

# Defending the Homeland

Logging and Monitoring at home

# Who am I

[@nullthreat](#)

Offensive Red Team for a major company  
I break stuff

Started security @ CNDSP

ADT for networks @ DOD

Designed and Deployed NSM on DOD net

# Talking Points

Perimeter Firewall

Central Logging

Host IDS

Network IDS

Basic Honeypots

Deployment Strategies

Disclaimer: The ideas and solutions presented are my opinion, feel free to disagree.

# OS'es

I use all Linux and Macs at home

I will not be talking about Windows at all, deal with it

Won't matter once we are talking NIDS

# Firewalls on the Cheap

As I see it there is only one good solution in this space



# PFSense

<http://www.pfsense.org>

- Fork of MonoWall
- Robust Firewall based on PF(FreeBSD)
- Multiple VPN Support built-in
  - OpenVPN, IPSec, L2TP, PPTP
- Package based add-ons
  - pfBlocker(block netblocks), Snort, Squid
- Runs on almost anything, Full PC or Embedded

# Embedded Solutions

ALIX 2D3/2D13 ~ 200\$ @ [store.netgate.com](http://store.netgate.com)



# PFsense on Alix Setup

Pauldotcom.com tech segment from episode 220

Google "alix pfsense pauldotcom" and you'll find the show notes

Spark notes:

Download IMG, Write to CF Card, Boot, Use Serial Terminal to do initial setup



# PFSense on Alix Setup

Pro Tip:

Don't put the box together until you flash the OS onto the card, You have to take the entire box apart to get the CF Card in and out.

# PFSense Demo



# Other Options

Surplus Cisco/Juniper/Checkpoint Hardware

Consumer Firewall Solutions

[http://en.wikipedia.org/wiki/List\\_of\\_router\\_or\\_firewall\\_distributions](http://en.wikipedia.org/wiki/List_of_router_or_firewall_distributions)

# Firewalls

Questions?

# Central Logging

I do this on my servers and VPSs

Could do on clients but....meh

Usually the same box that hosts my NIDS stuff

Lots of options

# syslogd

Ol' reliable

Been around since the dawn of freaking time  
originally part of sendmail circa 1980s

UDP Only(in most cases)

Easy-ish to configure but hard to really dial in

# syslogd

Server:

set -r flag in /etc/sysconfig/syslog

ex. SYSLOGD\_OPTIONS="-m 0 -r"

Client:

\*.\* @logs.example.com

\*.info;cron.!=info; mail.\* @logs.example.com

# syslogd

Baked in to most distros, esp old stuff (the vi of logging)

No database support

No advanced filters

Its time to move on to the new offerings



# syslog-ng

Original release 1998

Lots more customizable

- Better filters

- TCP transport

- Crypto(hooray)

- Database support

- (Paid Ver) Guaranteed delivery of Logs

Lots more complicated

# syslog-ng

Setup:

<https://wiki.archlinux.org/index.php/Syslog-ng>

My issue: Custom language for filter, powerful but complicated

If you go this route, may the googles be with you

# rsyslog

Default on most modern \*nix these days

Crypto(hooray) and guaranteed delivery of logs

rsyslog != windows support

# rsyslog

Setup:

<http://edgeofsanity.net/article/2012/06/17/central-logging-with-open-source-software.html>

Backwards compatible with original syslogd  
(syslog-ng might be aswell, didnt look it up)

My preferred solution, used this on 100+ servers pushing logs back to one central logging box

# Now what?

Lots of freaking datas, what now?

Shell scripts (puke)

Perl (lol)

Python (meh)

Logstash - <http://logstash.net/>

Web interfaces (yay)

Splunk (\$)

Arcsight(\$ x WTF!?)

ELSA (SPOILER ALERT)

# Splunk

<http://www.splunk.com/>

Free under 500mb (last I checked)

Needs POWERRRRRRR



Operations Dashboard | Actions ▾

Number of Errors in the last 24 hours

970

[View full results](#)

Number of Failed Purchase Transactions - Last 24 Hours

191

[View full results](#)

Number of Sign On Errors in the Last Hour

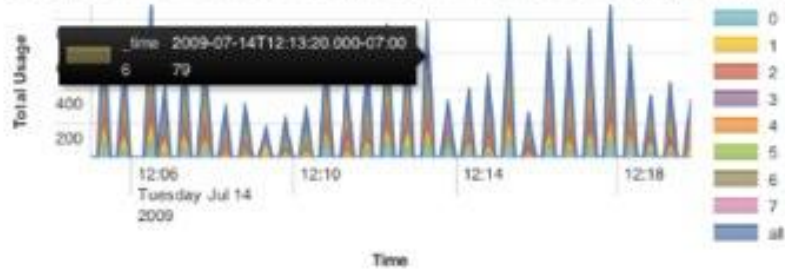
44

[View full results](#)

Usage by CPU - Last 15 Minutes

refreshed: Jul 14, 2009 12:25:43 PM

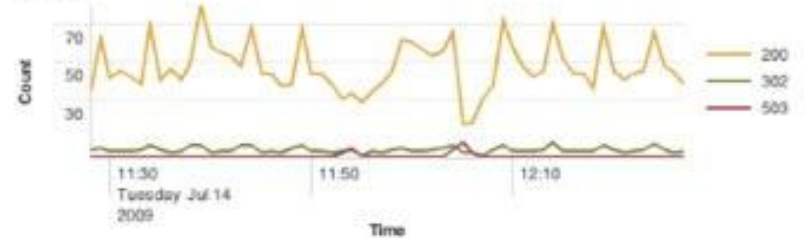
30 events scanned in the last 20 minutes (from 12:05 PM to 12:19 PM on Tuesday, July 14, 2009)



Web Access Count by Status - Last Hour

refreshed: Jul 14, 2009 12:28:10 PM

3,058 events scanned in the last 60 minutes (from 11:28:00 AM to 12:28:00 PM on Tuesday, July 14, 2009)



Top Users by CPU Consumption

refreshed: today at 12:28:48 PM.

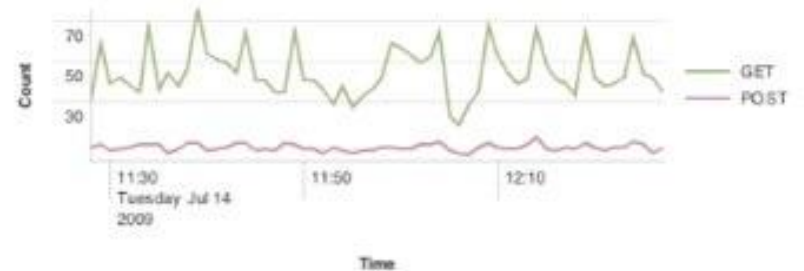
537 events scanned in the last 4 hours (from 8:00:00 AM to 12:28:48 PM on Tuesday, July 14, 2009)



Web Access Count by Method - Last Hour

refreshed: Jul 14, 2009 12:28:10 PM

3,058 events scanned in the last 60 minutes (from 11:28:00 AM to 12:28:00 PM on Tuesday, July 14, 2009)



Last 5 Events

refreshed: today at 12:28:48 PM.

# Splunk

Easy to setup

Yours won't look that cool

Has "apps" for lots of other tools



# ELSA

Enterprise Log Search and Archive

<https://code.google.com/p/enterprise-log-search-and-archive/>

Open source hotness

FREE



Query srcip:10.124.19.12 Submit Query Help

From 2011-11-21 22:05:51 To Add Term Report On Index

srcip:10.124.19.12 (10587) srcip:10.124.19.12 (10587) [Grouped by class] srcip:10.124.19.12 (172) [Grouped by hostname] srcip:10.124.19.12 (4154)

Result Options... Field Summary

host(4) program(4) class(3) srcip(1) srcport(74) dstip(22) dstport(3) expiration(2) hostname(2) subject(2) proto(2) conn\_bytes(43) o\_int(2) i\_int(2) conn\_duration(17) status\_code(1) content\_length(20) country\_code(3) method(2) site(8) uri(23) referer(7) user\_agent(1) domains(8)

Records: 100 / 4154 1486 ms < prev 1 2 3 4 5 6 7 next > 15

	Timestamp	Fields
Info	Tue Nov 22 08:53:20	1321973538.778549 vflpkUrpo6 10.124.19.12 47263 209.85.225.132 443 TLSv10 TLS_ECDHE_RSA_WITH_RC4_128_SHA s2.googleusercontent.com - CN=*.googleusercontent.com, View,ST=California,C=US 1320932962.000000 1352555962.000000 0ef6837e26d26f08700a9e03c863dafa ok host=165.189.226.172 program=bro_ssl class=BRO_SSL srcip=10.124.19.12 srcport=47263 dstip=209.85.225.132 dstport=443 expiration=1352555962 hostname=s2.googleusercontent.com s View,ST=California,C=US
Info	Tue Nov 22 08:53:20	1321973537.891299 oE6L8viiUv7 10.124.19.12 41018 199.59.149.198 443 TLSv10 TLS_RSA_WITH_RC4_128_SHA twitter.com 970e68f4de429d78cdc280f310267aa67ee8530e8be2e3ec924 Inc.,streetAddress=795 Folsom St, Suite 600,L=San Francisco,ST=California,postalCode=94107,C=US,serialNumber=4337446.2.5.4.15=#131450726976617465204F7267616E697A6174696F6E,1.3.6.1.4.1.311.60.2.1.2=#1308446 131001480 host=165.189.226.172 program=bro_ssl class=BRO_SSL srcip=10.124.19.12 srcport=41018 dstip=199.59.149.198 dstport=443 expiration=1343451599 hostname=twitter.com subject=CN=twit Folsom St, Suite 600,L=San Francisco,ST=California,postalCode=94107,C=US,serialNumber=4337446.2.5.4.15=#131450726976617465204F7267616E697A6174696F6E,1.3.6.1.4.1.311.60.2.1
Info	Tue Nov 22 08:53:25	Teardown UDP connection 144744478313156395 for DET-SEC-124.19:10.124.19.12/45091 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 213 host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=45091 dstip=10.68.15.11 dstport=53 conn_bytes=213 o_int=DE
Info	Tue Nov 22 08:53:25	Teardown UDP connection 144744478313156396 for DET-SEC-124.19:10.124.19.12/52757 to OUTSIDE:10.68.15.11/53 duration 0:02:02 bytes 213 host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=52757 dstip=10.68.15.11 dstport=53 conn_bytes=213 o_int=DE
Info	Tue Nov 22 08:53:26	Teardown UDP connection 144744478313156397 for DET-SEC-124.19:10.124.19.12/47309 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 217 host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=47309 dstip=10.68.15.11 dstport=53 conn_bytes=217 o_int=DE
Info	Tue Nov 22 08:53:26	Teardown UDP connection 144744478313156398 for DET-SEC-124.19:10.124.19.12/52485 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 284 host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=52485 dstip=10.68.15.11 dstport=53 conn_bytes=284 o_int=DE
Info	Tue Nov 22 08:53:26	Teardown UDP connection 144744478313156399 for DET-SEC-124.19:10.124.19.12/57404 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 172 host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=57404 dstip=10.68.15.11 dstport=53 conn_bytes=172 o_int=DE
Info	Tue Nov 22 08:54:20	Teardown UDP connection 144744478313156408 for DET-SEC-124.19:10.124.19.12/35728 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 221 host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=35728 dstip=10.68.15.11 dstport=53 conn_bytes=221 o_int=DE
Info	Tue Nov 22 08:54:20	Teardown UDP connection 144744478313156409 for DET-SEC-124.19:10.124.19.12/43103 to OUTSIDE:10.68.15.11/53 duration 0:02:03 bytes 221 host=165.189.82.68 program=%fwsm-5-302016 class=FIREWALL_CONNECTION_END proto=UDP srcip=10.124.19.12 srcport=43103 dstip=10.68.15.11 dstport=53 conn_bytes=221 o_int=DE
Info	Tue Nov 22	Teardown UDP connection 144744478313156410 for DET-SEC-124.19:10.124.19.12/51752 to OUTSIDE:10.68.15.11/53 duration 0:02:02 bytes 198

# ELSA v Splunk

Not a pretty

Free

Ease-ish to setup - more on this later

# Central Logging

Questions?

# HIDS

Host based intrusion detection systems

Monitor logs for malicious activity

File integrity monitoring

# HIDS - Software

Tripwire - <http://sourceforge.net/projects/tripwire>

Commercial product with Open src version

Samhain - <http://la-samhna.de/samhain/>

OSSEC - <http://www.ossec.net/>

Sagan - <http://sagan.quadrantsec.com/>

# Sagan

*"Sagan is an open source (GNU/GPLv2) high performance, real-time log analysis & correlation engine that run under \*nix operating systems (Linux/FreeBSD/OpenBSD/etc). It is written in C and uses a multi-threaded architecture to deliver high performance log & event analysis. Sagan's structure and rules work similarly to the Sourcefire "Snort" IDS/IPS engine. This was intentionally done to maintain compatibility with rule management software (oinkmaster/pulledpork/etc) and allows Sagan to correlate log events with your Snort IDS/IPS system. Sagan can also write to Snort IDS/IPS databases via Unified2/Barnyard2."*

```
root@localhost:~  
[*] Loading /usr/local/etc/sagan-rules/windows-misc.rules rule file  
[*] Loading /usr/local/etc/sagan-rules/wordpress.rules rule file  
[*] Loading /usr/local/etc/sagan-rules/xinetd.rules rule file  
[*] Loading /usr/local/etc/sagan-rules/zeus.rules rule file  
[*] Configuration file /usr/local/etc/sagan.conf loaded and 1974 rules loaded.  
[*] Sagan version 0.2.2-r1 is firing up!  
[*] Dropping privileges [UID: 502 GID: 503]  
[*] -----  
[*] Max Output Threads   : 50  
[*] Max Processor Threads: 50  
[*]  
[*] Sensor ID           : 1  
[*] Next CID            : 1  
[W] Inconsistent cid information for sid=1. Recovering by rolling forward to cid=0  
[*]  
[*]  
[*] ,-._-.-  -*> Sagan! <*-  
[*] \/)\"(\)  Version 0.2.2-r1  
[*]  (_o_)   Champ Clark III & The Quadrant InfoSec Team [quadrantsec.com]  
[*]  /_ \)   Copyright (C) 2009-2012 Quadrant Information Security, et al.  
[*] (|| ||)  Using PCRE version: 7.8 2008-09-05  
[*] oo-oo   Sagan is processing events....  
[*]  
[*] Attempting to open syslog FIFO (/var/run/sagan.fifo).  
[*] Successfully opened FIFO (/var/run/sagan.fifo).  
[*]  
[*] -----  
[*] Total number of events processed   : 0  
[*] Total number of events thresholded : 0 (0.000%)  
[*] Total number of events after      : 0 (0.000%)  
[*] Total number of signatures matched : 0 (0.000%)  
[*] Total output plugin dropped       : 0 (0.000%)  
[*] Total dropped                      : 0 (0.000%)  
[*] Average Events Per-Second: 0 [18 of 60 seconds. Calculating...]  
[*] -----  
[
```



# Sagan

Thanks to the snort-like features many existing tools to manage things like:

- Updating rules

- Parsing alerts to DB

- Web Interfaces to read alerts (Snorby!)

Heard great things about this tool but never used it

# OSSEC

## Supports via Agents:

- GNU/Linux (all distributions, including RHEL, Ubuntu, Slackware, Debian, etc)
- Windows 7, XP, 2000 and Vista
- Windows Server 2003 and 2008
- VMWare ESX 3.0,3.5 (including CIS checks)
- FreeBSD (all versions)
- OpenBSD (all versions)
- NetBSD (all versions)
- Solaris 2.7, 2.8, 2.9 and 10
- AIX 5.3 and 6.1
- HP-UX 10, 11, 11i
- MacOSX 10

# OSSEC

## Support via syslog:

- Cisco PIX, ASA and FWASM (all versions)
- Cisco IOS routers (all versions)
- Juniper Netscreen (all versions)
- SonicWall firewall (all versions)
- Checkpoint firewall (all versions)
- Cisco IOS IDS/IPS module (all versions)
- Sourcefire (Snort) IDS/IPS (all versions)
- Dragon NIDS (all versions)
- Checkpoint Smart Defense (all versions)
- McAfee VirusScan Enterprise (v8 and v8.5)
- Bluecoat proxy (all versions)
- Cisco VPN concentrators (all versions)

# OSSEC

Additional device support information:

[http://www.ossec.net/?page\\_id=36](http://www.ossec.net/?page_id=36)

# OSSEC

## Features:

- File Integrity Monitoring

- Log Monitoring

  - Logins (Success and Failed)

  - SUDO's

- Rootkit Detection

- Active Response

  - Add IPTables Rules, ect

# OSSEC Install Modes

If you choose 'server', you will be able to analyze all the logs, create e-mail notifications and responses, and also receive logs from remote syslog machines and from systems running the 'agents' (from where traffic is sent encrypted to the server).

If you choose 'agent'(client), you will be able to read local files (from syslog, snort, apache, etc) and forward them (encrypted) to the server for analysis.

If you choose 'local', you will be able to do everything the server does, except receiving remote messages from the agents or external syslog devices.

If you choose 'hybrid', you get the 'local' installation plus the 'agent' installation.

*Note: Stolen word for word from the installer*

# OSSEC

Setup:

<http://www.ossec.net/doc/manual/installation/index.html>

Super Easy, Pick type, next next next, Done

Ubuntu Bug Fix:

Change line 372 of install.sh

```
if [ "X${USER_AGENT_SERVER_IP}" = "X" -a "X${USER_AGENT_SERVER_NAME}" = "X" ]; then
```

# Example Logs

```
** Alert 1371080777.7617: - pam,syslog,authentication_success,  
2013 Jun 12 23:46:17 vps->/var/log/auth.log  
Rule: 5501 (level 3) -> 'Login session opened.'  
Jun 12 23:46:16 vps sshd[6697]: pam_unix(sshd:session): session opened for  
user nullthreat by (uid=0)
```

```
** Alert 1371080919.8382: - syslog, su,authentication_success,  
2013 Jun 12 23:48:39 vps->/var/log/auth.log  
Rule: 5303 (level 3) -> 'User successfully changed UID to root.'  
User: root  
Jun 12 23:48:38 vps su[6876]: + /dev/pts/0 root:root
```

*Default location: /var/ossec/logs/alerts/alerts.log*



# OSSEC DEMO

Installing a new Agent.....maybe

# HIDS

Questions?

# Network IDS

Looks at packets going across the wire

Most are rules based

```
alert tcp any any -> any any (msg:"Possible exploit"; content:"|90|";)
```

Very popular, several of options

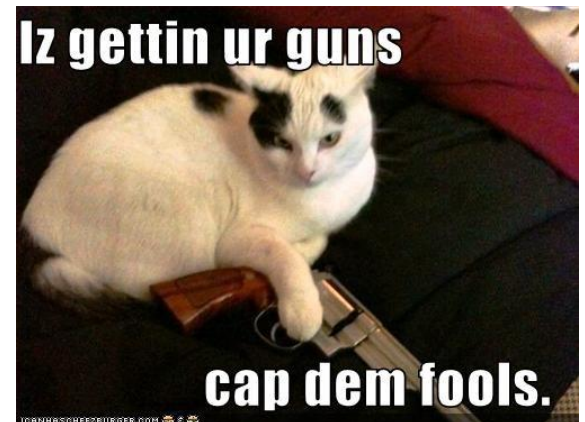
# Cap dem packets

Software and Hardware solutions

Use quality network cards

PCAP Files

FPC = TONS OF SPACE



# Software Taps

Deamonlogger - <http://www.snort.org/snort-downloads/additional-downloads#daemonlogger>

Others?

Don't use software taps

# Hardware Taps

Mirror/Span <- perfect for home in my opinion

Passive Taps <- Build your own, carry with

Regeneration taps <- what you need on larger networks

<http://www.digininja.org/interceptor/>

# Hardware Taps

<http://hakshop.myshopify.com/products/throwing-star-lan-tap> - 15\$

<http://hakshop.myshopify.com/products/throwing-star-lan-tap-pro> - 40\$

<http://www.instructables.com/id/Make-a-Passive-Network-Tap/> - Cheap

# Hardware Taps

<http://www.amazon.com/dp/B002YK8WMC> -  
Netgear GS105E - 35\$ <- What I use

[http://www.networktaps.com/ProductDetails.  
asp?ProductCode=TCTHG-K](http://www.networktaps.com/ProductDetails.asp?ProductCode=TCTHG-K) - nTAP gig tap -  
795\$ w/ free overnight shipping!!

Hubs!?!?!?



# The Tools

IDS: Snort, Suricata, Bro

Rules Management: PulledPork, Polman

Logging/Spooling: Barnyard2, Pigsty

Interfaces: SGUIL, Snorby, ELSA

This list IS NOT comprehensive

# Snort

<http://www.snort.org/>

Open source IDS from Sourcefire

Most popular, I have seen this thing  
EVERYWHERE

Signature/anomaly based

Session Edit View Bookmarks Settings Help

```
12/07-15:05:34.001135  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
tttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:104
3
12/07-15:05:34.001135  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:1043
12/07-15:05:34.001163  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
tttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:444
5
12/07-15:05:34.001163  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:4445
12/07-15:05:34.009147  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
tttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:217
9
12/07-15:05:34.009147  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:2179
12/07-15:05:34.012119  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
tttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:994
3
12/07-15:05:34.012119  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:9943
12/07-15:05:34.014243  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
tttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:667
12/07-15:05:34.014243  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:667
12/07-15:05:34.015088  [**] [1:2000545:6] ET SCAN NMAP -f -sS [**] [Classification: A
tttempted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:200
2
12/07-15:05:34.015088  [**] [1:2000537:6] ET SCAN NMAP -sS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 192.168.1.67:33811 -> 192.168.1.64:2002
```



Shell

Shell No. 2

Shell No. 3



# Suricata

<http://www.openinfosecfoundation.org/index.php/download-suricata>

Open Source IDS from OISF

Partially funded by DHS and SPAWAR

Signature/anomaly based

```
alfon@alfonubuntu: /var/log/suricata
GNU nano 2.2.4                               Archivo: fast.log

02/18/11-11:42:02.165385  [**] [1:2010937:2] ET POLICY Suspicious inbound to MySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority:
02/18/11-11:42:02.266498  [**] [1:2010937:2] ET POLICY Suspicious inbound to MySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority:
02/18/11-11:42:03.032122  [**] [1:2010936:2] ET POLICY Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Prior
02/18/11-11:42:03.142702  [**] [1:2010936:2] ET POLICY Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Prior
02/18/11-11:42:05.443471  [**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority:
02/18/11-11:42:05.553307  [**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority:
02/18/11-11:42:06.975324  [**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 1
02/18/11-11:42:08.065538  [**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 19
02/18/11-11:42:08.065538  [**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 192.168.1.
02/18/11-11:42:14.629472  [**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 19
02/18/11-11:42:14.629472  [**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 192.168.1.
02/18/11-11:42:21.096947  [**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 1
02/18/11-11:42:21.189087  [**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 19
02/18/11-11:42:21.189087  [**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 192.168.1.
02/18/11-11:42:24.256391  [**] [1:2002910:4] ET SCAN Potential VNC Scan 5800-5820 [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 1
02/18/11-11:42:25.129073  [**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Prior
02/18/11-11:42:25.235976  [**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Prior
02/18/11-11:42:27.754723  [**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 19
02/18/11-11:42:27.754723  [**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 192.168.1.
02/18/11-11:42:34.316666  [**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 19
02/18/11-11:42:34.316666  [**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 192.168.1.
02/18/11-11:42:35.300050  [**] [1:2002910:4] ET SCAN Potential VNC Scan 5800-5820 [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 1
02/18/11-11:42:40.881240  [**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 19
02/18/11-11:42:40.881240  [**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 192.168.1.
02/18/11-11:42:41.988569  [**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 1
02/18/11-11:42:43.176379  [**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] (6) 1
02/18/11-11:42:46.077869  [**] [1:2002993:5] ET SCAN Rapid POP3S Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priori
02/18/11-11:42:50.614771  [**] [1:2002992:5] ET SCAN Rapid POP3 Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priorit
02/18/11-11:42:52.932680  [**] [1:2002994:5] ET SCAN Rapid IMAP Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priorit
02/18/11-11:42:56.540211  [**] [1:2002995:8] ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priori
02/18/11-11:43:27.921391  [**] [1:2002995:8] ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priori
```

It should look very similar to Snort

# Snort V Suricata

## Snort

Single Threaded  
Packages Available  
Lots of Documentation  
IPv6 @ compile time  
Limited configuration  
Libpcap

## Suricata

Multi-Threaded  
Build from src  
Limited external docs  
IPv6 native  
Highly configurable  
Libpcap, PF\_RING...

# BRO IDS aka Big Brother

<http://www.bro.org/index.html>

Open Source

15 years of research in supercomputer labs  
and Berkeley CS institute

Flexible detection methods

# BRO IDS

I'm a total BRO noob

This guy knows his stuff! <http://liamrandall.com/>

Parses and classifies all the traffic, tags for easy searching

Incredibly powerful language for describing protocols and events - BRO Lang



# Bro Demo



# Rules management

For Snort or Suricata

Use pulled pork <https://code.google.com/p/pulledpork/>

Google will help you install and config this

Topic is boring, moving on

# Spooling

Takes the stuff from the console and makes it useful

Barnyard2 - The industry standard

<https://github.com/firnsy/barnyard2/>

Pigsty - New kid on the block

<http://threatstack.github.io/pigsty/>

<http://snorby.org:3009/> - Cool Demo, lets look

# Interfaces - ACID/BASE

ACID - Analysis Console for Intrusion  
Databases

Last Updated '03

BASE - Basic Analysis and Security Engine

Last Updated in '09

# Basic Analysis and Security Engine (BASE)

- Most recent Alerts: [any protocol](#), [TCP](#), [UDP](#), [ICMP](#)
- Today's: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
- Last 24 Hours: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
- Last 72 Hours: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
- Most [recent 15 Unique Alerts](#)
- Last Source Ports: [any](#), [TCP](#), [UDP](#)
- Last Destination Ports: [any](#), [TCP](#), [UDP](#)
- Most [frequent 5 Alerts](#)
- Most Frequent Source Ports: [any](#), [TCP](#), [UDP](#)
- Most Frequent Destination Ports: [any](#), [TCP](#), [UDP](#)
- Most frequent 15 addresses: [source](#), [destination](#)

Added 0 alert(s) to the Alert cache

Queried on : Thu October 14, 2004 22:02:36

Database: snort\_log@localhost (schema version: 106)

Time window: [2004-09-02 16:05:49] - [2004-10-08 11:25:41]

[Search](#)

[Graph Alert data](#)

Graph alert [detection time](#)

## Sensors: 1

Unique Alerts: 14

categories:5

Total Number of Alerts: 84

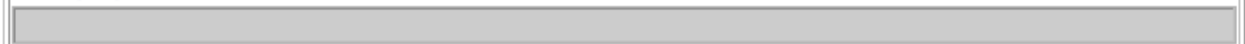
- Src IP addrs: 5
- Dest. IP addrs: 9
- Unique IP links 13
- Source Ports: 68
  - TCP ( 68) UDP ( 0)
- Dest. Ports: 12
  - TCP ( 12) UDP ( 0)

## Traffic Profile by Protocol

TCP (96%)



UDP (0%)



ICMP (4%)



Portscan Traffic (0%)



[Alert Group Maintenance](#) | [Cache & Status](#) | [Administration](#)

BASE 0.9.7.2 ( by [Kevin Johnson](#) and the BASE Project Team

Built on ACID by Roman Danyliw )

[Loaded in 0 seconds]

Meta	<b>ID #</b>	<b>Time</b>	<b>Triggered Signature</b>	
	1 - 84	2004-10-08 11:25:41	[snort] NETBIOS SMB IPC\$ share unicode access	
	<b>Sensor</b>	<b>name</b>	<b>interface</b>	<b>filter</b>
	192.168.1.4	eth0	none	
	<b>Alert Group</b>	none		

IP	<b>source addr</b>	<b>dest addr</b>	<b>Ver</b>	<b>Hdr Len</b>	<b>TOS</b>	<b>length</b>	<b>ID</b>	<b>flags</b>	<b>offset</b>	<b>TTL</b>	<b>chksum</b>
	192.168.1.100	192.168.1.4	4	5	0	122	14356	0	0	128	16049
	<b>FQDN</b>	<b>Source Name</b>		<b>Dest. Name</b>							
		Unable to resolve address		kevinanddenise.homelinux.com							
	<b>Options</b>	none									

TCP	<b>source port</b>	<b>dest port</b>	<b>R1</b>	<b>R0</b>	<b>URG</b>	<b>ACK</b>	<b>PSH</b>	<b>SYN</b>	<b>FIN</b>	<b>seq #</b>	<b>ack</b>	<b>offset</b>	<b>res</b>	<b>window</b>	<b>urp</b>	<b>chksum</b>
	1613	139				X	X			990153569	3328611299	5	0	63669	0	32195
	<b>Options</b>	none														

length = 82

```

000 : 00 00 00 4E FF 53 4D 42 75 00 00 00 00 18 07 C8      ...N.SMBu.....
010 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE  .....
020 : 64 00 C0 00 04 FF 00 4E 00 08 00 01 00 23 00 00      d.....N....#..
030 : 5C 00 5C 00 4C 00 4F 00 52 00 49 00 45 00 4E 00      \\.L.O.R.I.E.N.
040 : 5C 00 49 00 50 00 43 00 24 00 00 00 3F 3F 3F 3F      \.I.P.C.$...????
    
```

# Sguil

The De'Facto interface from a few years back

Still widely used

Multiple data sources

Correlation engine

I found it very difficult to setup and manage





# **Sguil/Squert Demo**



# Snorby

<https://snorby.org/>

Free and open source

All web 2.0 - Ruby, Rails, JS, HTML5

IOS App

Dev by Former GE CERT and Mandiant





# Snorby





Reads data from database





Snort, Suricata, Sagan





Supports FPC via OpenFPC

Large install base, lots of documents on how to setup

 (portscan) TCP Portscan 35 minutes ago - 06/02/10 - 10:19:55 AM  
Source: 192.168.56.1 - Destination: 192.168.56.101  
Sensor: 5 - Event Category: **Unclassified**   

 (portscan) Open Port 35 minutes ago - 06/02/10 - 10:19:55 AM  
Source: 192.168.56.1 - Destination: 192.168.56.101  
Sensor: 5 - Event Category: **Unclassified**   

 (portscan) Open Port 35 minutes ago - 06/02/10 - 10:19:55 AM  
Source: 192.168.56.1 - Destination: 192.168.56.101  
Sensor: 5 - Event Category: **Unclassified**   

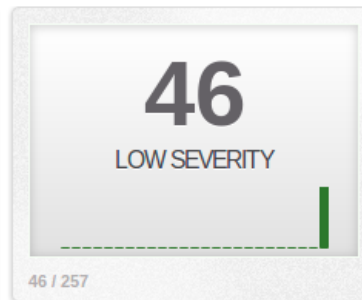
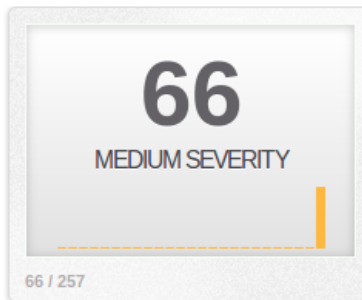
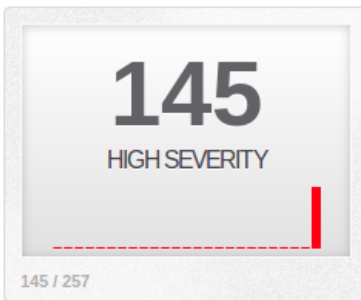
 (portscan) Open Port 35 minutes ago - 06/02/10 - 10:19:55 AM  
Source: 192.168.56.1 - Destination: 192.168.56.101  
Sensor: 5 - Event Category: **Unclassified**   

## Dashboard

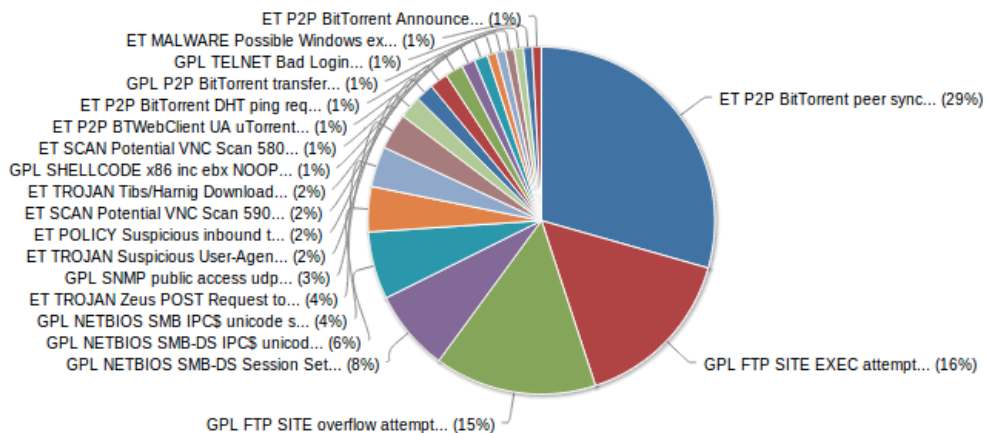
More Options

[LAST 24](#)
[TODAY](#)
[YESTERDAY](#)
[THIS WEEK](#)
[THIS MONTH](#)
[THIS QUARTER](#)
[THIS YEAR](#)

Updated: 09/27/12 3:07:06 PM



[Sensors](#)
[Severities](#)
[Protocols](#)
[Signatures](#)
[Sources](#)
[Destinations](#)



### TOP 5 SENSOR

derbycon1-eth0:1	157
derbycon1-eth0:2	100

### TOP 5 ACTIVE USERS

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

### LAST 5 UNIQUE EVENTS

ET TROJAN Zeus POST Request to C...	9
ET INFO Packed Executable Download	1
GPL SNMP trap tcp	1
ET POLICY Suspicious inbound to ...	4
ET POLICY Suspicious inbound to ...	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

# Snorby

Logout

173.84.162.140.0 -> 173.255.236.165.0  
1:27 PM

[APACHE] Apache robots.txt access 1  
213.186.122.3:514 -> 64.251.27.63:80  
12:36 PM

ET POLICY Reserved IP Space 10  
5.34.243.145:2065 -> 173.255.236.165:8118  
11:25 AM

Add to Queue

False Positive

[OPENSSSH] Accepted publickey 8  
173.255.236.165:35459 -> 173.255.236.165:22  
11:19 AM

ET POLICY Reserved IP Space 2  
101.210.251.235:50024 -> 173.255.236.165:80  
10:43 AM

[APACHE] Apache robots.txt access 2  
66.249.76.110:514 -> 64.251.27.63:80  
8:27 AM

ET POLICY Reserved IP Space 2  
23.22.23.223:40981 -> 173.255.236.165:443  
7:20 AM

Events

Queue

Settings

# Snorby Demo

Snorby 2

# My Workflow

Feed all the BRO logs into ELSA for indexing

Take alerts from Snorby

Pull PCAP with OpenFPC

Search IPs in ELSA

Not owned, False positive from crap iPhone Ad



# Workflow Demo

Suricata + Snorby + Bro + ELSA

# Setting up the tools

Search google and build it yourself, this sucks

OSSIM - <http://communities.alienvault.com/>

Insta-Snorby - <https://github.com/Snorby/insta-snorby>

Security Onion

Threat Stack Incident Response System

# Security Onion

<http://securityonion.blogspot.com/>

Doug Burks

Free

Backtrack/kali for defenders

LiveCD or HD Install

# Security Onion

Ubuntu

Snort, Suricata, Bro

Sguil, Squert, Snorby, ELSA

Xplico, Network Miner and others

# Security Onion



# TS:IRS

<https://www.threatstack.com/#/products/incident-response-system>

Cloud Based IDS

Commercial Project (its not cheap for home)

7 day free trial!

Gave me a free month to show it off to you guys

# TS:IRS

Crazy easy to setup

Ubuntu server install

Copy/Paste one liner

Wait

IDS

**TS:IRS**





# NSM

Questions?

# Honeypots

Not going to go into much detail here

Very very simple honeypots

Low interaction

Free and Open Source

# Kippo - The SSH Honeytrap

<https://code.google.com/p/kippo/>

SSH Honeytrap

Looks like OS but won't install software

Lulztastic

<http://kippo.rpg.fi/playlog/?l=20100316-233121-1847.log>

# Kippo

Needs to be tweaked or easy to detect

Not a ton of info but google should help

Neat WebUI - <http://bruteforce.gr/kippo-graph>

# Artillery

<https://www.trustedsec.com/downloads/artillery/>

Project from Dave Kennedy aka Rel1k

Python Based Honeypot, File System Monitoring, System Hardening and Real time threat intel feed

Free

# Artillery

Default Honeypot Ports:

135,445,22,1433,3389,8080,21,5900,25,53,  
110,1723,1337,10000,5800,44443

Very simple to deploy and configure

# People to Follow

@mephux - Snorby and ThreatStack

@securityonion

@bro\_ids

@hectaman - Liam Randall, Mandiant and  
BRO

@chrissanders88 - Practical Packet Analysis

@dave\_rel1k - Trusted Sec and Artillery (SET)

<https://github.com/gamelinux>

<https://github.com/threatstack>

# Books

Practical Packet Analysis - Chris Sanders

All of Richard Bejtlichs books (pre-order new)

[http://www.amazon.com/gp/product/1593275099/ref=oh\\_details\\_o00\\_s01\\_i00?ie=UTF8&psc=1](http://www.amazon.com/gp/product/1593275099/ref=oh_details_o00_s01_i00?ie=UTF8&psc=1)

The TCP/IP Guide - Charles M Kozierok

Network Forensics - Sherri Davidoff and  
Jonathan Hamm



# Thanks

Black Lodge & \_Them

Dustin Webber and ThreatStack for long term demo

Security Onion for being so awesome and making IDS easy

Contact me @nullthreat on twitter