

# The principle of Network Security Monitoring[NSM]

C.S.Lee[geek00L@gmail.com]  
<http://geek00L.blogspot.com>

# Claim:

Before I proceed, I would like to make it clear about the topic I gonna deliver, I'm not here to talk about

- How to monitor the network architecture?
- How to secure the network architecture?

I'm here to talk about

- The concept of NSM framework and why NSM is important to you

# REAL WORLD NETWORK SECURITY IMPLEMENTATION AND PROBLEM

In order to secure the network. Most of companies deploy equipments such as,

- Proxy
- Firewall
- Host Intrusion Detection System(HIDS)
- Network Intrusion Detection System(NIDS)
- Intrusion Prevention System(IPS)
- ETC

Clearly enough, they are thinking that those devices offer network security, instead of monitoring their network security.

# Accuse Market Hype!!!!

Most decision makers believe in market hype instead of his people, when market promotes and pushes Firewall device, all companies go to get one, and these days when everyone talk about Intrusion Prevention System(IPS), your boss will ask you whether there's a need to deploy IPS. Though they don't know what the hell is IPS all about.

- Business men who sell the working out of box defensive devices don't care about your security, they care about their sales. Promoting and advertising is their main priority instead of delivering the right thing.
- Remember, the device itself won't give you any security promises, monitoring is the part that playing the main role to secure your network.
- Elite hacker can easily compromise your network by evading your firewall or IDS/IPS, and who gonna watch them after all?

After all the devices been deployed, another issue raises, you will have to answer your boss about –

- When the network is compromised?
- Why the network is compromised?
- How the network is compromised?

And the most hilarious question should be

- Why we have already deployed all the expensive defensive perimeters and the network still get compromised?

NETWORK SECURITY IS NOT DETERMINED  
BY MARKET. DON'T LET MARKET TEACHES  
US WHAT IS NETWORK SECURITY ALL  
ABOUT!!!!!!

THEY SHOULD STOP DELIVERING FALSE  
SENSE OF NETWORK SECURITY!!!!!!

# REAL WORLD THREATS

Threat – party with the capabilities and intentions to exploit a vulnerabilities in an asset.

Two type of threats

Unstructured threat – lack of methodologies, money and objective. It normally consists of crackers, script kiddies and worms.

Structured threat – adversaries with formal methodology, a financial sponsored, and a defined objective. It normally consists of economy spies, organized criminals, terrorists, intelligent agencies

Now we have already understand what kind of security perimeters been deployed by the companies and the threats that coming along, let's look at its perspective in depth.

# SECURITY VS THREATS

THE NEVER ENDING RACE

# Firewall

A logical barrier designed to prevent unauthorized or unwanted communications between segments of a computer network

## Firewall – Weakness

However if you are deploying services and it is vulnerable, you are still exposed to the attacks. We can see clearly about the recent php worms that crawling on port 80 where you have to have that port opened if you are running web services.

When people come to realized the important role of firewall?

When blaster hitting port 139/TCP and slammer going wild on port 1434/udp in the internet, I guess everyone still remember the bitter experience. Later sasser worms that spreading across internet by targeting port 445/TCP. And recent php worms that crawling on port 80/TCP.

# Intrusion Detection System

The underlying technology

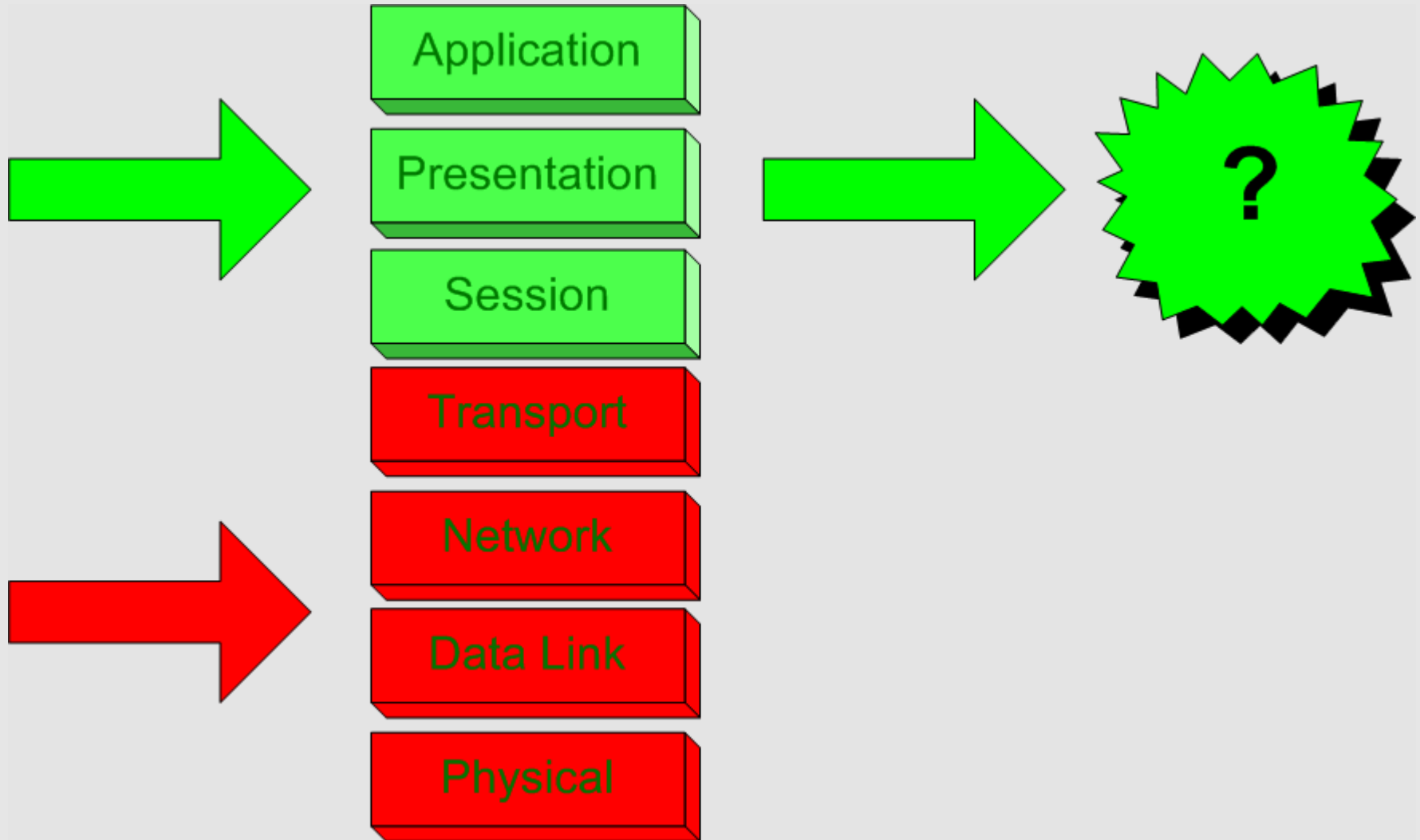
It is actually performing checking on the application layers with its protocol decoders and investigating the payload data.

Detecting anomaly transport layer and network layer, and some on data link layer as well.

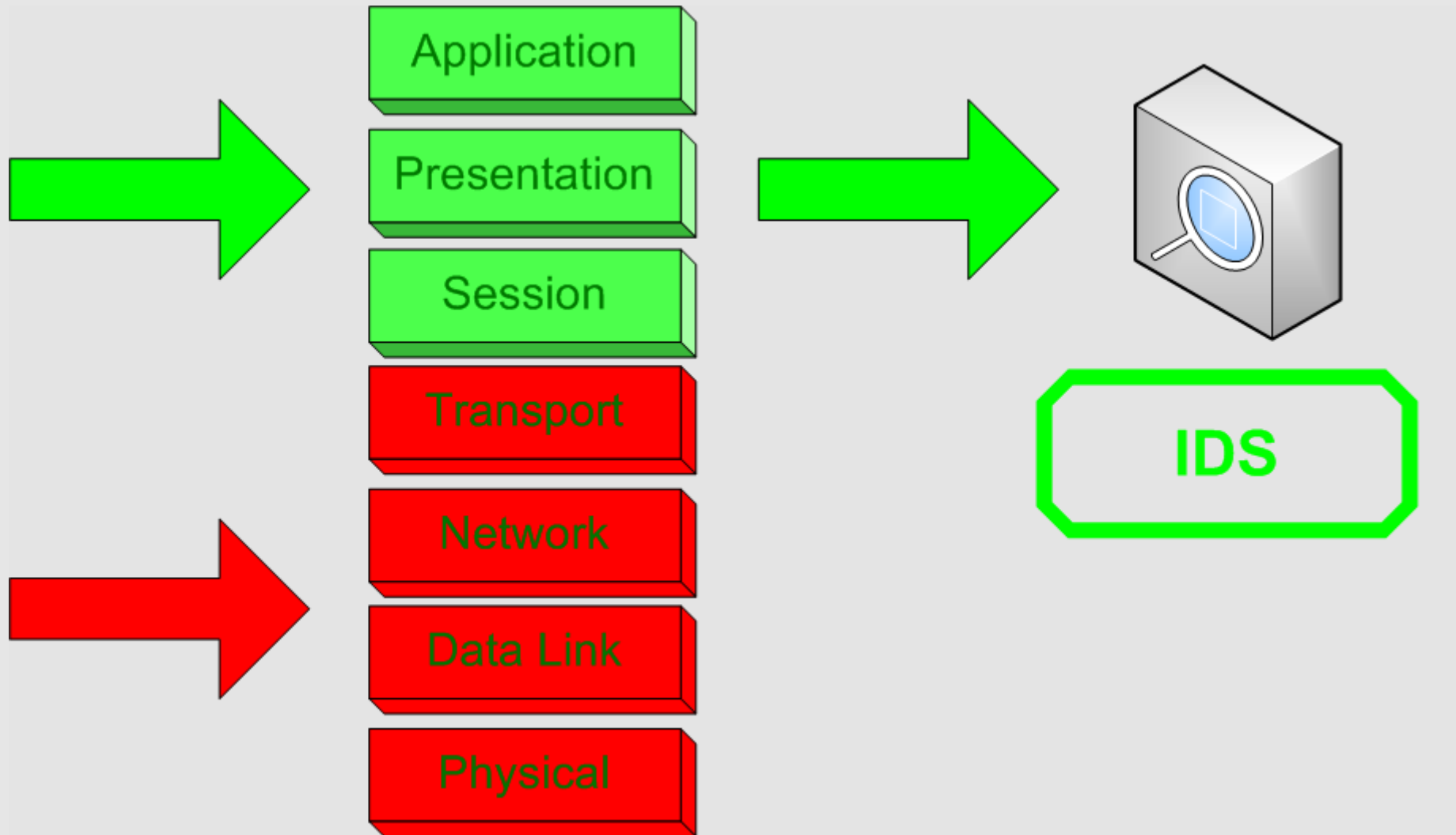
Some advance IDS can do more but it is out of the topic here.

So why we need Intrusion Detection System(IDS) since we already have firewall?

# Firewall



# Intrusion Detection System



# **Intrusion Detection System – Weakness**

- False Positive/Negative
- Usually defeated by 0 days exploit
- Encrypted connection is the nightmare for IDS
- Only as good as it's detection engine and signature rule set.

# Intrusion Prevention System??????

I'm not gonna talk about Intrusion Prevention System(IPS) since it is IDS + Firewall or some people call it application firewall.

IPS is actually intrusion detection system with policy enforcement capabilities. That's all.

Which party has upper hand?

Firewall + IDS is configured with prefixed static rules and signatures where it is good enough to detect and filter most of the intrusions that performed by unstructured threat(worms mitigation, script kiddies and crackers) where they are using already published codes and exploits. But for serious and skillful hacker, normally they are knowledgeable enough to circumvent or bypass firewall + IDS. Remember IDS is just a program used to analyze scientifically but not psychologically.

Firewall + IDS vs Unstructured threats =

Static  $\geq$  < Static

Structured threats vs Firewall + IDS

Dynamic  $>$  Static

Clearly enough, with firewall and intrusion detection system(IDS) or other defensive perimeters, it is not enough to sustain the structured threats. Hence we need a better framework that can integrate with the mindset and skills of Security Analyst.

And as security analyst, 3 principles must keep in mind

- Some intruders are smarter than you
- Some intruders are unpredictable
- Prevention eventually fail

To change the scene,

Security Analyst(Firewall + IDS + ETC) vs  
Structured Threats

Dynamic  $\geq$  < Dynamic

The Firewall, IDS and ETC becomes subset of security analyst. It's human intelligence against human intelligence war now instead of machine against human.

The question is

What security analyst need to acquire in order to perform Incident Response, Incident Handling, Network Forensic and creating countermeasure plan?

The answer is only one - all the necessary data that collected through out the incident!!!

Hence ...

We need Network Security  
Monitoring Framework

# What is Network Security Monitoring(NSM)?

In year 2002, Bamm Vischer and Richard Bejtlich defined NSM as “the collection, analysis and escalation of indications and warnings(I&W) to detect and respond to intrusions”

# NSM Approach



Before we look at NSM in depth, let's see what CSI team do when they are reaching the crime scene .....

CSI Infamous Quote: Assume Nothing

- Collecting **full content data** in the crime scene
- In the process of data collection, equipment that used by criminal may provide **alert data(clues)**
- Clues will lead to the starting scope of investigation.
- Tracking with the alert data(clues). It may be right or wrong. For example, there's knife in the crime scene but not necessary it is used to kill but maybe the victim was killed by using poison. Clever Criminal used to mislead and confuse the Investigator.

– The one who get killed normally will have connection to someone who has purpose of killing him. Normally crime scene investigator will start looking at the people who has connection to the victim. That's where they classify the **statistical data**(which is the most possible/suspicious criminal) by analyzing **session data**(connections between criminal and victim). If someone has done it, for sure he has done it.

– Remember clue maybe wrong, but statistical data and session data is true all the while since it is what was happening(fact).

It's all about data collection. Can anyone analyze and escalate without enough data?

NSM, not relies on what kind of equipments or devices you deploy, but more concern on collecting data in 4 forms.

- Statistical data
- Session data
- Full Content data
- Alert data

# Statistical and Session Data

## Statistical Data

- Network traffic aggregates
- Protocol breakdown and distributions
- Tools available: tcpdstat, ethereal

## Session Data

- Record connection pair, the conversation between two hosts. The basic elements include src ip, src port, dst ip, dst port, protocol and timestamps.
- Tools available: argus, ipaudit

# Statistical Data

AnalystT | ackstorm.pcap - Ethereal | Conversations: ackstorm.pcap | Ethereal: Protocol Hierarchy S | 1:44

Ethereal: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▼ Frame	100.00%	2271	1765851	0.351	0	0	0.000
▼ Ethernet	100.00%	2271	1765851	0.351	0	0	0.000
▼ Internet Protocol	98.90%	2246	1764351	0.351	0	0	0.000
▼ Transmission Control Protocol	94.01%	2135	1754420	0.349	927	61028	0.012
SSH Protocol	0.22%	5	610	0.000	5	610	0.000
▼ Hypertext Transfer Protocol	52.97%	1203	1692782	0.337	1132	1593527	0.317
Unreassembled Fragmented Packet	0.88%	20	29964	0.006	20	29964	0.006
▼ CompuServe GIF	0.66%	15	20475	0.004	3	2407	0.000
Unreassembled Fragmented Packet	0.53%	12	18068	0.004	12	18068	0.004
Media Type	0.48%	11	12552	0.002	11	12552	0.002
Line-based text data	0.62%	14	19610	0.004	14	19610	0.004
▼ JPEG File Interchange Format	0.48%	11	16654	0.003	0	0	0.000
Unreassembled Fragmented Packet	0.48%	11	16654	0.003	11	16654	0.003
▼ User Datagram Protocol	1.37%	31	4011	0.001	0	0	0.000
Domain Name Service	1.32%	30	3885	0.001	30	3885	0.001
Routing Information Protocol	0.04%	1	126	0.000	1	126	0.000
Internet Control Message Protocol	3.52%	80	5920	0.001	80	5920	0.001
▼ Logical-Link Control	0.84%	19	1140	0.000	0	0	0.000
Spanning Tree Protocol	0.84%	19	1140	0.000	19	1140	0.000
Address Resolution Protocol	0.26%	6	360	0.000	6	360	0.000

OK

# Session Data

AnalystT | ackstorm.pcap - Ethereal | Ethereal: Protocol Hierarchy S | Conversations: ackstorm.pcap | 1:43

Conversations: ackstorm.pcap

Ethernet: 4 | Fibre Channel | FDDI | IPv4: 49 | IPX | JXTA | SCTP | TCP: 60 | Token Ring | UDP: 16 | WLAN | RSVP

TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
203.87.186.218	1873	67.18.208.100	http	1	60	1	60	0	0
206.248.68.170	1206	67.18.208.100	http	1	54	0	0	1	54
71.34.95.37	mciautoreg	67.18.208.100	http	1	54	0	0	1	54
60.48.153.154	10816	67.18.208.100	http	1	370	0	0	1	370
220.233.15.233	2863	67.18.208.100	http	2	114	1	60	1	54
220.233.15.233	2868	67.18.208.100	http	2	3028	0	0	2	3028
63.109.248.62	52050	67.18.208.100	http	2	152	1	74	1	78
202.134.2.126	38079	67.18.208.100	http	2	152	1	74	1	78
71.193.85.110	29890	67.18.208.100	http	3	3082	0	0	3	3082
219.92.219.10	1257	67.18.208.100	http	3	4542	0	0	3	4542
218.208.32.220	44195	67.18.208.100	http	3	198	1	66	2	132
218.208.32.220	44183	67.18.208.100	http	3	198	1	66	2	132
218.208.32.220	44256	67.18.208.100	http	3	198	1	66	2	132
67.150.8.119	4732	67.18.208.100	http	3	186	3	186	0	0
201.25.41.142	50528	67.18.208.100	http	3	174	2	120	1	54
218.111.129.170	62051	67.18.208.100	http	3	174	2	120	1	54
66.249.72.231	40227	67.18.208.100	http	4	264	2	132	2	132
203.39.81.25	6511	67.18.208.100	http	4	264	2	132	2	132
219.92.219.10	1254	67.18.208.100	http	4	228	2	120	2	108
219.95.238.120	3617	67.18.208.100	http	4	228	2	120	2	108
200.29.149.250	62268	67.18.208.100	http	4	228	2	120	2	108
203.223.134.81	ampr-info	67.18.208.100	http	6	1371	4	578	2	793
203.144.143.6	32952	67.18.208.100	http	6	2552	3	527	3	2025
70.57.211.194	2380	67.18.208.100	http	7	412	4	242	3	170
70.57.211.194	2381	67.18.208.100	http	7	412	4	242	3	170

Copy

Name resolution

X Close

# Alert Data

- Collected by Intrusion Detection System
- Serve as clue/indication of intrusion. No false positive or false negative, but helps in generate event of interest.
- Tools available: snort, bro-ids

# Alert Data

Show Packet Data  Show Rule

www.snort.org

nvd.nist.gov

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 139 (msg:"NETBIOS SMB Session Setup AndX request unicode username overflow attempt"; flow:to\_server,established; content:"|00 00|"; distance:0; content:"|00 00|");

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum						
	192.168.0.239	192.168.0.5	4	5	0	390	1675	2	0	128	28834						
TCP	Source Port	Dest Port	U	A	P	R	S	F	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum		
	1123	139	.	.	.	X	X	.	.	.	1773717601	2501129558	5	0	63608	0	41469
DATA	<pre> 00 00 01 5A FF 53 4D 42 73 00 00 00 00 18 07 C8      ...Z.SMBs..... 03 00 42 53 52 53 50 59 4C 20 10 00 00 00 FF FE      ..BSRSPYL ..... 01 E8 80 00 0C FF 00 5A 01 04 41 32 00 00 00 00      .....Z..A2.... 00 00 00 B8 00 00 00 00 00 00 D4 00 00 A0 1F 01 A1      ..... 81 B5 30 81 B2 A2 81 AF 04 81 AC 4E 54 4C 4D 53      ..0.....NTLMS 53 50 00 03 00 00 00 18 00 18 00 6C 00 00 00 18      SP.....1.... 00 18 00 84 00 00 00 10 00 10 00 40 00 00 00 0C      .....@..... 00 00 00 50 00 00 00 10 00 10 00 50 00 00 00 10      P          \                 </pre>																

Search Packet Payload

Hex

Text

NoCase

# Full Content Data

- Log every single bit of network traffic
- Forensic sounds
- To perform forensic analysis on hard drive, investigator needs to have access to full content data in the hard drive in order to locate evidence. That's why they image the hard drive.
- The same with NSM, we need to log every single bit of network traffic in order to analyze.
- Tools available: tcpdump, tethereal

**PUTTING IT ALTOGETHER**



<http://sguil.sf.net>

# Sguil – The Analyst Console for NSM

- The only Open Source Suite that built upon the NSM framework.
- Written in TCL/TK by Bamm Visscher, with contributors in Sguil community.
- Considered it to be only suite that utilize the capabilities of security analyst.

Created By analyst – For analyst



# Sguil – Data Collection

Alert Data – Snort(IDS mode)

Session Data – Sancp

Full Content Data – Second Instance of snort(packet logger mode)

Statistical Data – You have freedom to use anything on hand, my preference goes to tcpdstat, ifstat, trafshow or ntop.

# Sguil – Nifty Features for Analyst

- Whois, reverse dns and dshield port lookup
- Communication within Security Analyst
- Transcript generation
- Launching ethereal/netdude for protocol analysis
- Sguil DB query too
- Correlation with Nessus
- Event escalation and categorize

# Performing Quick Analysis with Sguil

1. Snort alerts on event of interest(clue)
2. Query session data for event of interest to understand the conversation between two hosts.
3. Generating transcript for human readable output.
4. Analyzing full content data if it is necessary.
5. Escalate the event

# Sguil DEMO

# Sguil Deployment

You can choose to deploy sguil in different ways depends on your network environment and criteria.

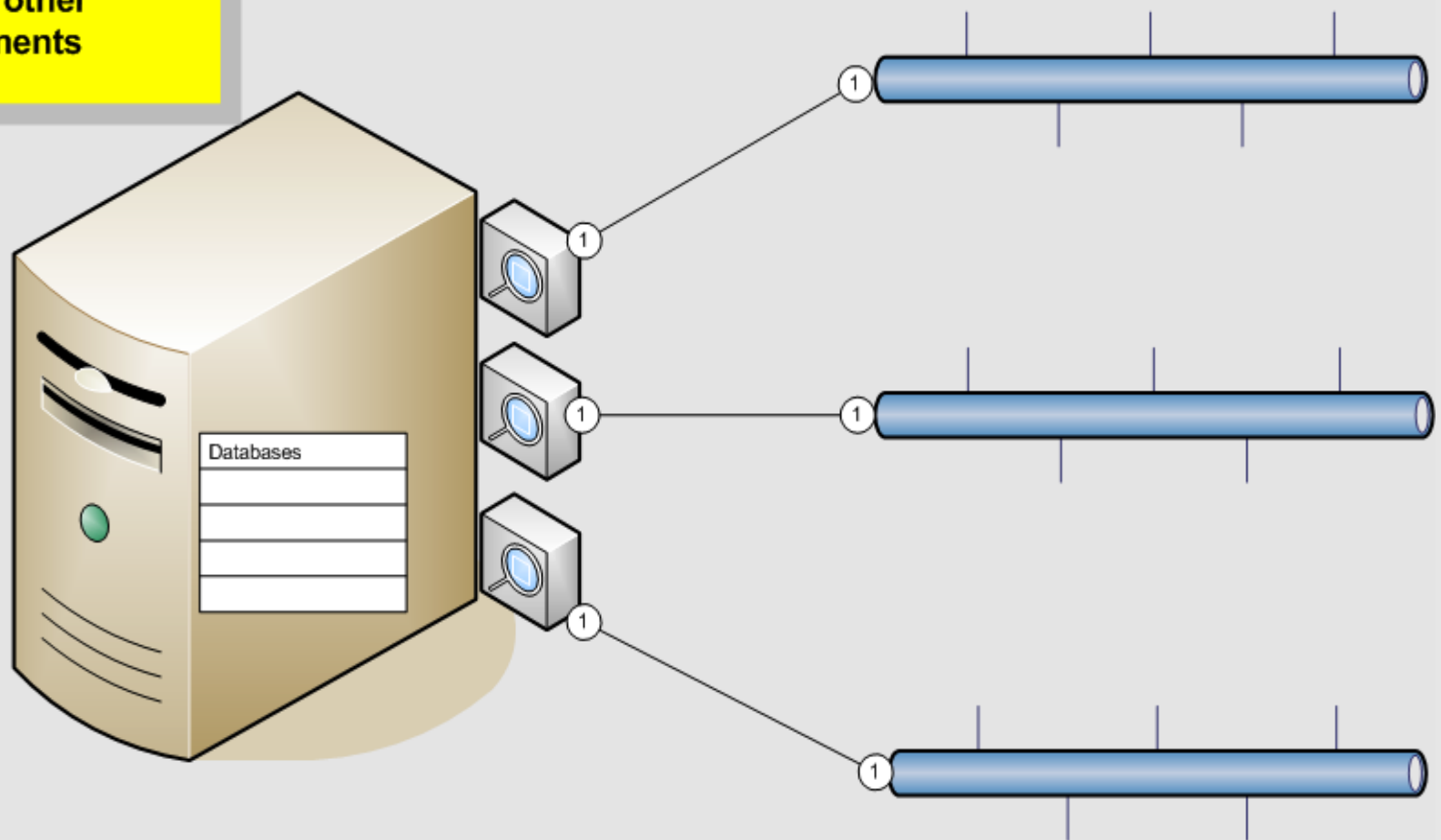
- All in One Boxen
- Separated Boxen(Distributed Environment)

# Sguil - All In One Boxen

- All the sguil components including analysis tools are installed in the same box.
- MySQL is installed in the same box to store alert and session data.
- Sguil client is installed in the same box so that analyst can perform their task.
- Monitor multiple network pipes with multiple of snort(IDS) instances on each separated network interfaces.

# Sguil All In One Box

- Sguil Server
- Sguil Sensor Agents
- Sguil Client
- Mysql DB
- And all other components
- 



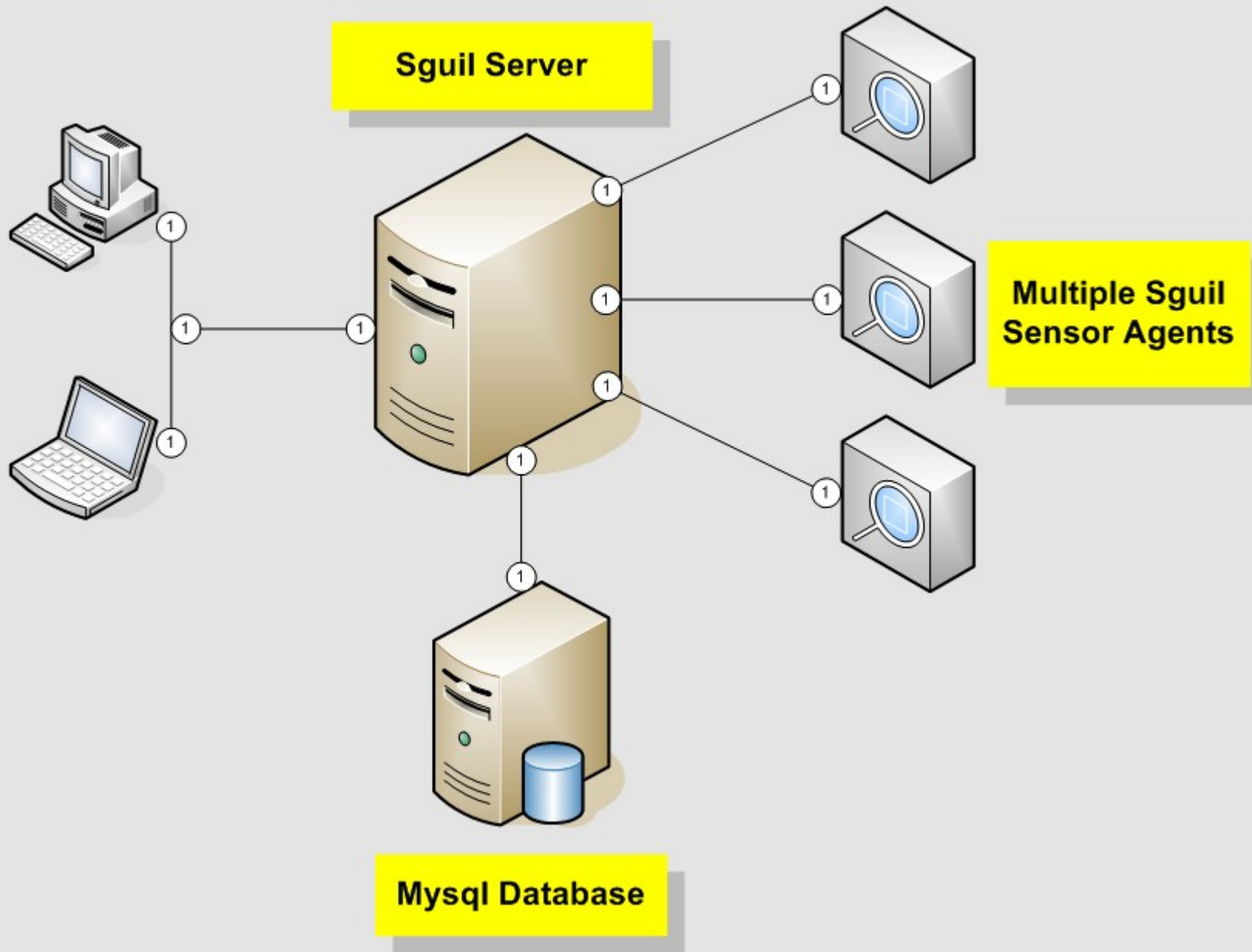
# Sguil - Distributed Environment

- Every sguil components will be installed in separated boxes.
- Sguil server will be standalone with multiple sensor agent boxes connected to it.
- Sguil sensor agents will insert it's alert and session data to the database through sguil server. Full content data is stored in sensor unless pulled by sguil client.
- Sguil client(analyst console) will be launched by connecting to sguil server.

# Sguil In Separated Box – Distributed Environment

## Sguil Client

- Equiped with ethereal and all network analysis tools



# Projects that spawned from Sguil

InstantNSM: Getting NSM work in a glance

– <http://sourceforge.net/projects/instantnsm>

Squert: NSM reporting tool

– <http://squert.sourceforge.net/>

Knoppix-NSM: LiveCD based NSM

– <http://www.securixlive.com/knoppix-nsm/>

# Sguil Misc

You can download the Sguil VMware Image at

<http://www.vmware.com/vmtn/appliances/community.html>

FreeBSD and OpenBSD Sguil installation scripts are available via

[http://www.bejtlich.net/sguil\\_install\\_scripts.tar.gz](http://www.bejtlich.net/sguil_install_scripts.tar.gz)

[http://www.dissectible.org/anonymous/Sguil\\_OBSD/](http://www.dissectible.org/anonymous/Sguil_OBSD/)

# REFERENCE

I don't sell books, but these two books are well recommended in order to deploy NSM framework.

- The Tao Of NSM: Beyond Intrusion Detection System
- Extrusion Detection: Security Monitoring for Internal Intrusions

Both books are written by Richard Bejtlich

# NSM Blog ToRead

- <http://taosecurity.blogspot.com>
- <http://geek00L.blogspot.com>
- <http://infosecpotpourri.blogspot.com>
- <http://proxy.11a.nu>

Q & A

Thank you ..... (: ])