GLOSARIO

Argus	Herramienta para el análisis de flujos del tráfico de red.
CAIDA	Cooperative Association for Internet Data Analysis. Organización dedicada al monitoreo y análisis del tráfico en Internet.
CERT	Computer Emergency Response Team.
DKN	Término para hacer referencia a una Darknet en esta tesis.
DoS	Denial of service. Ataque de negación de servicio que atenta contra la disponibilidad de un sistema o red.
Firewall	Sistema de control y filtrado de paquetes de red.
Honeynet	Estrictamente se refiere a un honeypot de alta interacción (equipo real); comúnmente hace referencia también a un conjunto de honeypots en un ambiente controlado.
Honeypot	Sistema diseñado para ser atacado o alcanzado por tráfico o entidad maliciosa con el fin de detectar y analizar la actividad que ocurre en él.
Honeywall	Sistema de control y análisis del tráfico de red en una honeynet.
IBN	Internet Background Noise. Telescopio de seguridad de la organización SWITCH.
ICMP	Internet Control Message Protocol. Protocolo para control y notificación de errores en el protocolo de Internet (IP).
IDP	Intrusion Detection and Prevention, Sistema de detección y prevención de intrusiones en un sistema o red.
IDS	Intrusion Detection System, Sistema de detección de intrusos en un sistema o red.
IMS	Internet Motion Sensor. Telescopio de red desarrollado por la Universidad de Michigan y la firma Arbor Networks.
IP	Internet Protocol, protocolo de comunicación no orientado a conexión utilizado para establecer comunicación entre equipos de una red.

IPS	Intrusion Prevention System, sistema de prevención de intrusos en un sistema o red.
ISP	Internet Service Provider. Proveedor de servicios de Internet.
Malware	Término para hacer referencia a software malicioso (malicious software)
Payload	Contenido del campo de datos en un paquete de red.
P2P	Peer to Peer. Red de computadoras en las que las conexiones se hacen entre equipos sin necesidad de clientes o servidores. Cada equipo es un nodo.
Ra tolos	Conjunto de herramientas del cliente de Argus.
SAI	Sistema de Atención a Incidentes de la Subdirección de Seguridad de la Información / UNAM-CERT.
Snort	Sistema de detección de intrusos desarrollado por Sourcefire.
SSH	Secure Shell, servicio de red para estableces comunicaciones cifradas entre un cliente y un servidor UNIX.
TCP	Transmission Control Protocol, protocolo de la capa de transporte del modelo TCP/IP.
TSU	Telescopio de Seguridad de la UNAM.
UNAM	Universidad Nacional Autónoma de México.
URL	Uniform Resource Locator. Secuencia de caracteres en un formato estándar para nombrar recursos en Internet.
VRT	Vulnerability Research Team. Equipo de investigación y desarrollo de la firma de seguridad Sourcefire, creadora del IDS Snort.

ANEXOS

ANEXO A – COMPARATIVA DE TIEMPOS DE DETECCIÓN PARA DARKNETS DE DIFERENTES TAMAÑOS

Tabla A.1 Muestra las probabilidades de ver al menos k paquetes en una red /8 cuando un equipo envía 500 paquetes por segundo durante 60 segundos.

k	N	P	P	P
50	500pps * 60sec = 30000 paq	2^{-8}	$P = 1 - \sum_{y=0}^{50-1} \binom{30000}{y} (2^{-8})^{y} (1 - 2^{-8})^{30000-y}$	**≈100%**
75	500pps * 60sec = 30000 paq	2^{-8}	$P = 1 - \sum_{y=0}^{75-1} \binom{30000}{y} (2^{-8})^{y} (1 - 2^{-8})^{30000-y}$	**99.998%**
100	500pps * 60sec = 30000 paq	2^{-8}	$P = 1 - \sum_{y=0}^{100-1} \binom{30000}{y} (2^{-8})^{y} (1 - 2^{-8})^{30000-y}$	**95.2%**
125	500pps * 60sec = 30000 paq	2^{-8}	$P = 1 - \sum_{y=0}^{125-1} \binom{30000}{y} (2^{-8})^{y} (1 - 2^{-8})^{30000-y}$	**24.66%**
150	500pps * 60sec = 30000 paq	2^{-8}	$P = 1 - \sum_{y=0}^{150-1} \binom{30000}{y} (2^{-8})^{y} (1 - 2^{-8})^{30000-y}$	**0.19%**
200	500pps * 60sec = 30000 paq	2^{-8}	$P = 1 - \sum_{y=0}^{200-1} \binom{30000}{y} (2^{-8})^{y} (1 - 2^{-8})^{30000-y}$	**2.05x10-15%**

Tabla A.2 Muestra las probabilidades de ver al menos k paquetes en una red **/16** cuando un equipo envía 1000 paquetes por segundo durante 7 minutos.

K	N	P	P	P [%]
2	1000pps*420sec= 420000paq	2^{-16}	$P = 1 - \sum_{y=0}^{2-1} \binom{420000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**95.397**
4	1000pps*420sec= 420000paq	2^{-16}	$P = 1 - \sum_{y=0}^{4-1} \binom{420000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**76.594**
6	1000pps*420sec= 420000paq	2^{-16}	$P = 1 - \sum_{y=0}^{6-1} \binom{420000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**45.905**
8	1000pps*420sec= 420000paq	2^{-16}	$P = 1 - \sum_{y=0}^{8-1} \binom{420000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**19.769**
10	1000pps*420sec= 420000paq	2^{-16}	$P = 1 - \sum_{y=0}^{10-1} \binom{420000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**6.187**

Tabla A.3 Muestra las probabilidades de ver al menos k paquetes en una red **/16** cuando un equipo envía 1000 paquetes por segundo durante 8 minutos.

K	N	P	P	P [%]
2	1000pps*480sec= 480000paq	2^{-16}	$P = 1 - \sum_{y=0}^{2-1} \binom{480000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**97.683**
4	1000pps*480sec= 480000paq	2^{-16}	$P = 1 - \sum_{y=0}^{4-1} \binom{480000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**85.459**
6	1000pps*480sec= 480000paq	2^{-16}	$P = 1 - \sum_{y=0}^{6-1} \binom{480000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**59.74**
8	1000pps*480sec= 480000paq	2^{-16}	$P = 1 - \sum_{y=0}^{8-1} \binom{480000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**31.405**
10	1000pps*480sec= 480000paq	2^{-16}	$P = 1 - \sum_{y=0}^{10-1} \binom{480000}{y} (2^{-16})^{y} (1 - 2^{-16})^{420000-y}$	**12.312**

ANEXO B – ESQUEMA DE LA BASE DE DATOS PARA ALMACENAMIENTO DE LA INFORMACIÓN DE LOS INCIDENTES DE LA DARKNET

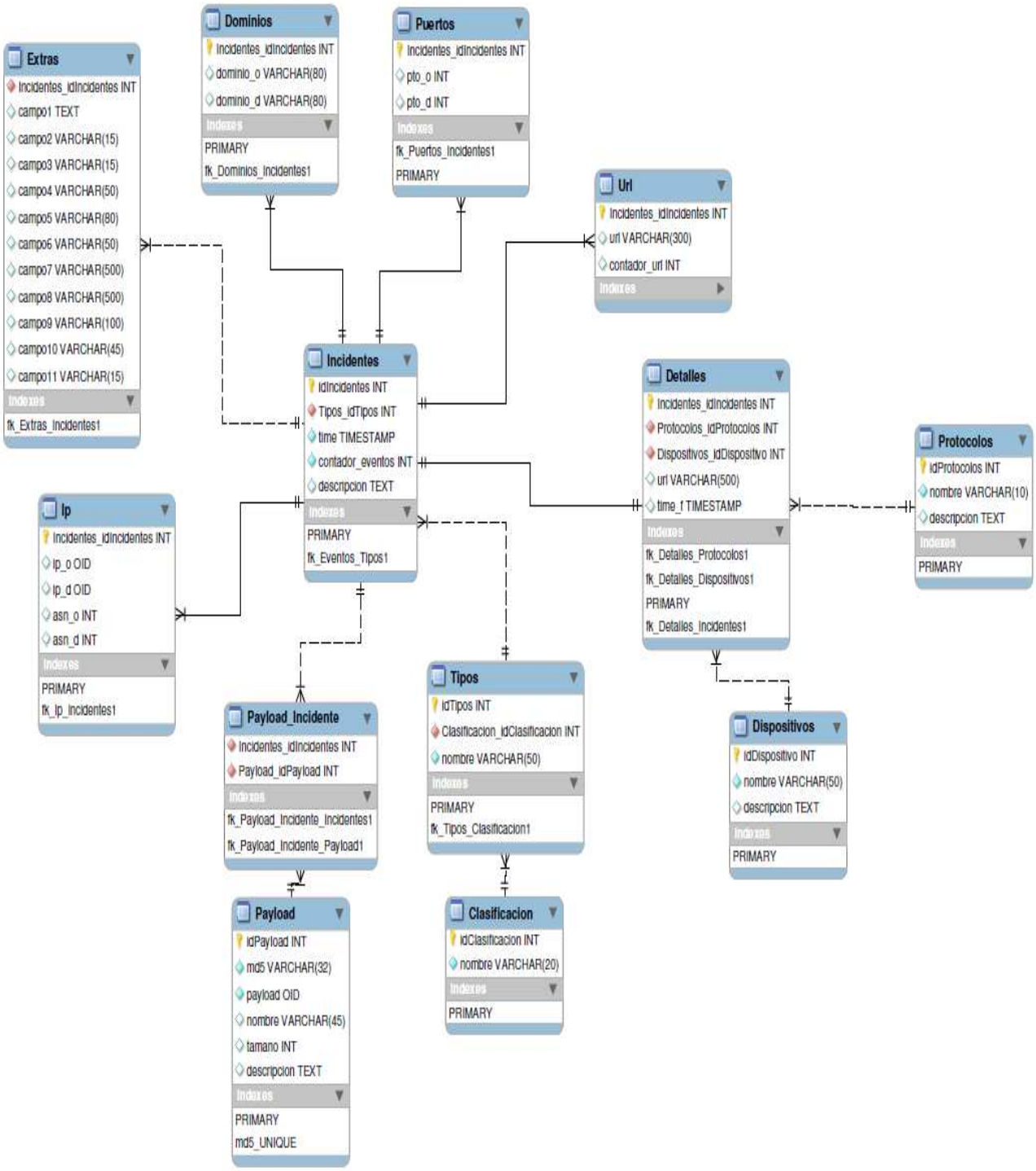

Diagrama B.1 Esquema de la base de datos del TSU

ANEXO C – EJEMPLO DEL FORMATO UNIFICADO PARA ALMACENAMIENTO DE INFORMACIÓN DE INCIDENTES

a) Archivo de incidentes

dkn|163|tcp|83.110.67.184|||||||1271362670|1271362370|SQL WORM 1433|/data/dkn/events_connections/tcp-83.110.67.184-1433-1271362370.det|/data/dkn/events_connections/tcp-83.110.67.184-1433-1271362370.tgz|

b) Archivo de detalles

/data/dkn/events_connections/tcp-83.110.67.184-1433-1271362370.det

TS SRCIP&SPORT SRCIP&DPORT MD5 PAYLOAD STRINGS(Rules)

1271362370|83.110.67.184|3518|132.247.0.232|1433|||||||
1271362378|83.110.67.184|4368|132.247.0.232|1433|285850d4aff8df0e2839ecd6bca68011|||||-(0)|
1271362378|83.110.67.184|4374|132.247.0.232|1433|36dc32801e14fbcdd23436759389f4d4|||||-(0)|
1271362378|83.110.67.184|4394|132.247.0.232|1433|cfd5cff90daae596afab961957826d3c|||||-(0)|
1271362378|83.110.67.184|4432|132.247.0.232|1433|b27e34b029eafa04e44fa4af416ed8cd|||||-(0)|
1271362378|83.110.67.184|4442|132.247.0.232|1433|910729ad1d2de99522b537b05ffd00a2|||||-(0)|
1271362378|83.110.67.184|4446|132.247.0.232|1433|ab1336d70e64574b411b6a133129c557|||||-(0)|

c) Archivo de payloads

```
tmp# tar -zxvf tcp-83.110.67.184-1433-1271362370.tgz
data/honeytrap/attacks/285850d4aff8df0e2839ecd6bca68011
data/honeytrap/attacks/36dc32801e14fbcdd23436759389f4d4
data/honeytrap/attacks/cfd5cff90daae596afab961957826d3c
data/honeytrap/attacks/b27e34b029eafa04e44fa4af416ed8cd
data/honeytrap/attacks/910729ad1d2de99522b537b05ffd00a2
data/honeytrap/attacks/ab1336d70e64574b411b6a133129c557
```

ANEXO D – EJEMPLO DEL ANÁLISIS DE FLUJOS (STA)

a) Archivo general de sesiones de la captura de tráfico en un lapso determinado.

Paquetes/sesión	*IP origen*	*IP destino&puerto*	*Protocolo*
50	113.138.135.169	132.247.0.6.445	tcp
45	113.134.23.32	132.247.0.92.445	tcp
43	113.138.135.169	132.247.0.8.445	tcp
33	180.183.218.8	132.247.0.20.445	tcp
28	180.183.218.8	132.247.0.16.445	tcp
22	113.138.135.169	132.247.0.5.445	tcp
20	113.134.23.32	132.247.0.83.445	tcp
16	113.134.23.32	132.247.0.97.445	tcp
13	67.46.8.42	132.247.0.5.445	tcp
11	67.46.8.42	132.247.0.5.139	tcp
10	66.82.9.22	132.247.0.5.80	tcp
10	180.183.218.8	132.247.0.19.445	tcp
7	180.183.218.8	132.247.0.6.445	tcp
5	180.183.218.8	132.247.0.14.445	tcp

b) Archivo con información estadística sobre la captura

racount	records	total_pkts	src_pkts	dst_pkts	total_bytes	src_bytes	dst_bytes
sum	650	5807	2939	2868	806674	407881	398793

c) Archivo con la relación de actividad entre equipos

```
2.89.94.160: (1) 132.247.0.18
46.166.86.35: (1) 132.247.0.125
50.22.42.62: (6) 132.247.0.66, 132.247.0.70, 132.247.0.78 - 132.247.0.79, 132.247.0.83,
132.247.0.93
58.170.110.136: (1) 132.247.0.80
59.182.11.129: (1) 132.247.0.85
67.46.8.42: (1) 132.247.0.5
83.211.35.77: (1) 132.247.0.15
88.119.145.173: (1) 132.247.0.33
91.220.176.249: (1) 132.247.0.125
92.240.68.153: (1) 132.247.0.186
95.211.81.35: (1) 132.247.0.122
113.134.23.32: (12) 132.247.0.83 - 132.247.0.86, 132.247.0.88 - 132.247.0.90,
132.247.0.92 - 132.247.0.94, 132.247.0.96 - 132.247.0.97
113.138.135.169: (4) 132.247.0.5 - 132.247.0.8
113.165.167.160: (1) 132.247.0.157
114.203.34.204: (1) 132.247.0.113
115.22.231.89: (1) 132.247.0.146
132.247.0.97: (1) 113.134.23.32
178.37.16.115: (1) 132.247.0.216
180.183.218.8: (15) 132.247.0.2 - 132.247.0.3, 132.247.0.5 - 132.247.0.9, 132.247.0.11 -
132.247.0.16, 132.247.0.19 - 132.247.0.20
201.48.211.161: (1) 132.247.0.96
201.225.119.155: (1) 132.247.0.201
202.116.160.171: (1) 132.247.0.159
208.64.126.120: (3) 132.247.0.165, 132.247.0.245, 132.247.0.248
```

d) Archivo con el análisis de payloads de los flujos según reglas

El módulo genera n archivos como este según el número de reglas especificadas.

more stamod_sessions_POSIBLE_WORM_MS-DS_445-tcp-445-string.dat

```
18    113.138.135.169        132.247.0.6.445    s[50]=.....SMBr.......PC NETWORK
15    113.138.135.169        132.247.0.8.445    s[50]=.....SMBr.......PC NETWORK
14      113.134.23.32       132.247.0.92.445    s[50]=.....SMBr.......PC NETWORK
11      180.183.218.8       132.247.0.20.445    s[50]=.....SMBr.......PC NETWORK
 7      113.134.23.32       132.247.0.83.445    s[50]=.....SMBr.......PC NETWORK
 3      180.183.218.8       132.247.0.20.445    s[50]=.....SMBs.........BSRSPYL.A2.
 3    113.138.135.169        132.247.0.6.445    s[50]=...<.SMBs.........BSRSPYL A2.
 2    113.138.135.169        132.247.0.6.445    s[50]=...<.SMBs.........BSRSPYL .A2
 2    113.138.135.169        132.247.0.5.445    s[50]=.....SMBs.........BSRSPYL A2.
 2      113.134.23.32       132.247.0.97.445    s[50]=.....SMBr.......x..PC NETWORK
```

more stamod_sessions_SSH_SCAN_O_POSIBLE_SSH_BRUTEFORCE_ATTACK-tcp-22-string.dat

```
 1      114.247.15.79       132.247.0.92.22     s[50]=SSH-2.0-libssh-0.2.......diff
 1      114.247.15.79       132.247.0.92.22     s[50]=SSH-2.0-libssh-0.2..@....diff
 1      114.247.15.79       132.247.0.92.22     s[50]=SSH-2.0-libssh-0.2..A....diff
 1      114.247.15.79       132.247.0.92.22     s[50]=SSH-2.0-libssh-0.2.......diff
 1      114.247.15.79       132.247.0.92.22     s[50]=SSH-2.0-libssh-0.2.......diff
 1      114.247.15.79       132.247.0.92.22     s[50]=SSH-2.0-libssh-0.2.......diff
 1      114.247.15.79       132.247.0.92.22     s[50]=SSH-2.0-libssh-0.2..h....diff
 1      114.247.15.79       132.247.0.92.22     s[50]=...q3....Y..!..T.N>...4R...y.
 1      114.247.15.79       132.247.0.92.22     s[50]=.n@..?..W....-.1k.Qk.V.t.>A.k
 1      114.247.15.79       132.247.0.92.22     s[50]=N.U+|]o~...8..%..6...[.m.oF..
 1      114.247.15.79       132.247.0.92.22     s[50]=..l. ..*r........k....5L1..\v
 1      114.247.15.79       132.247.0.92.22     s[50]=...].h.o......S.L....IOsQ.n.3
```

ANEXO E – EJEMPLO DE ANÁLISIS DE TRÁFICO DE RED CON IDS (STA)

a) Top de incidencias

```
::::::::::::::
top.alert
::::::::::::::
297     |       SQL SA brute force login attempt TDS v7/8
45      |       WEB-IIS view source via translate header
12      |       SQL Worm propagation attempt
12      |       SQL version overflow attempt
12      |       SQL Worm propagation attempt OUTBOUND
6       |       NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt
4       |       POLICY VNC server response
3       |       ET SCAN Behavioral Unusual Port 1433 traffic, Potential Scan or Infection
2       |       ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)
2       |       EXPLOIT RealVNC server authentication bypass attempt
2       |       ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15)
1       |       ET SCAN Sipvicious Scan

::::::::::::::
top.class
::::::::::::::
297     |        [Classification: An attempted login using a suspicious username was detected] [Priority:
2]
45      |        [Classification: access to a potentially vulnerable web application] [Priority: 2]
24      |        [Classification: Misc Attack] [Priority: 2]
22      |        [Classification: Attempted Administrator Privilege Gain] [Priority: 1]
9       |        [Classification: Misc activity] [Priority: 3]
1       |        [Classification: Attempted Information Leak] [Priority: 2]

::::::::::::::
top.dstip
::::::::::::::
276     |       SQL SA brute force login attempt TDS v7/8||132.247.0.25
21      |       SQL SA brute force login attempt TDS v7/8||132.247.0.11
3       |       WEB-IIS view source via translate header||132.247.0.8
3       |       WEB-IIS view source via translate header||132.247.0.6
2       |       POLICY VNC server response||132.247.0.26
2       |       POLICY VNC server response||132.247.0.58
2       |       WEB-IIS view source via translate header||132.247.0.4
1       |       SQL version overflow attempt||132.247.0.200
1       |       EXPLOIT RealVNC server authentication bypass attempt||132.247.0.26
1       |       SQL Worm propagation attempt OUTBOUND||132.247.0.158
1       |       SQL Worm propagation attempt||132.247.0.167
1       |       SQL Worm propagation attempt||132.247.0.230
1       |       SQL Worm propagation attempt||132.247.0.117
1       |       SQL Worm propagation attempt||132.247.0.19
1       |       SQL Worm propagation attempt||132.247.0.87
1       |       SQL Worm propagation attempt||132.247.0.162
1       |       SQL Worm propagation attempt||132.247.0.178
1       |       SQL version overflow attempt||132.247.0.162
1       |       WEB-IIS view source via translate header||132.247.0.21
1       |       SQL Worm propagation attempt||132.247.0.57
1       |       SQL version overflow attempt||132.247.0.169

::::::::::::::
top.dstport
::::::::::::::
297     |       SQL SA brute force login attempt TDS v7/8||1433
45      |       WEB-IIS view source via translate header||80
12      |       SQL Worm propagation attempt OUTBOUND||1434
12      |       SQL version overflow attempt||1434
12      |       SQL Worm propagation attempt||1434
4       |       POLICY VNC server response||5900
3       |       ET SCAN Behavioral Unusual Port 1433 traffic, Potential Scan or Infection||1433
2       |       EXPLOIT RealVNC server authentication bypass attempt||5900
2       |       ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)||445
2       |       ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15)||445
1       |       ET SCAN Sipvicious Scan||5060
```

```
::::::::::::::
top.srcip
::::::::::::::
276     |       SQL SA brute force login attempt TDS v7/8||216.14.118.202
21      |       SQL SA brute force login attempt TDS v7/8||62.149.163.103
19      |       WEB-IIS view source via translate header||116.10.255.17
13      |       WEB-IIS view source via translate header||221.172.58.255
6       |       SQL Worm propagation attempt OUTBOUND||211.138.238.198
6       |       SQL Worm propagation attempt||211.138.238.198
6       |       SQL version overflow attempt||211.138.238.198
5       |       WEB-IIS view source via translate header||117.206.96.68
2       |       POLICY VNC server response||190.209.54.203
```

b) Información por alerta

```
::::::::::::::
ETEXPLOITMicrosoft_Windows_NETAPI_Stack_Overflow_Inbound_-_MS08-067__25).top
::::::::::::::


[  TOP IP ADDRESS ]
[ ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)  ]
[  DST CONNECTIONS  ]
                  1    ->      132.247.0.57
                  1    ->      132.247.0.18


[  TOP IP ADDRESS ]
[ ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)  ]
[  SRC CONNECTIONS  ]
                  1    ->      132.247.17.12
                  1    ->      132.247.17.4


[  TOP PORTS ]
[ ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)  ]
[  DST CONNECTIONS  ]
                  2    ->      [ 445 ]


[  TOP PORTS ]
[ ET EXPLOIT Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (25)  ]
[  SCR CONNECTIONS  ]
                  1    ->      [ 2714 ]
                  1    ->      [ 2677 ]



::::::::::::::
NETBIOSSMB-DSsrvsvc_NetrPathCanonicalize_WriteAndX_little_endian_overflow_attempt.top
::::::::::::::


[  TOP IP ADDRESS ]
[ NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt  ]
[  DST CONNECTIONS  ]
                  1    ->      132.247.0.76
                  1    ->      132.247.0.57
                  1    ->      132.247.0.15
                  1    ->      132.247.0.18
                  1    ->      132.247.0.8
                  1    ->      132.247.0.39


[  TOP IP ADDRESS ]
[ NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt  ]
[  SRC CONNECTIONS  ]
                  3    ->      132.247.17.4
                  3    ->      132.247.17.12


[  TOP PORTS ]
[ NETBIOS SMB-DS srvsvc NetrPathCanonicalize WriteAndX little endian overflow attempt  ]
[  DST CONNECTIONS  ]
                  6    ->      [ 445 ]
```

ANEXO F – EJEMPLO DE INFORMACIÓN ALMACENADA EN EL TSU

Con el diseño de la base de datos se pueden hacer consultas tan específicas como se deseen. A continuación se muestran dos ejemplos.

a) Incidentes reportados

```
1673745 | 2011-02-03 02:24:51 | 5b799e45c5f0dafa24cbe619231d2cc2 | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | f7f3d106107fbf546fc794241575da7c | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | 01ca38ad531f36358934cd3502b3334c | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | 93c9266d46ec8d198e2098dff76e924d | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | 173dc42d82b8601bed9eed90b24ec081 | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | 153d7cd4d182df7ad684d65d91875c91 | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | f04ede2677abfa415ebdf67c75fceb91 | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | 29d9545b825a128c214c603acc5e13ee | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673745 | 2011-02-03 02:24:51 | 7afc42de0745f7e3047ff02b4b0e57fc | SSH SCAN O POSIBLE SSH BRUTEFORCE ATTACK
1673748 | 2011-02-03 02:26:09 | a0aa4a74b70cbca5a03960df1a3dc878 | SQL WORM 1434
1673749 | 2011-02-03 02:27:08 | 99e30239984e4c331bcc2986643d066b | GENERAL SCAN PORT [17871]
1673751 | 2011-02-03 02:30:01 | d56e7f0145ed8e9b996c169d576bdbef | GENERAL SCAN PORT [19814]
1673752 | 2011-02-03 02:30:40 | 07d39626a6f0a2d4b0bcb98b5d30d1b6 | GENERAL SCAN PORT [33435]
1673754 | 2011-02-03 02:30:54 | 07d39626a6f0a2d4b0bcb98b5d30d1b6 | PORTSWEEP
1673756 | 2011-02-03 02:33:08 | 0262ca5d4446a40394f6f7e83804bdd4 | GENERAL SCAN PORT [18423]
1673757 | 2011-02-03 02:33:16 | 2afe80d2d26ad50b52f0157eacb5870c | GENERAL SCAN PORT [16617]
1673758 | 2011-02-03 02:34:09 | 99e30239984e4c331bcc2986643d066b | GENERAL SCAN PORT [17871]
1673773 | 2011-02-03 02:42:54 | 07d39626a6f0a2d4b0bcb98b5d30d1b6 | PORTSWEEP
1673774 | 2011-02-03 02:43:45 | d56e7f0145ed8e9b996c169d576bdbef | GENERAL SCAN PORT [19814]
1673775 | 2011-02-03 02:43:55 | 99e30239984e4c331bcc2986643d066b | GENERAL SCAN PORT [6305]
1673779 | 2011-02-03 02:45:20 | 40329bee034a98c02454a3479ef5e6a9 | GENERAL SCAN PORT [19838]
1673783 | 2011-02-03 02:49:13 | 4302dbc6caa9c9ec6d0e3f47282746c0 | GENERAL SCAN PORT [19812]
1673784 | 2011-02-03 02:50:28 | b79073b70f3c61c6af2f07997a247b33 | GENERAL SCAN PORT [17871]
1673785 | 2011-02-03 02:50:28 | 99e30239984e4c331bcc2986643d066b | GENERAL SCAN PORT [17871]
1673786 | 2011-02-03 02:50:34 | c90329e824064e777f8719643320923f | GENERAL SCAN PORT [19677]
1673788 | 2011-02-03 03:04:14 | ef401db3ed6bb1ab29c5cdc06cfeb636 | GENERAL SCAN PORT [6305]
1673789 | 2011-02-03 03:04:14 | 99e30239984e4c331bcc2986643d066b | GENERAL SCAN PORT [6305]
1673797 | 2011-02-03 03:06:20 | d56e7f0145ed8e9b996c169d576bdbef | GENERAL SCAN PORT [19814]
1673798 | 2011-02-03 03:06:21 | 16d5ef7e85234f256f5e4b6b70519f27 | GENERAL SCAN PORT [4899]
1673798 | 2011-02-03 03:06:21 | d5e36a27c2d953a56652820e7563fa49 | GENERAL SCAN PORT [4899]
1673799 | 2011-02-03 02:52:13 | c9edc6804196dc694eb346cf62f9067f | GENERAL SCAN PORT [6133]
1673800 | 2011-02-03 02:52:26 | d56e7f0145ed8e9b996c169d576bdbef | GENERAL SCAN PORT [19814]
1673801 | 2011-02-03 02:52:26 | 15fd6c77950d29548982fb44b6ddd4a3 | GENERAL SCAN PORT [19814]
1673802 | 2011-02-03 02:53:58 | a0aa4a74b70cbca5a03960df1a3dc878 | SQL WORM 1434
1673807 | 2011-02-03 02:57:44 | 99e30239984e4c331bcc2986643d066b | GENERAL SCAN PORT [17871]
1673809 | 2011-02-03 02:59:34 | d56e7f0145ed8e9b996c169d576bdbef | GENERAL SCAN PORT [19814]
1673811 | 2011-02-03 02:59:50 | 420bc97a9e2304d22d7382fec7a8571c | GENERAL SCAN PORT [19556]
1673812 | 2011-02-03 03:00:09 | 685d502a075912c4227e12e28c7885a8 | GENERAL SCAN PORT [23680]
1673816 | 2011-02-03 03:00:32 | a0aa4a74b70cbca5a03960df1a3dc878 | SQL WORM 1434
1673819 | 2011-02-03 03:02:57 | a0aa4a74b70cbca5a03960df1a3dc878 | SQL WORM 1434
1673821 | 2011-02-03 03:11:08 | 62abf75a6760ee1a4cdcb2a1fe89d0ac | GENERAL SCAN PORT [19814]
1673823 | 2011-02-03 03:11:32 | 99e30239984e4c331bcc2986643d066b | GENERAL SCAN PORT [6305]
1673826 | 2011-02-03 03:12:20 | a0aa4a74b70cbca5a03960df1a3dc878 | SQL WORM 1434
1673827 | 2011-02-03 03:12:33 | a0aa4a74b70cbca5a03960df1a3dc878 | SQL WORM 1434
1673828 | 2011-02-03 03:14:01 | 3c0a1a13a0469bb1803c5e4270ea91a4 | GENERAL SCAN PORT [51464]
1673833 | 2011-02-03 03:15:43 | d56e7f0145ed8e9b996c169d576bdbef | GENERAL SCAN PORT [19814]
```

b) Detalles de eventos específicos

```
1673734 | 2011-02-03 02:19:48 | 218.15.136.38 | 32911  | 132.248.194.73 | 22 | b83ba7ca61feeb830a04fe4ae889966c
1673734 | 2011-02-03 02:19:52 | 218.15.136.38 | 33158  | 132.248.194.73 | 22 | 7c6147f2417a5b74b1fe9585a43dd676
1673734 | 2011-02-03 02:19:55 | 218.15.136.38 | 33397  | 132.248.194.73 | 22 | 44eec06e38e7649b7d98412b18983087
1673734 | 2011-02-03 02:19:58 | 218.15.136.38 | 33660  | 132.248.194.73 | 22 | aae658a6b4b4ed274c6225c18e8a4346
1673734 | 2011-02-03 02:20:02 | 218.15.136.38 | 33910  | 132.248.194.73 | 22 | a8cbf2a3a2e442fc5059ce1ad9371742
1673734 | 2011-02-03 02:20:05 | 218.15.136.38 | 34155  | 132.248.194.73 | 22 | e5cbae0b5ca3b2a8b022a389339c7d2b
1673734 | 2011-02-03 02:20:09 | 218.15.136.38 | 34397  | 132.248.194.73 | 22 | 311a9b35473b14284d24d6c3d9eea2cb
1673734 | 2011-02-03 02:20:12 | 218.15.136.38 | 34631  | 132.248.194.73 | 22 | b50533d3352fcc9c3855783192ca8081
1673734 | 2011-02-03 02:20:16 | 218.15.136.38 | 34904  | 132.248.194.73 | 22 | e4c6cd45d1c296ff1ec9a87c03507a74
1673734 | 2011-02-03 02:20:19 | 218.15.136.38 | 35127  | 132.248.194.73 | 22 | 5ae5b60ec9eec88177817a728e956e2c
1673734 | 2011-02-03 02:20:23 | 218.15.136.38 | 35374  | 132.248.194.73 | 22 | 49bd374892df8ef3686a10803c4620bc
1673734 | 2011-02-03 02:20:26 | 218.15.136.38 | 35627  | 132.248.194.73 | 22 | d28eedc5a297e4ebffd93edd456bea87
```

ANEXO G – EJEMPLOS DE BITÁCORAS DEL MÓDULO

a) DKN AGENT

```
[2011-01-28 14:24:29] - [AGENT | check_active_events   ] STARTING SCP TRANSFER MODE (NO DB) (360)sec
[2011-01-28 14:24:29] - [AGENT | check_active_events   ] STARTING STAMOD (120)sec
[2011-01-28 14:24:29] - [AGENT | stamod                 ] ERROR Unable to exec STAMOD. Min time must be
(300) sec.
[2011-01-28 14:24:29] - [AGENT | stamod                ] FIXING The program will execute each (300) sec.
[2011-01-28 14:24:29] - [AGENT | stamod                ] Executing STA Module PID Handler(15841)
[2011-01-28 14:24:29] - [AGENT(0) | check_active_events] STARTING VERIFICATION PROCESS
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file  ]      Expiring event AEV: [X|tcp-109.72.207.69-
53|1296182653|1296182353|GENERAL SCAN PORT [53]|]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file    ]        Adding incident to agent file :
[/data/dkn/tmp/AGENT0.exp]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file  ]      Expiring event AEV: [X|tcp-92.240.68.152-
80|1296183021|1296182721|GENERAL SCAN PORT [80]|]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file    ]        Adding incident to agent file :
[/data/dkn/tmp/AGENT0.exp]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file  ]      Expiring event AEV: [X|udp-132.248.204.1-
46594|1296183027|1296182727|GENERAL SCAN PORT [46594]|]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file    ]        Adding incident to agent file :
[/data/dkn/tmp/AGENT0.exp]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file  ]     Expiring event AEV: [X|udp-132.248.204.1-53-
132.248.194.73|1296183027|1296182730|PORTSWEEP|]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file    ]        Adding incident to agent file :
[/data/dkn/tmp/AGENT0.exp]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file  ]      Expiring event AEV: [X|tcp-12.139.31.211-
135|1296183095|1296182795|GENERAL SCAN PORT [135]|]
[2011-01-28 14:24:29] - [AGENT(0) | expire_event_file    ]        Adding incident to agent file :
[/data/dkn/tmp/AGENT0.exp]

 [2011-01-28 14:24:33] - [AGENT(0) | proc_events              ]         Logging new Incident from
[/data/dkn/events_connections/udp-119.248.51.32-37927-1296186220.evt]
[2011-01-28 14:24:33] - [AGENT(0) | createtar                      ]          Creating Tar file
(/data/dkn/events_connections/udp-114.252.89.39-37927-1296186220.tgz)                                with
(/data/dkn/tmp/attacks/445f18dc3bb3de26d491685b249a9dd1)
[2011-01-28 14:24:33] - [AGENT(0) | proc_events              ]         Logging new Incident from
[/data/dkn/events_connections/udp-114.252.89.39-37927-1296186220.evt]
[2011-01-28 14:24:33] - [AGENT(0) | createtar                      ]          Creating Tar file
(/data/dkn/events_connections/udp-60.6.52.199-37927-1296186147.tgz)                                  with
(/data/dkn/tmp/attacks/0eb0c3ca996d3648705416c4a69132cf)
[2011-01-28 14:24:33] - [AGENT(0) | proc_events              ]         Logging new Incident from
[/data/dkn/events_connections/udp-60.6.52.199-37927-1296186147.evt]
[2011-01-28 14:24:33] - [AGENT(0) | createtar                      ]          Creating Tar file
(/data/dkn/events_connections/udp-120.8.105.140-37927-1296186178.tgz)                                with
(/data/dkn/tmp/attacks/473ddda95ba18f00c4123e7f3e895b76)
[2011-01-28 14:24:33] - [AGENT(0) | proc_events              ]         Logging new Incident from
[/data/dkn/events_connections/udp-120.8.105.140-37927-1296186178.evt]
[2011-01-28 14:24:33] - [AGENT(0) | createtar                      ]          Creating Tar file
(/data/dkn/events_connections/udp-110.245.128.240-37927-1296186169.tgz)                              with
(/data/dkn/tmp/attacks/29204203152f28cbac02df22e4d86a8
0)
[2011-01-28 14:24:33] - [AGENT(0) | proc_events              ]         Logging new Incident from
[/data/dkn/events_connections/udp-110.245.128.240-37927-1296186169.evt]
[2011-01-28 14:24:33] - [AGENT(0) | createtar                      ]          Creating Tar file
(/data/dkn/events_connections/udp-124.67.37.34-37927-1296186201.tgz) with

[2011-01-28 14:30:34] - [AGENT(33) | proc_events              ]         Logging new Incident from
[/data/dkn/events_connections/udp-132.248.204.1-53-132.248.194.73-1296246342.evt]
[2011-01-28 14:30:35] - [AGENT | transfer_file                        ]            Transfering
(192.168.1.1:2290|dkn|****|/data/incidents/|/data/dkn/events_connections/alert-TCP-201.127.23.156-
COMMUNITYWEB-ATTACKSGFIMailSecurit
yManagementHostOverflowAttemptLongAcceptParameter.det) PID Handler (15840)->(21512)
[2011-01-28 14:30:35] - [AGENT | transfer_file                        ]            Transfering
(192.168.1.1:2290|dkn|****|/data/incidents/|/data/dkn/events_connections/alert-TCP-189.136.44.47-
COMMUNITYWEB-ATTACKSGFIMailSecurity
ManagementHostOverflowAttemptLongAcceptParameter.det) PID Handler (15840)->(21512)
[2011-01-28 14:30:35] - [AGENT | transfer_file                        ]            Transfering
(192.168.1.1:2290|dkn|****|/data/incidents/|/data/dkn/events_connections/tcp-221.172.58.255-445-
1296183060.det) PID Handler (15840)-
>(21511)
[2011-01-28 14:30:35] - [AGENT | transfer_file                        ]            Transfering
(192.168.1.1:2290|dkn|****|/data/incidents/|/data/dkn/events_connections/alert-TCP-187.137.97.229-
COMMUNITYWEB-ATTACKSGFIMailSecurit
yManagementHostOverflowAttemptLongAcceptParameter.det) PID Handler (15840)->(21512)
```

b) DKN STA

```
[2011-01-28 14:29:29] - ************* [STRUCTURED TRAFFIC ANALYSIS MODULE] **************
[2011-01-28 14:29:29] - ************************************************************

[2011-01-28 14:29:29] - [STAMOD | getdata       ] STARTING STA MODULE
[2011-01-28 14:29:29] - [STAMOD | getdata       ] |- Creating STA log directory        (/data/dkn/stamod/20110128-1429) ->
[2011-01-28 14:29:29] - [STAMOD | getdata       ] |- Creating STA Argus directory      (/data/dkn/stamod/20110128-1429/argus)
->
[2011-01-28 14:29:29] - [STAMOD | getdata       ] |- Creating STA Snort directory      (/data/dkn/stamod/20110128-1429/snort)
->
[2011-01-28 14:29:29] - [STAMOD | getdata           ] |- Creating STA procfiles directory   (/data/dkn/stamod/20110128-
1429/snort/procfiles/) ->
[2011-01-28 14:29:29] - [STAMOD | getdata           ] |- Creating STA alert top directory   (/data/dkn/stamod/20110128-
1429/snort/alert_top/) ->
[2011-01-28 14:29:29] - [STAMOD | getdata           ] |- Creating STA alert info directory (/data/dkn/stamod/20110128-
1429/snort/alert_info/) ->
[2011-01-28 14:29:29] - [STAMOD | argus_exec    ] |- Stopping argus daemon ... OK
[2011-01-28 14:29:29] - [STAMOD | argus_exec    ] |- Starting argus daemon ... OK
[2011-01-28 14:29:29] - [STAMOD | argus_data    ] |- GENERATING ARGUS DATA
[2011-01-28 14:29:29] - [STAMOD | argus_data    ]      |- Creating racount file           ... OK
[2011-01-28 14:29:32] - [STAMOD | argus_data    ]      |- Creating hosts file             ... OK
[2011-01-28 14:29:37] - [STAMOD | argus_data    ]      |- Creating traffic sessions file  ... OK
[2011-01-28 14:29:44] - [STAMOD | argus_data    ]      |- Creating traffic sessions of defined rules ->
[2011-01-28 14:29:44] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-22-[-]>  ... OK
[2011-01-28 14:29:46] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-22>  ... OK
[2011-01-28 14:29:48] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-1433-[-]>  ... OK
[2011-01-28 14:29:51] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-1433>  ... OK
[2011-01-28 14:29:53] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-1434-[-]>  ... OK
[2011-01-28 14:29:55] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-1434>  ... OK
[2011-01-28 14:29:58] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <udp-1434-[-]>  ... OK
[2011-01-28 14:30:00] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <udp-1434>  ... OK
[2011-01-28 14:30:02] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-6666-[PING]>  ... OK
[2011-01-28 14:30:04] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-6666>  ... OK
[2011-01-28 14:30:07] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-6667-[PONG]>  ... OK
[2011-01-28 14:30:08] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-6667>  ... OK
[2011-01-28 14:30:11] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-6668-[-]>  ... OK
[2011-01-28 14:30:13] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-6668>  ... OK
[2011-01-28 14:30:15] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-6669-[-]>  ... OK
[2011-01-28 14:30:18] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-6669>  ... OK
[2011-01-28 14:30:20] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-25-[-]>  ... OK
[2011-01-28 14:30:22] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-25>  ... OK
[2011-01-28 14:30:25] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-5900-[-]>  ... OK
[2011-01-28 14:30:27] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-5900>  ... OK
[2011-01-28 14:30:29] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-139-[-]>  ... OK
[2011-01-28 14:30:32] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-139>  ... OK
[2011-01-28 14:30:36] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-445-[-]>  ... OK
[2011-01-28 14:30:46] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-445>  ... OK
[2011-01-28 14:30:53] - [STAMOD | argus_radata_r]         |- Creating stats REGEX PAYLOAD for rule <tcp-9000-[PING]>  ... OK
[2011-01-28 14:30:56] - [STAMOD | argus_radata_r]         |- Creating stats GENERAL for rule <tcp-9000>  ... OK
[2011-01-28 14:30:59] - [STAMOD | snort_data    ] |- STARTING SNORT ANALYSIS WITH (/data/dkn/stamod/20110128-1429/20110128-
1429.cap) and OUTDIR (/data/dkn/stamod/20110128-1429) SNORTCONF (/usr/local/snort/etc/s
nort.conf)    ...  [2011-01-28 14:31:33] - [STAMOD | snort_data        ]           |- Setting SNORT alert file to
(/data/dkn/stamod/20110128-1429/snort/procfiles//sta_snortalert) ->
[2011-01-28 14:31:33] - [STAMOD | snort_data     ]        |- Setting SNORT log file (pcap) to (/data/dkn/stamod/20110128-
1429/snort/procfiles//sta_snortalert) ... OK
[2011-01-28 14:31:33] - [STAMOD | convalert        ]          |- Converting to pipe format (/data/dkn/stamod/20110128-
1429/snort/procfiles//sta_snortalert)
[2011-01-28 14:31:33] - [STAMOD | snort_top     ]      |- Starting SNORT top processing
[2011-01-28 14:31:33] - [STAMOD | snort_alert   ]      |- Processing information of top alerts [dstip]
[2011-01-28 14:31:33] - [STAMOD | snort_alert   ]      |- Processing information of top alerts [srcip]
[2011-01-28 14:31:33] - [STAMOD | snort_alert   ]      |- Processing information of top alerts [dstport]
[2011-01-28 14:31:33] - [STAMOD | snort_alert   ]      |- Processing information of top alerts [srcport]
[2011-01-28 14:31:33] - [STAMOD | getdata        ] |- Verifying argus daemon or retrying start ... [2011-01-28 14:31:33] -
[STAMOD | argus_exec    ] |- Starting argus daemon ... [2011-01-28 14:31:33] -
Process terminated.
```