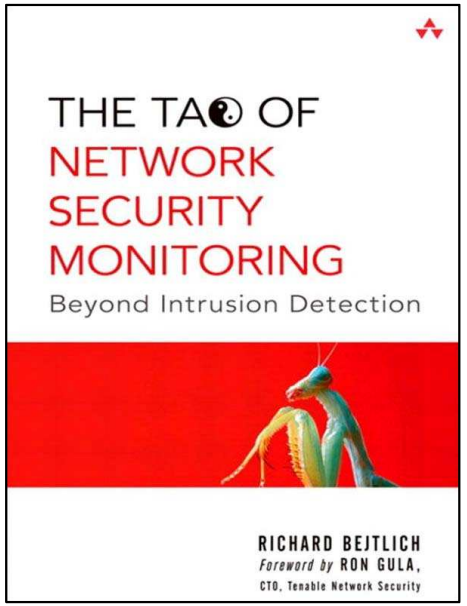
Security Onion is a **FREE** (Ubuntu based) Linux distro for:

- 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.

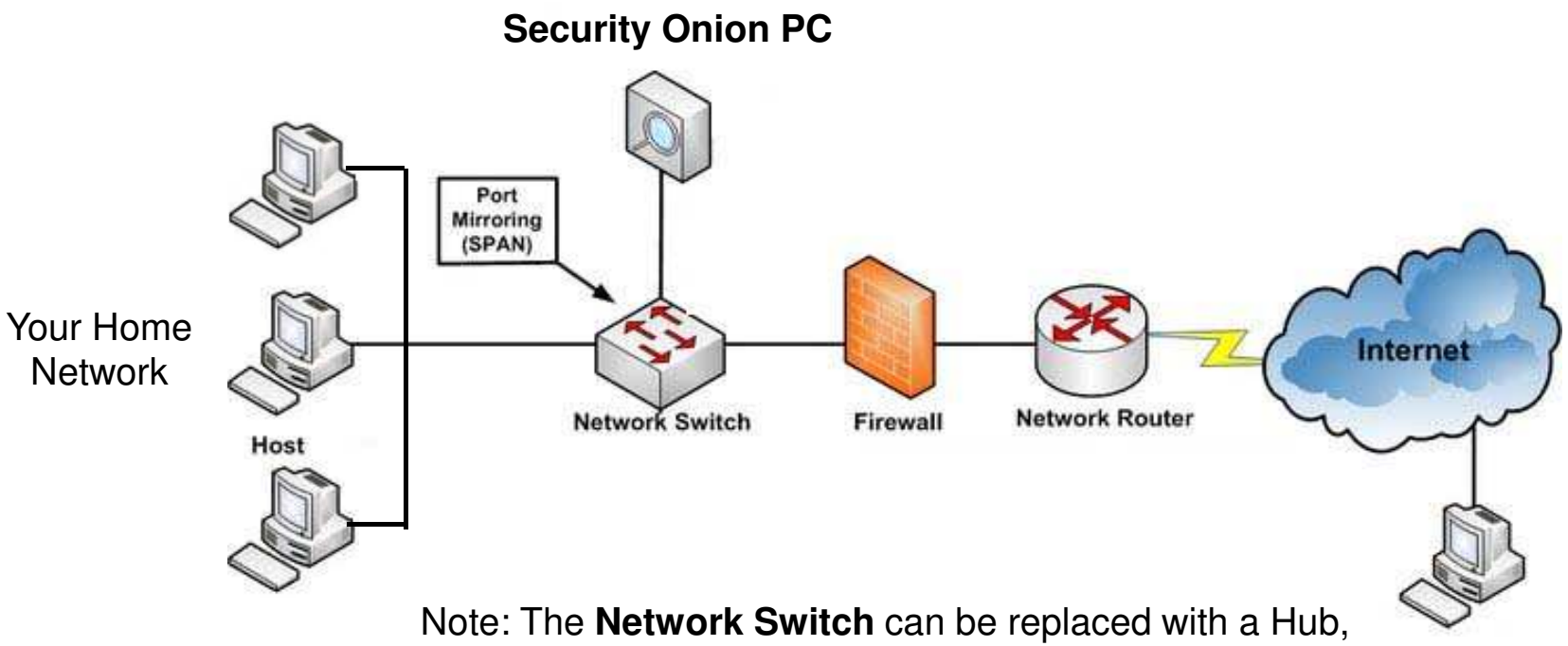
We will be using the Standalone deployment

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.

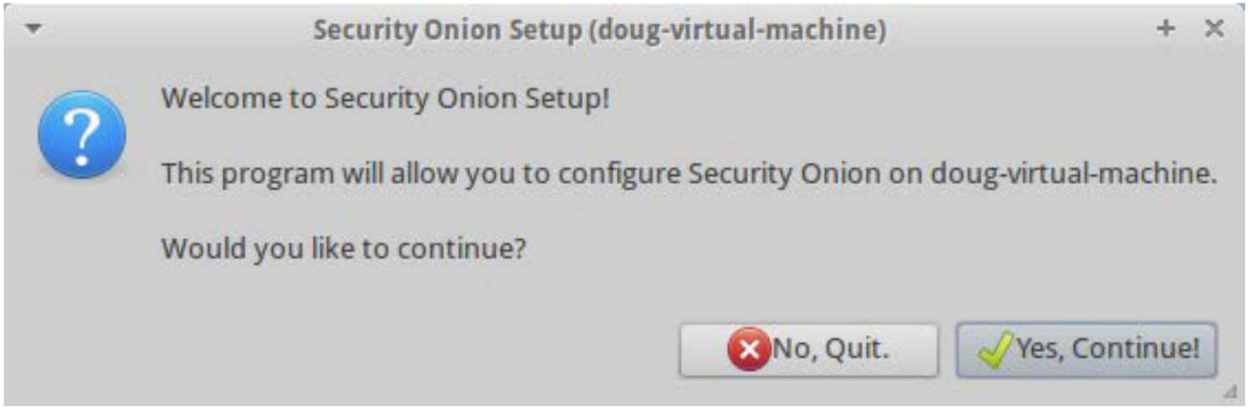
What Data Does SO Give You?

- *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**

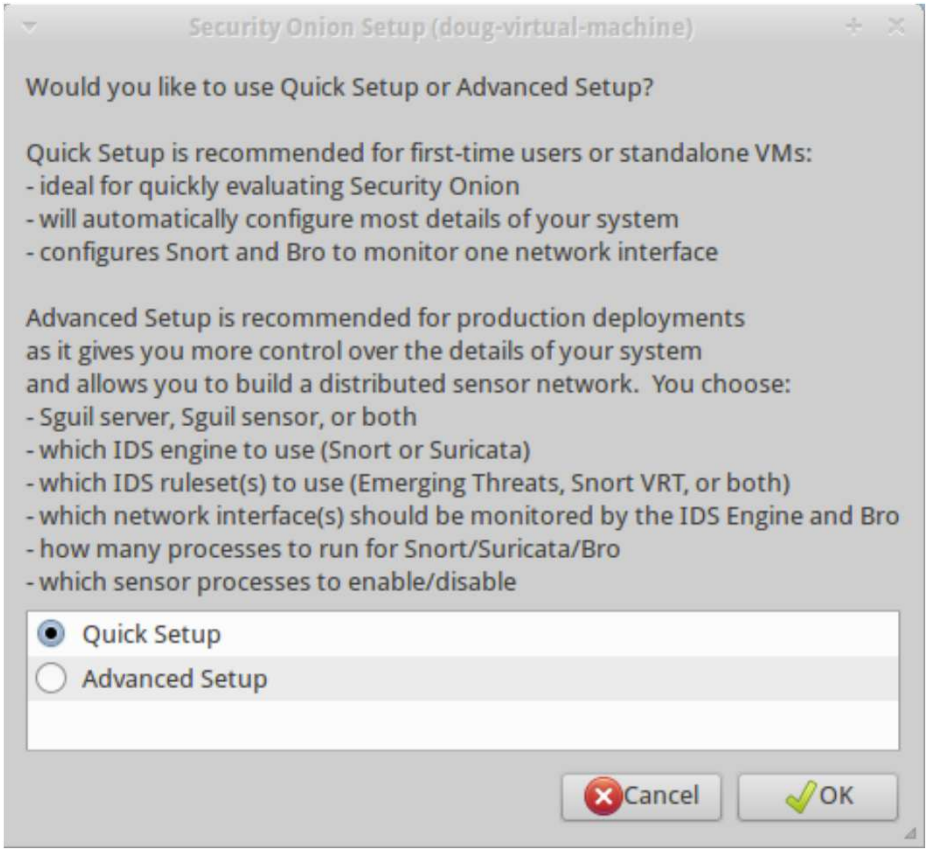
Does SO Scale?

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

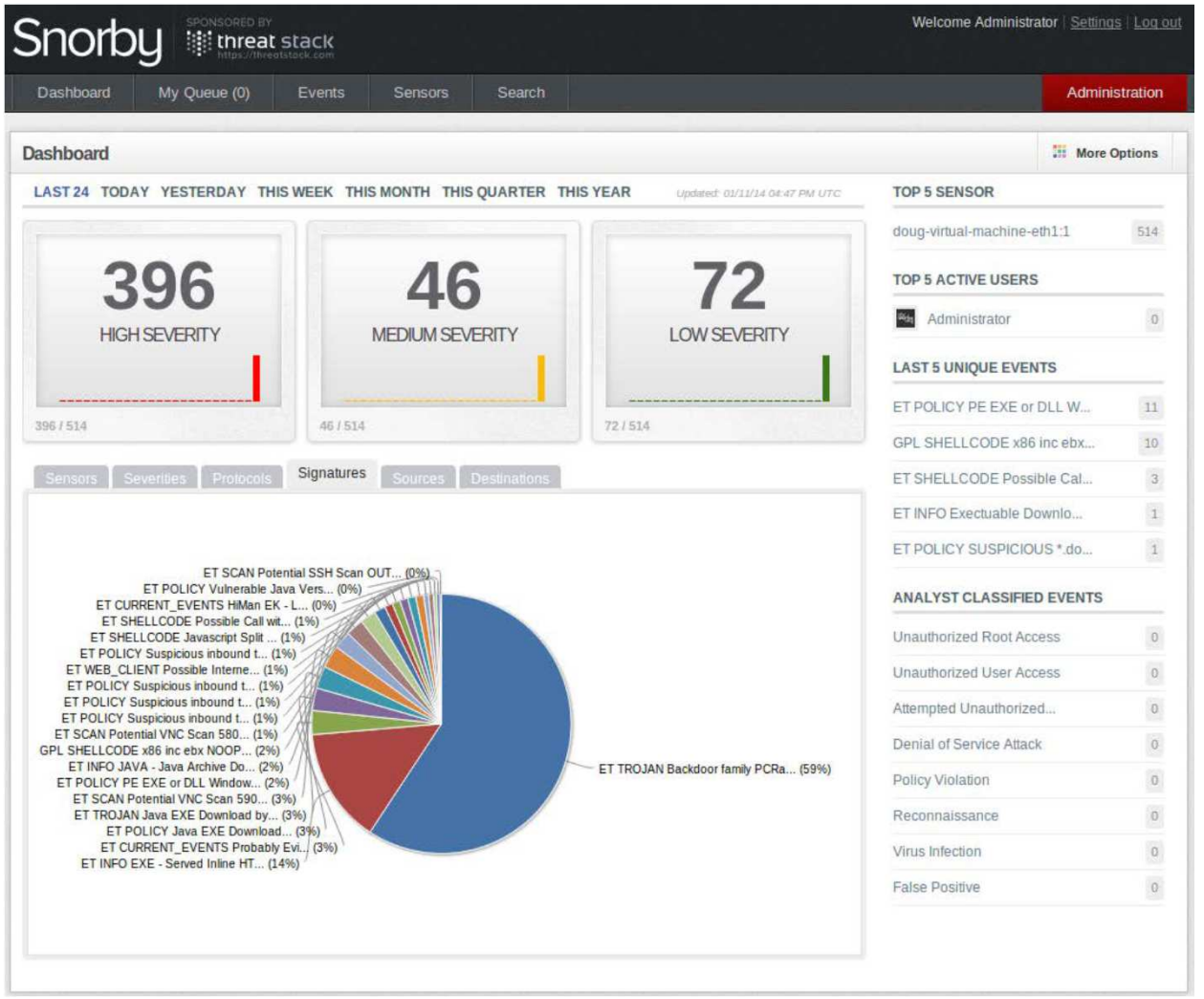
What does SO Look Like?



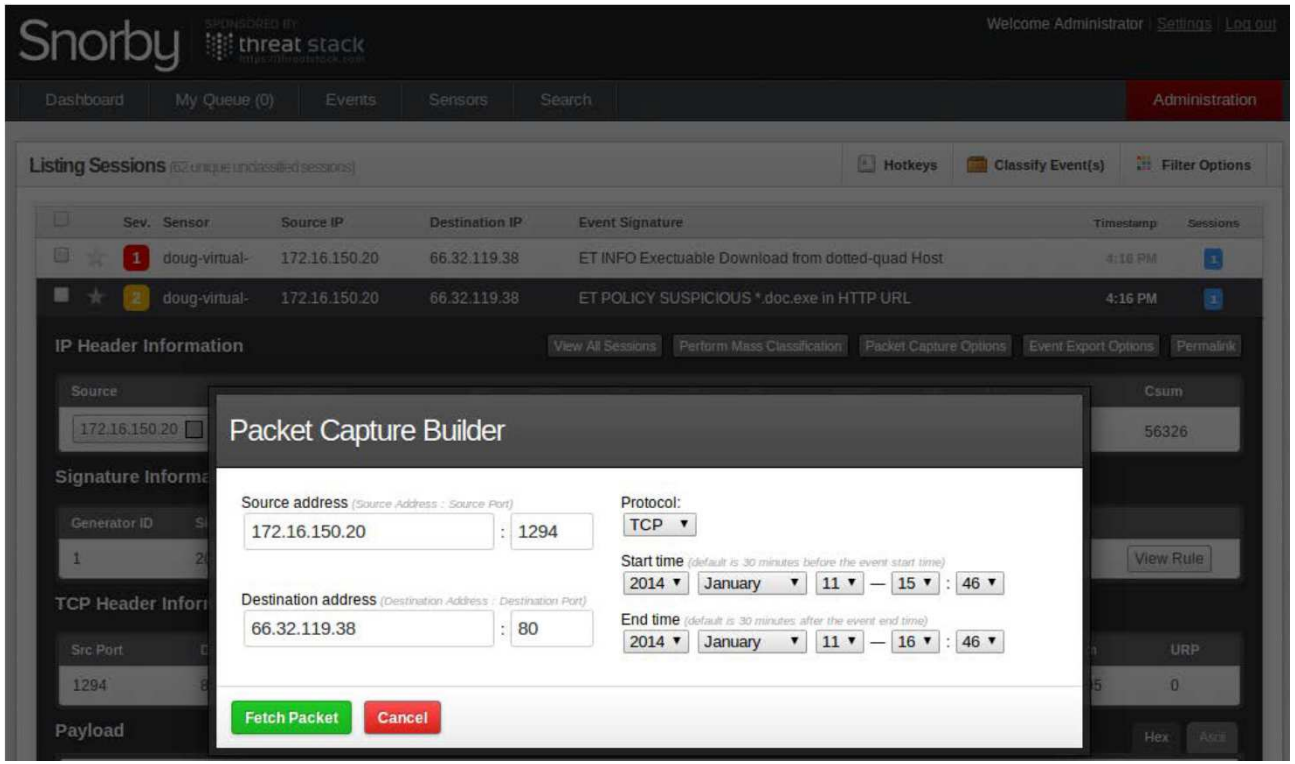
Answer a Few Simple Questions…
(not all shown - Demo Later)



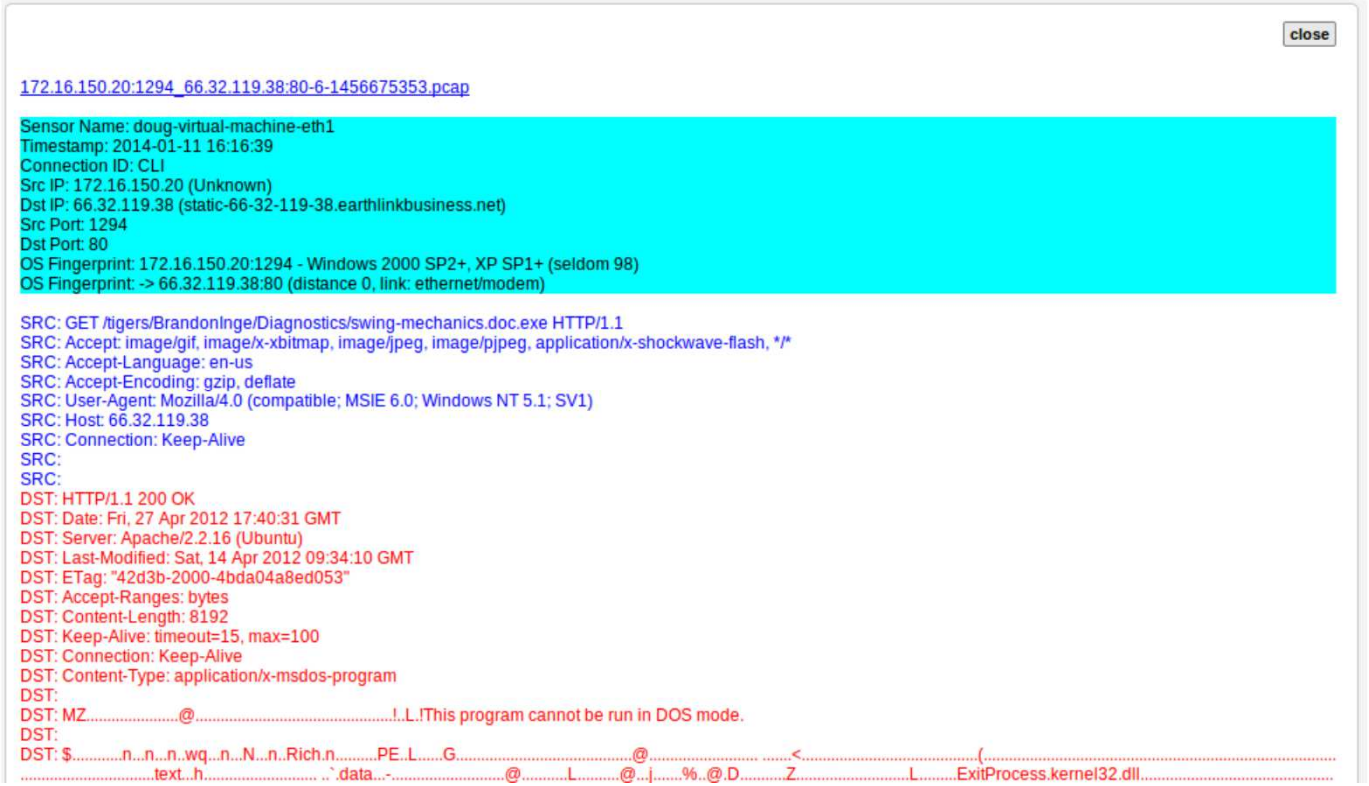
Snorby


Snorby
SPONSORED BY
threat stack
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Dashboard
More Options
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
ET SCAN Potential SSH Scan OUT... (0%)
ET POLICY Vulnerable Java Vers... (0%)
ET CURRENT_EVENTS HiMan EK - L... (0%)
ET SHELLCODE Possible Call wit... (1%)
ET SHELLCODE Javascript Split ... (1%)
ET POLICY Suspicious inbound t... (1%)
ET WEB_CLIENT Possible Interne... (1%)
ET POLICY Suspicious inbound t... (1%)
ET POLICY Suspicious inbound t... (1%)
ET POLICY Suspicious inbound t... (1%)
ET SCAN Potential VNC Scan 580... (1%)
GPL SHELLCODE x86 inc ebx NOOP... (2%)
ET INFO JAVA - Java Archive Do... (2%)
ET POLICY PE EXE or DLL Window... (2%)
ET SCAN Potential VNC Scan 590... (3%)
ET TROJAN Java EXE Download by... (3%)
ET POLICY Java EXE Download... (3%)
ET CURRENT_EVENTS Probably Evi... (3%)
ET INFO EXE - Served Inline HT... (14%)
ET TROJAN Backdoor family PCRa... (59%)
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

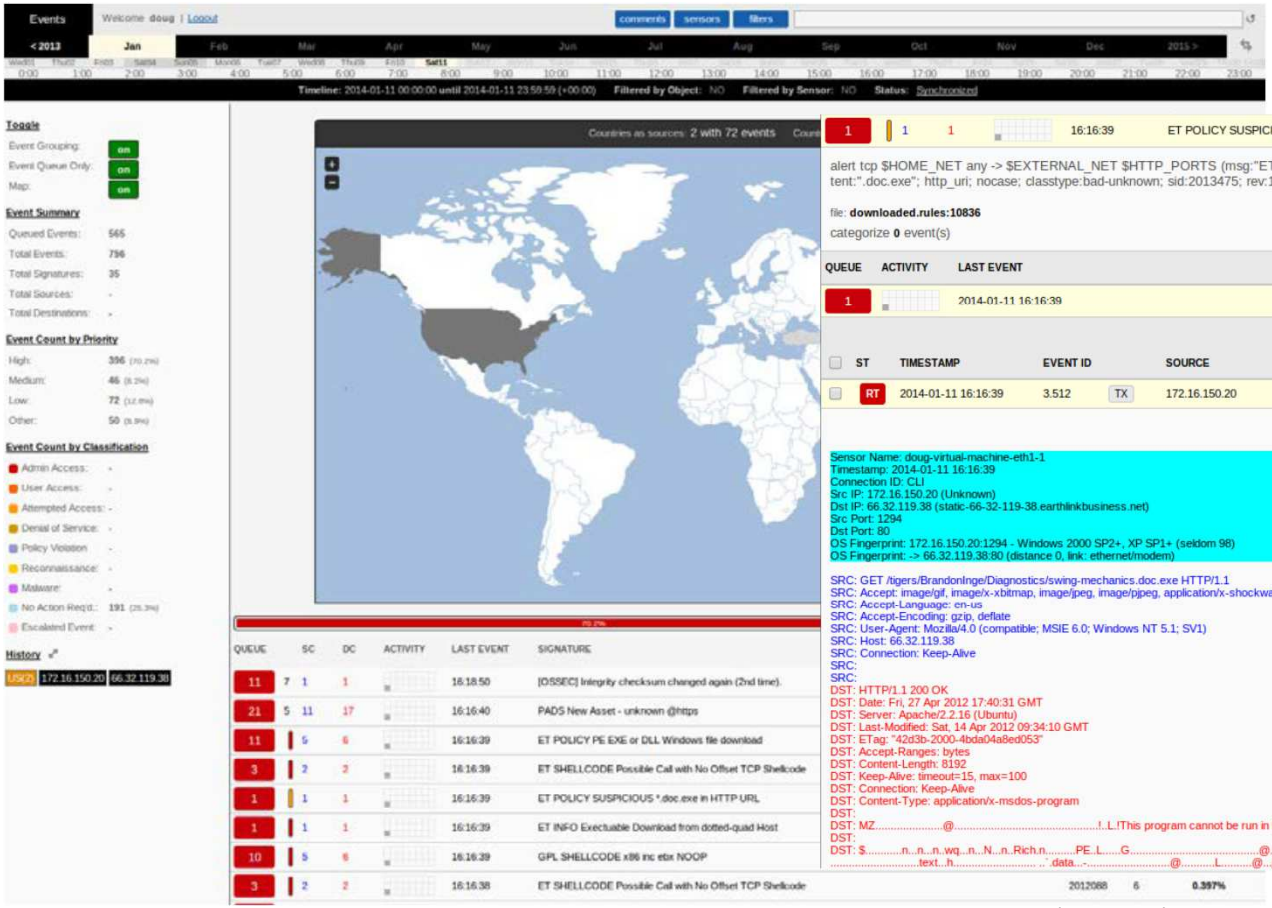
Pivot to PCAP from Snorby



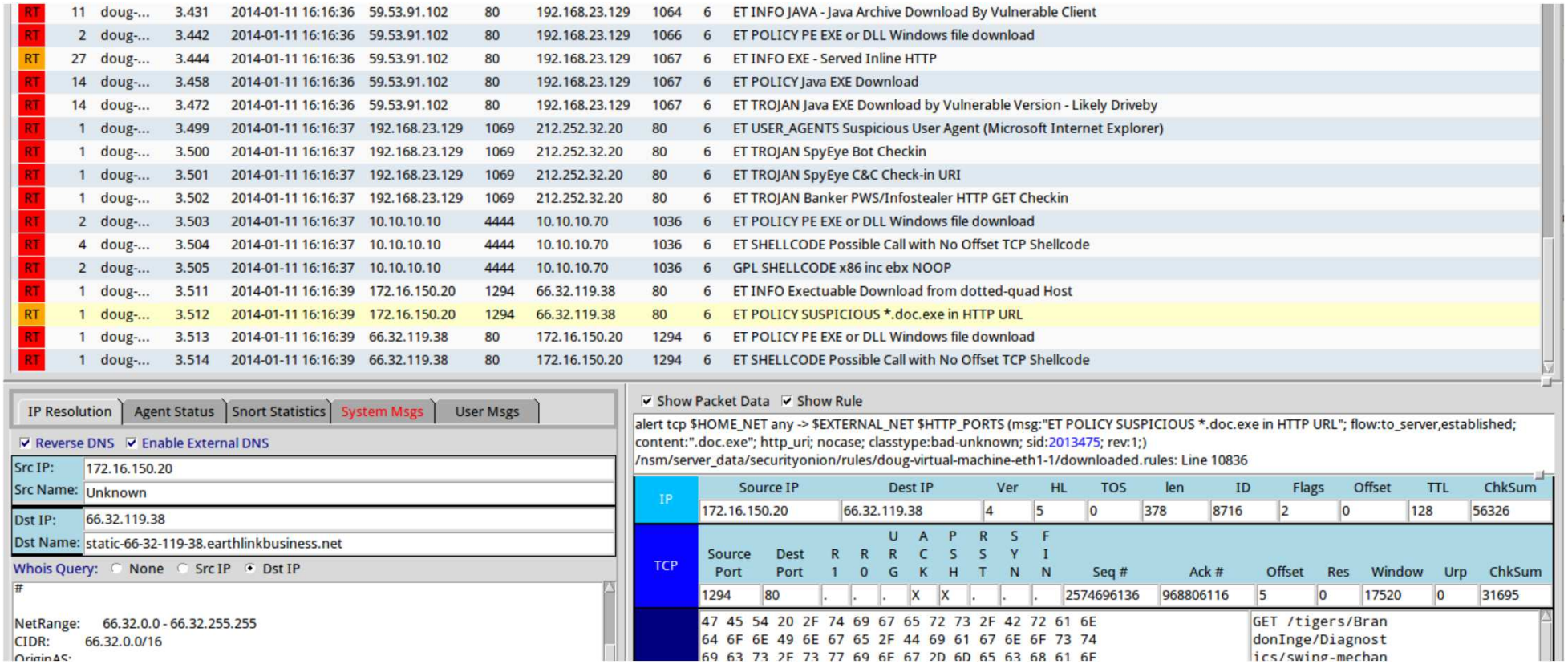
Pivot to CapMe to view Packet Contents



Squert Web Interface



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 Exectuable 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

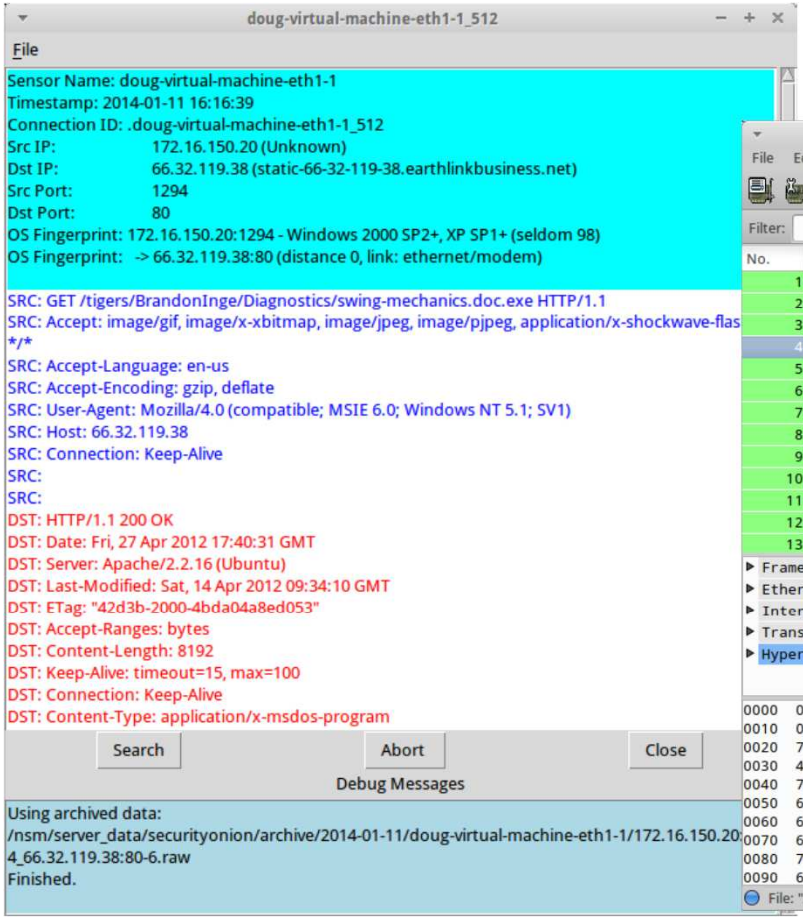
```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY SUSPICIOUS *.doc.exe in HTTP URL"; flow:to_server,established;
content:".doc.exe"; http_uri; nocase; classtype:bad-unknown; sid:2013475; rev:1;)
/nsm/server_data/securityonion/rules/doug-virtual-machine-eth1-1/downloaded.rules: Line 10836
```

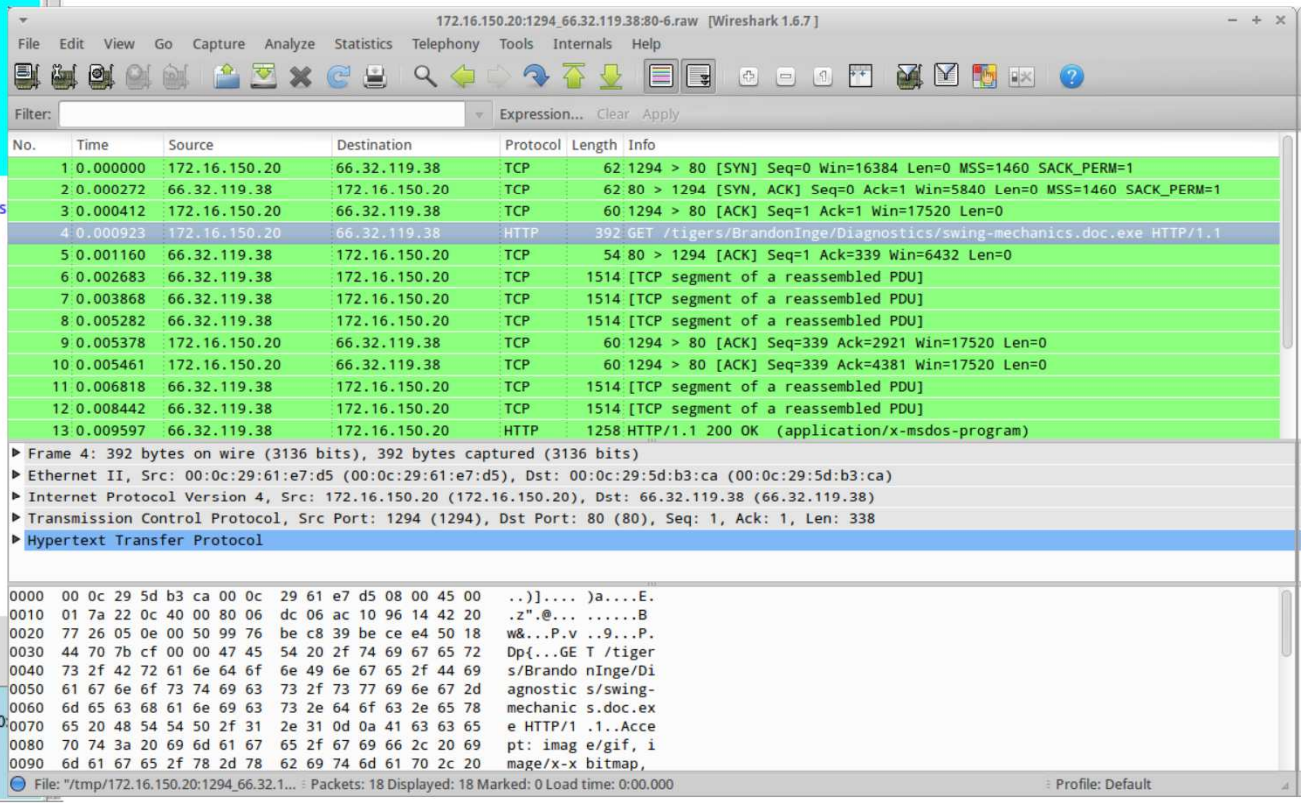
	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	172.16.150.20	66.32.119.38	4	5	0	378	8716	2	0	128	56326

	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	1294	80	.	.	.	X	X	.	.	.	2574696136	968806116	5	0	17520	0	31695

```
47 45 54 20 2F 74 69 67 65 72 73 2F 42 72 61 6E   GET /tigers/Bran
64 6F 6E 49 6E 67 65 2F 44 69 61 67 6E 6F 73 74   donInge/Diagnost
69 63 73 2F 73 77 69 6E 67 2D 6D 65 63 68 61 6E   ics/swing-mechan
```

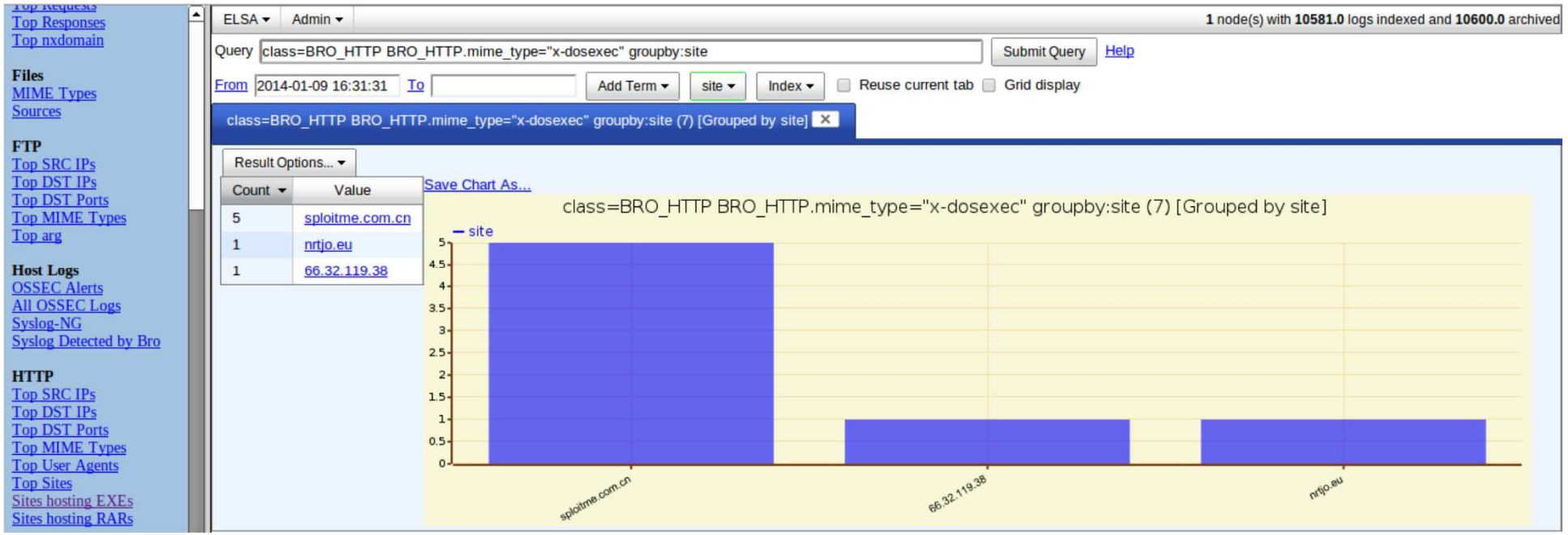
Pivot to PCAP from Sguil



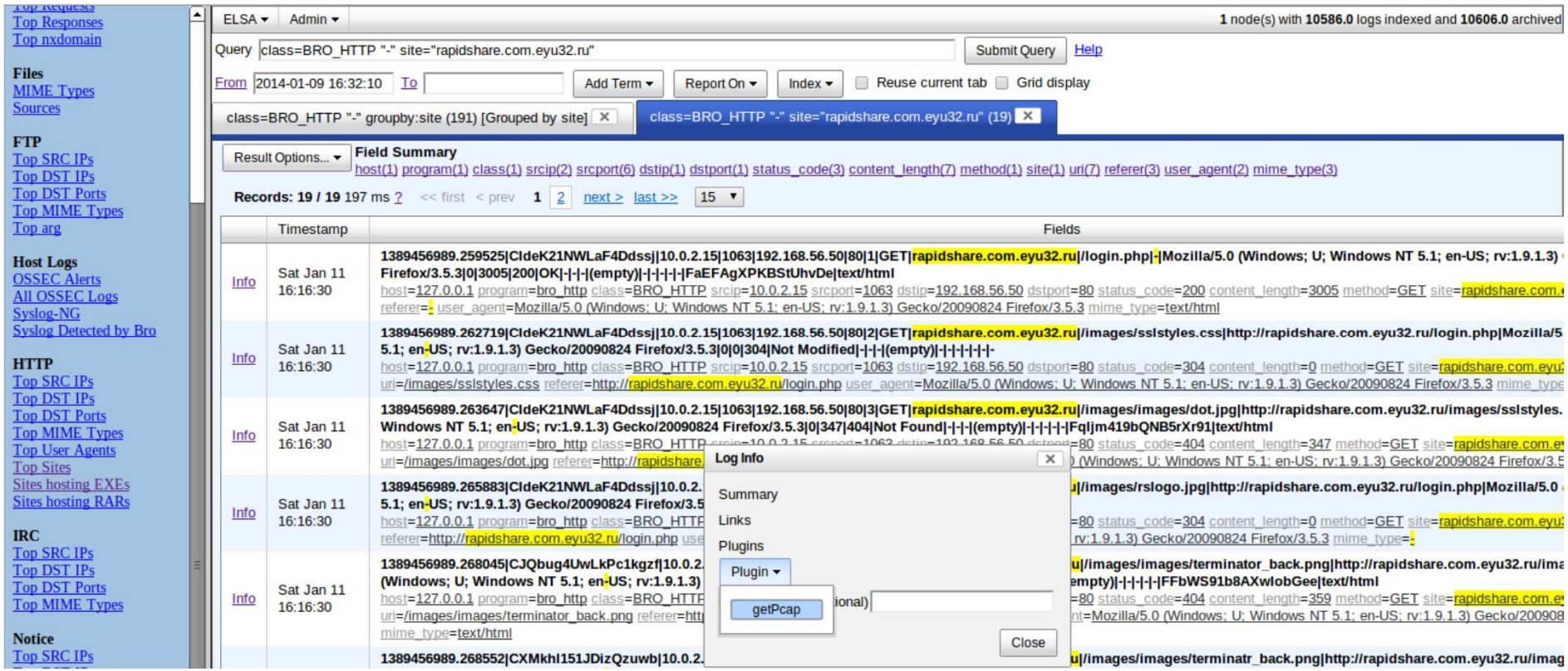


Network Miner

ELSA (Enterprise Log Search and Archive)



Pivot to PCAP from ELSA



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

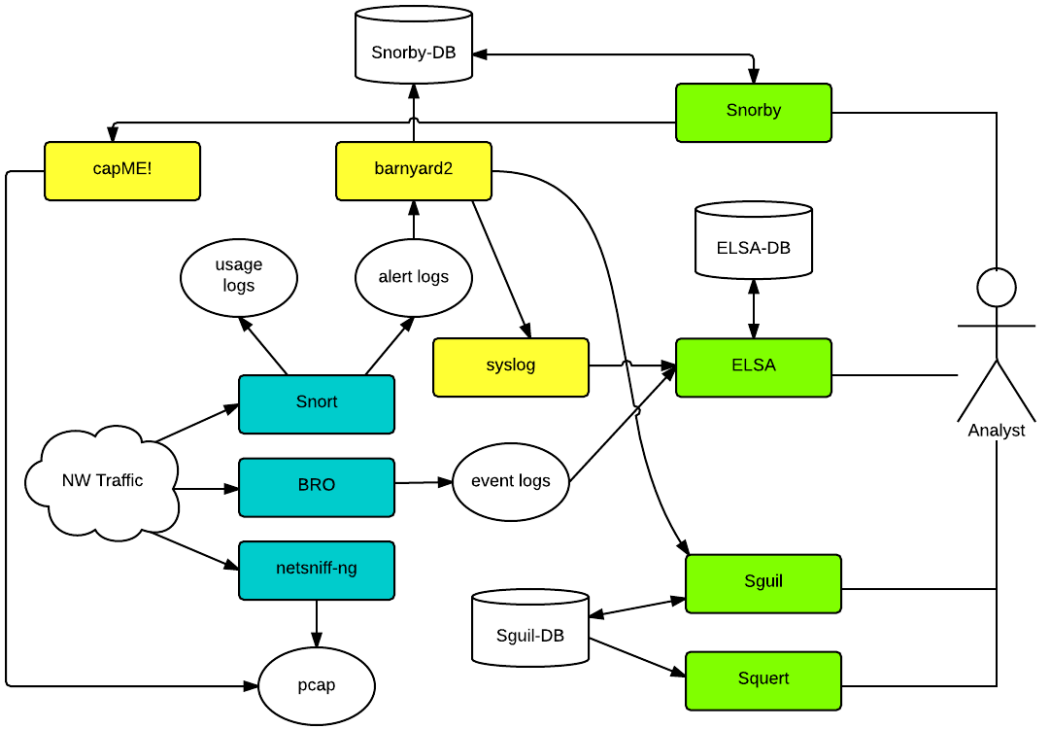
- Bro Network Security Monitor (https://www.bro.org/)
- ELSA - Enterprise Log Search and Archive (https://github.com/mcholste/elsa)
- NetworkMiner (http://www.netresec.com/?page=NetworkMiner)
- Netsniff-ng (http://netsniff-ng.org/)
- OSSEC (Open Source HIDS SECurity) (https://ossec.github.io/)
- Security 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/gamelinux/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/installingsecurityonionon virtualbox
- 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=PLljFITO9rB15jhnSfR6shBEskTgGbta2k

EXTRA CREDIT – A Look Under the Hood

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.

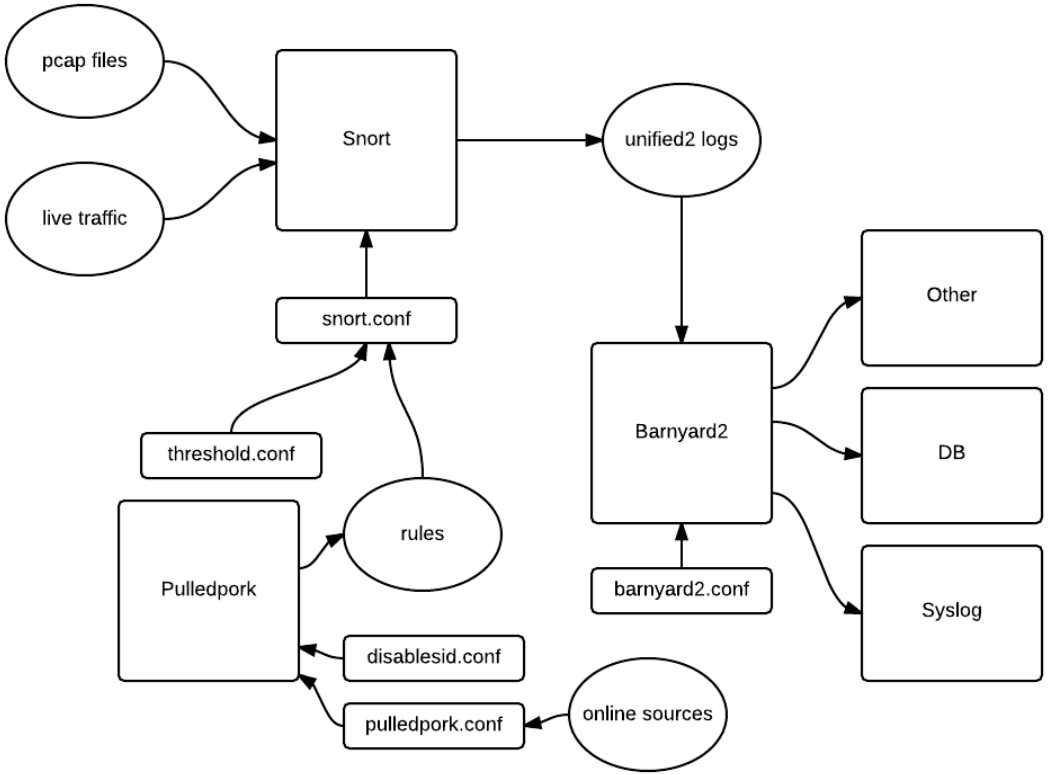
SO - Intermediate Processors

- **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?