ACME! Computer Security Research

Rastreando fluxos para detecção de eventos em redes

GTER - Grupo de Trabalho de Engenharia e Operação de Redes
27ª Reunião

19 de junho de 2009

Jorge Luiz Corrêa
André Proto

ACME! Computer Security Research
UNESP – IBILCE – São José do Rio Preto – SP
Coordenador: Prof. Dr. Adriano Mauro Cansian

jorge@acmesecurity.org

andreproto@acmesecurity.org

ACME! Computer Security Research

Agenda

- Motivação e objetivos.
- Fluxos e exportação.
- Coleta: arquitetura de armazenamento.
- Assinaturas.
- Modelo de rastreamento de fluxos.
- Resultados.

ACME! Computer Security Research

Agenda

- **Motivação e objetivos.**
- Fluxos e exportação.
- Coleta: arquitetura de armazenamento.
- Assinaturas.
- Modelo de rastreamento de fluxos.
- Resultados.

ACME! Computer Security Research

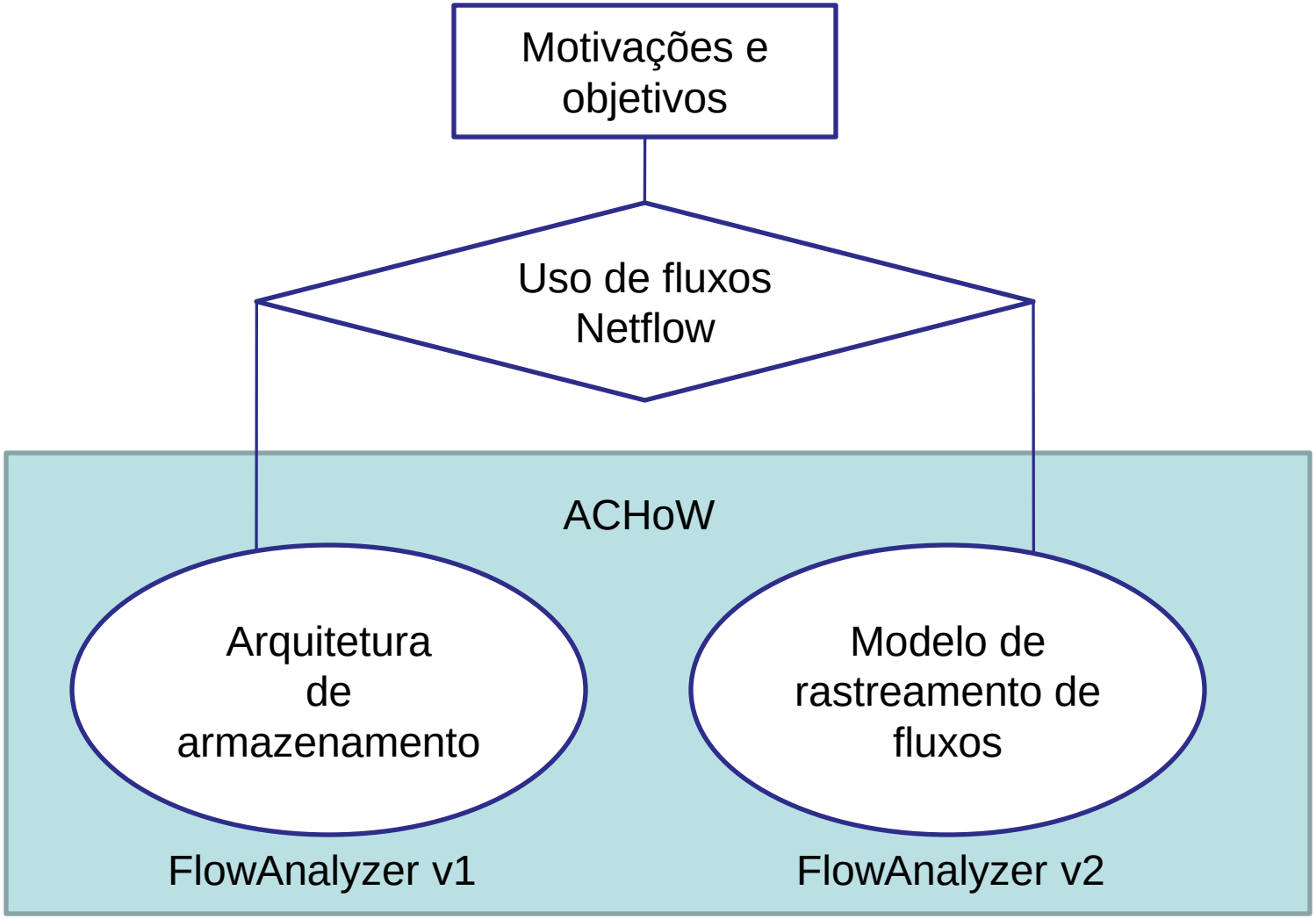
Motivação e objetivos

- A principal motivação é a necessidade dentro do Instituto de se *identificar* determinados tipos de tráfego, principalmente:
  - Consumo abusivo de banda;
  - Aplicações que infringem a política de rede da Universidade;
  - Disseminação de artefatos maliciosos;
  - De forma rápida e com informações relevantes.

Motivação e objetivos (2)

- Assim, os objetivos são:
  - Monitorar sem interferir diretamente no tráfego (sem análise de *payload*);
  - Desenvolver um ponto único de monitoramento;
  - Baixo custo;
  - Versatilidade na manipulação de fluxos;
  - Descrever eventos em meio a totalidade de fluxos;
  - Criar uma ferramenta que auxilie na busca por ocorrências passadas (análise pericial).

Motivação e objetivos (3)



ACME! Computer Security Research

Agenda

- Motivação e objetivos.
- **Fluxos e exportação.**
- Coleta: arquitetura de armazenamento.
- Assinaturas.
- Modelo de rastreamento de fluxos.
- Resultados.

ACME! Computer Security Research

Fluxos e exportação

- Todo o sistema é baseado em informações fornecidas pelos fluxos de rede.
- Netflow v5 (motivos):
  - Restrições do ambiente do Instituto;
  - Pesquisas e ferramentas anteriores utilizaram esta versão;
  - *Cumpre a demanda,* com uma complexidade inferior.
- Importante:
  - Netflow v5 não permite controlar taxa de amostragem.
    - Isto é importante para a detecção de eventos.

Fluxos e exportação (2)

Registro de fluxo - Netflow versão 5

Byte 3	Byte 2	Byte 1	Byte 0

source ip address			
destination ip address			
next hop ip address			
input interface index		**output interface index**	
packets			
bytes			
start time of flow			
end time of flow			
source port		**destination port**	
pad	**tcp flags**	**ip protocol**	tos
source AS		destination AS	
src netmask length	dst netmask length	padding	

Nem todos os campos são utilizados.

ACME! Computer Security Research

Agenda

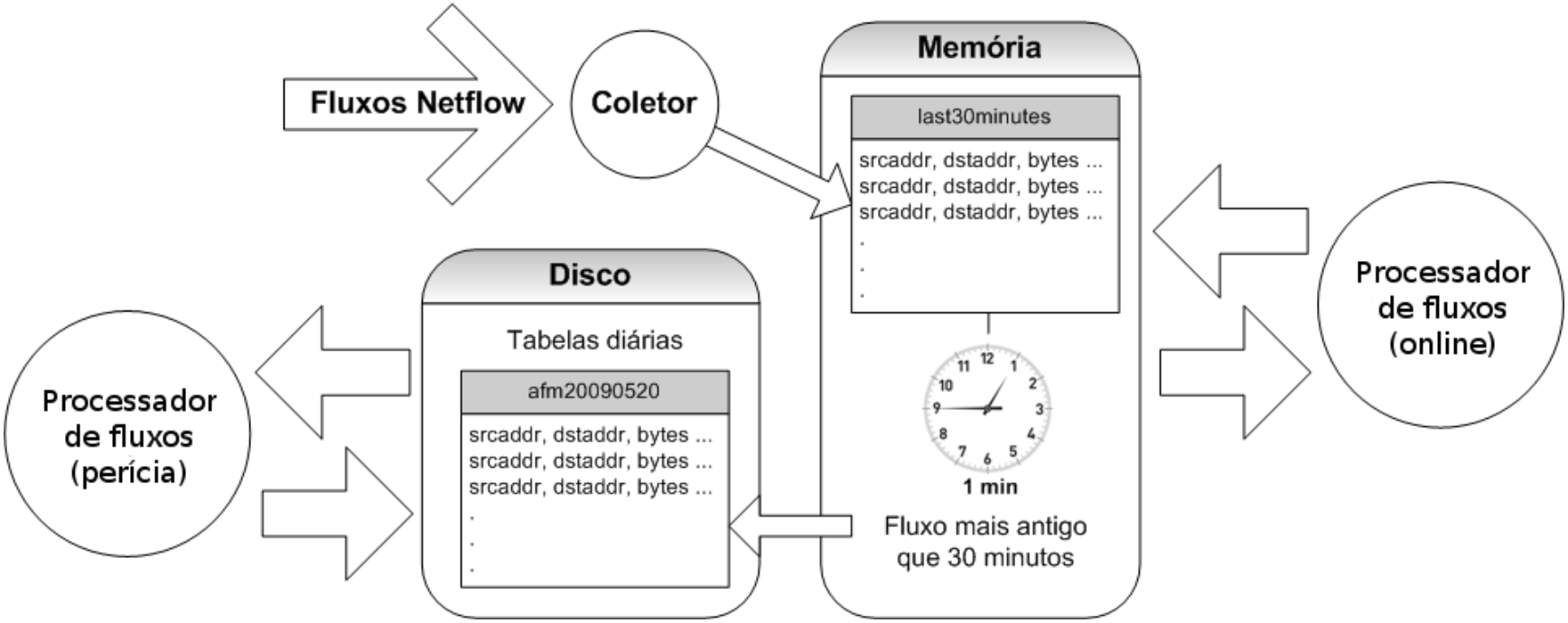
- Motivação e objetivos.
- Fluxos e exportação.
- **Coleta: arquitetura de armazenamento.**
- Assinaturas.
- Modelo de rastreamento de fluxos.
- Resultados.

Coleta: arquitetura de armazenamento

- **Coletor**
  - Software responsável por receber fluxos Netflow, fazer o tratamento de dados e armazenar no banco;
  - Cria o *schema* e as tabelas automaticamente.
- **Características do banco de dados**
  - Utiliza uma tabela em memória para os últimos 30 minutos de fluxos;
  - No disco, tabelas são separadas por dia;
  - Cada tabela é indexada pela marca de tempo do campo *first*;
  - Procedimento executa a cada minuto para retirar fluxos da memória e armazenar em disco (facilita indexação);
  - *Views* são possíveis, mas utilizadas com cautela.
    - Ex.: semana, mês, input, output, etc.

Coleta: arquitetura de armazenamento (2)

Arquitetura de armazenamento



ACME! Computer Security Research

Agenda

- Motivação e objetivos.
- Fluxos e exportação.
- Coleta: arquitetura de armazenamento.
- **Assinaturas.**
- Modelo de rastreamento de fluxos.
- Resultados.

Assinaturas

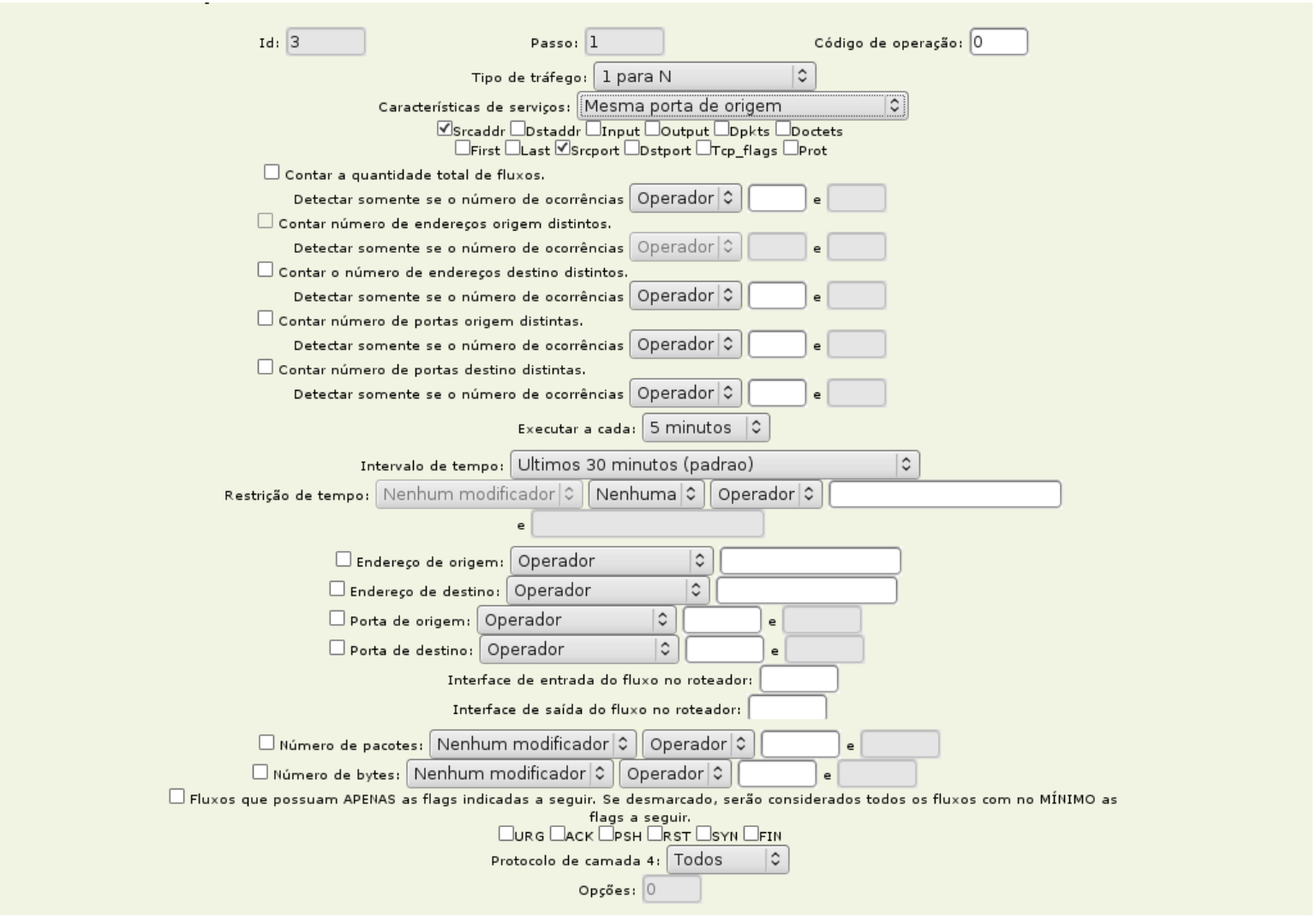
- **Características das assinaturas do rastreador de fluxos**
  - São *descrições de tráfego, no âmbito dos fluxos;*
  - São organizadas em passos:
    - Cada assinatura pode conter quantos passos forem necessários para a descrição do evento;
    - Cada passo possui um código de operação (operação a ser executada).
  - São de dois tipos:
    - Abuso (descrição de eventos com características detectáveis e similares em todas as instâncias);
    - Anomalia (descrição de comportamento por meio de limiares característicos de cada ambiente)

Assinaturas (2)

- **Campos comuns aos dois tipos de assinatura**
  - Id
  - Passo
  - Código de operação
  - Intervalo de tempo
  - Intervalo de execução
  - Características de tempo
  - Restrições de endereços
  - Restrições de portas
  - Interfaces do roteador;
  - Número de pacotes e número de bytes;
  - Flags;
  - Protocolo (carregado pelo IP);
  - Opções.

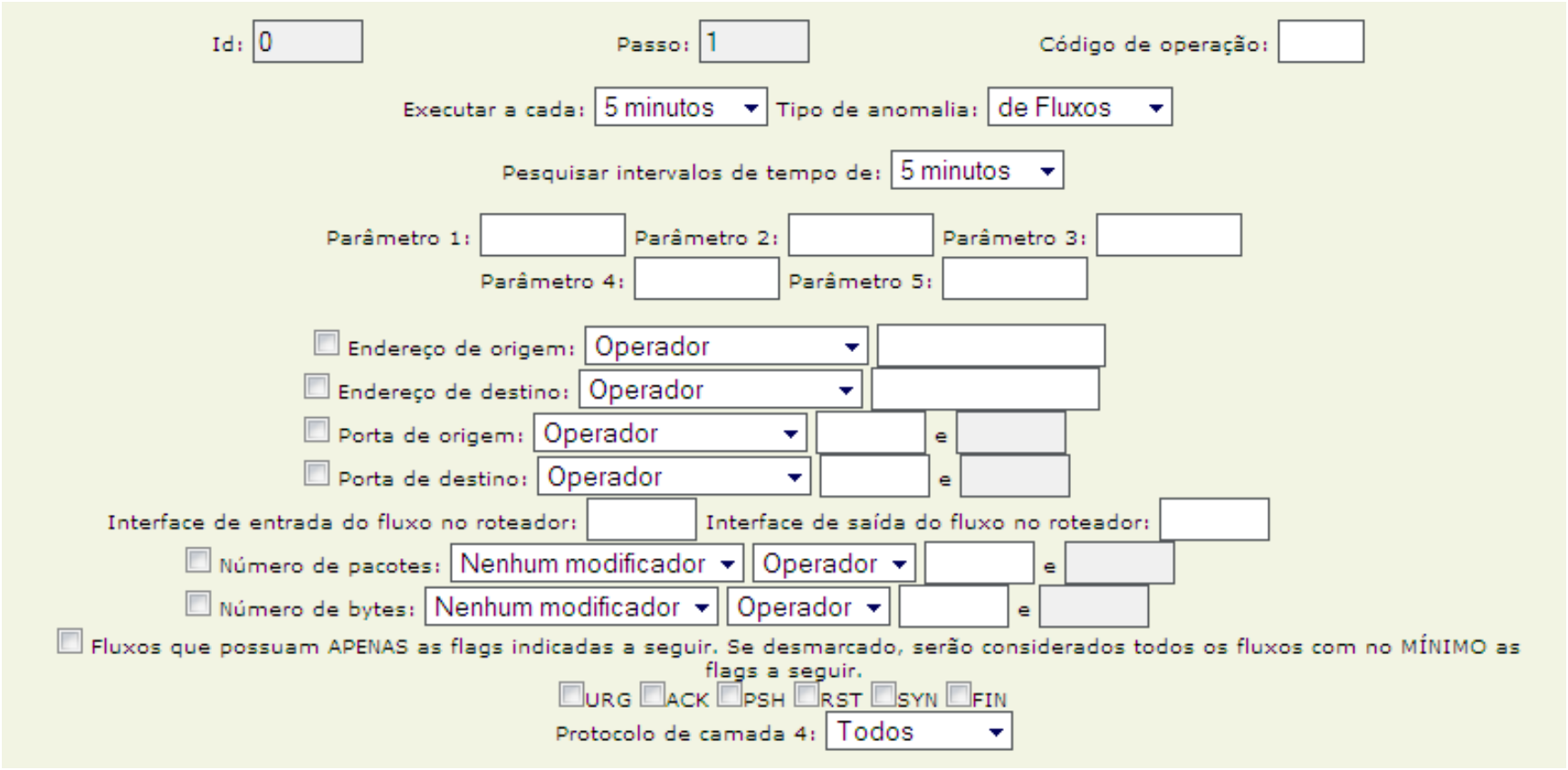
Assinaturas (3)

Assinatura de abuso



Assinaturas (4)

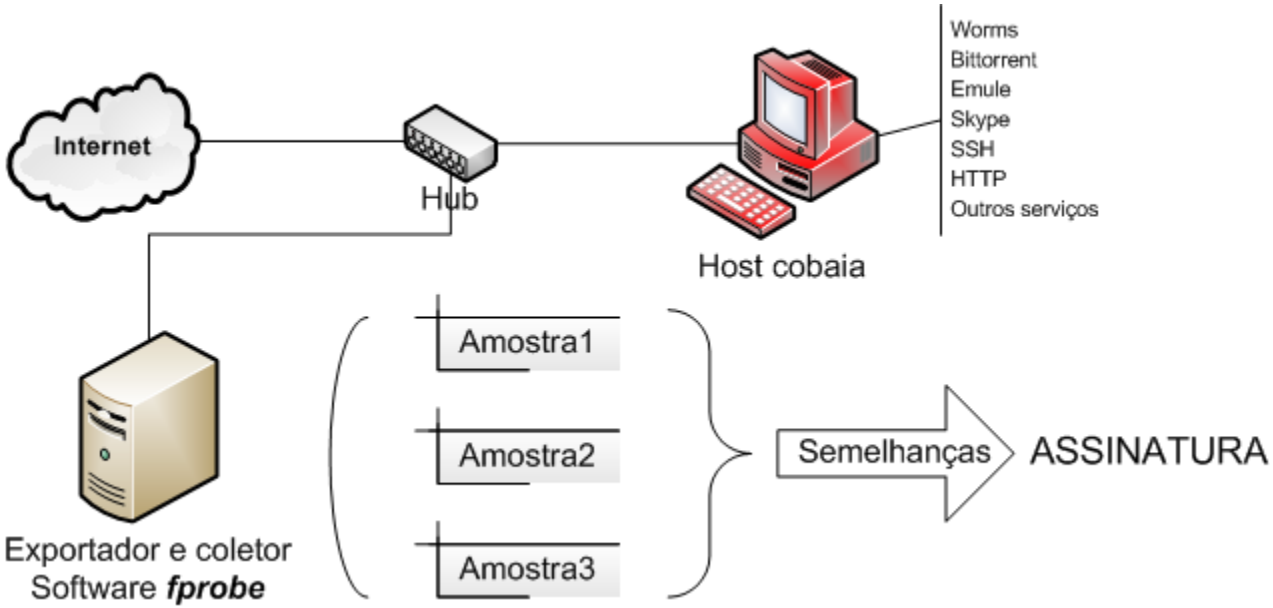
Assinatura de anomalia



Assinaturas (5)

- **Geração de assinaturas**
  - Atualmente é um processo manual;
  - Consiste em analisar isoladamente os fluxos gerados pelo evento que se deseja detectar;
  - Três coletas são realizadas para cada evento;
  - Analisa-se estas coletas em busca de padrões que se repetem em todas elas;
  - Para artefatos, o sistema é reinstalado a cada execução;
  - Para a geração dos fluxos é utilizado o software ***fprobe***.

Assinaturas (6)



ACME! Computer Security Research

Agenda

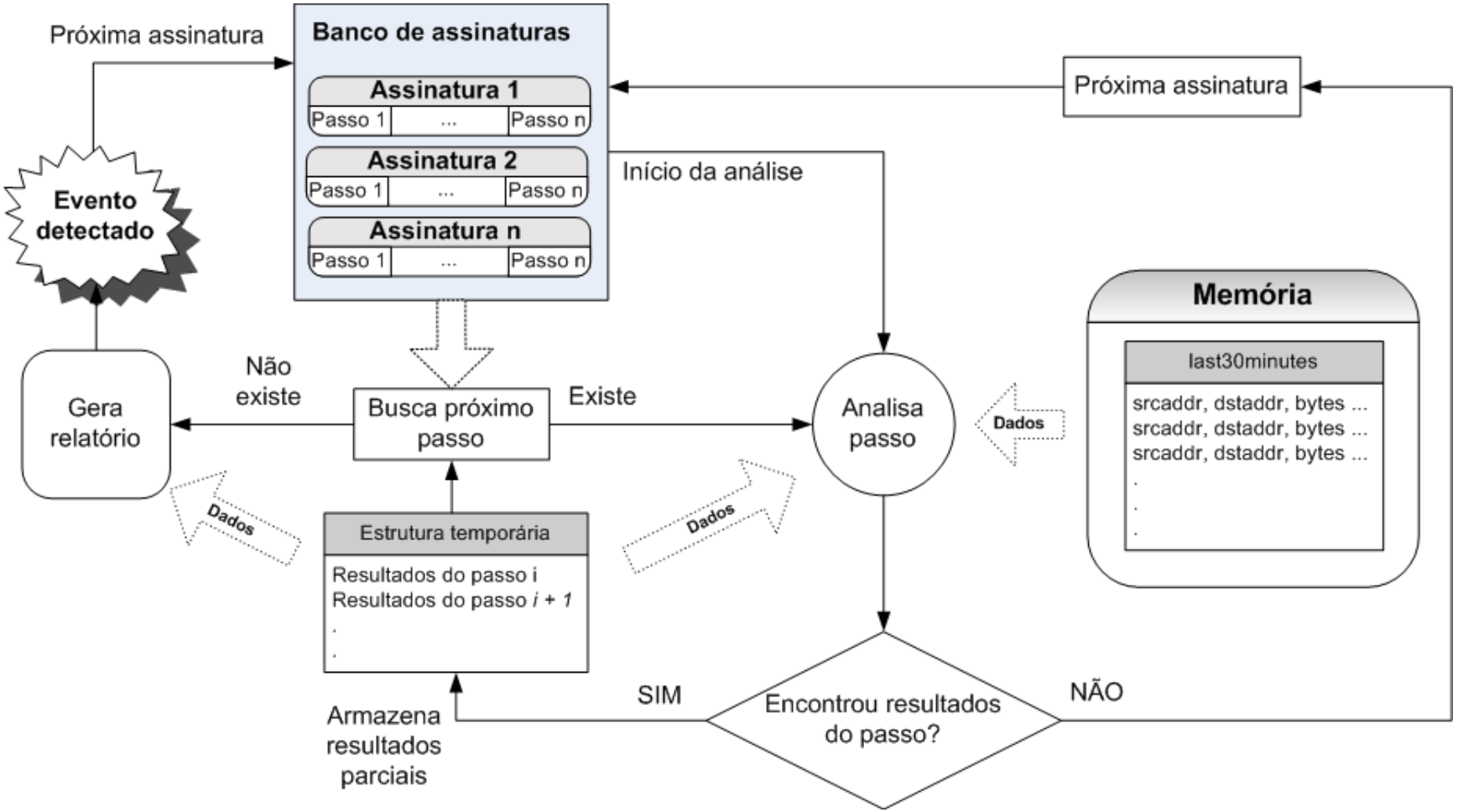
- Motivação e objetivos.
- Fluxos e exportação.
- Coleta: arquitetura de armazenamento.
- Assinaturas.
- **Modelo de rastreamento de fluxos.**
- Resultados.

Modelo de rastreamento de fluxos

- **Como funciona**
  - Detecção de cada passo, de cada assinatura;
    - Todos os passos devem ser encontrados;
  - Detecção '*online*' utiliza os fluxos armazenados em memória;
  - Detecção '*offline*' utiliza fluxos armazenados em disco, sendo um processo mais lento;
  - Ao detectar todos os passos de um evento, este constará na página de relatórios.

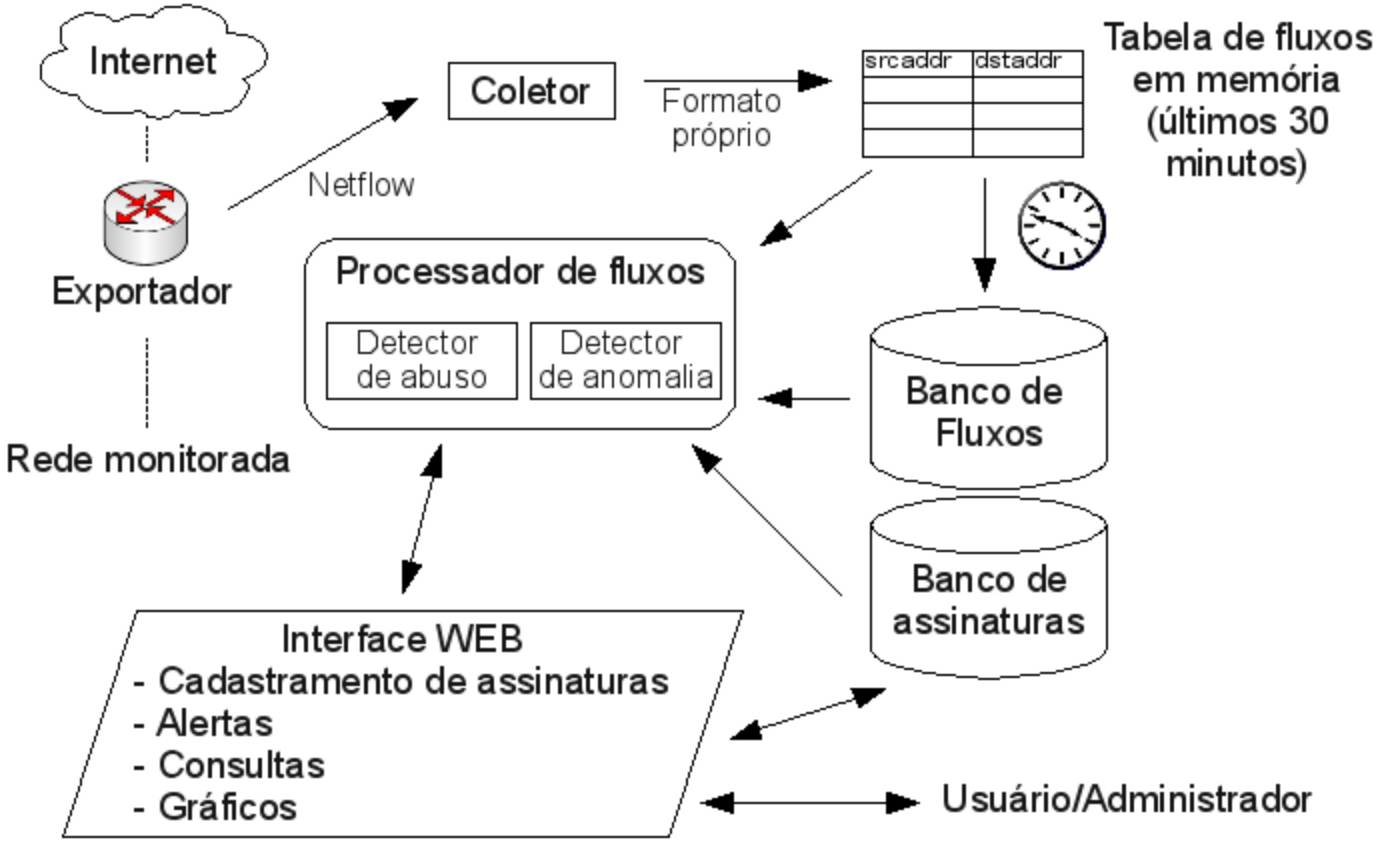
Modelo de rastreamento de fluxos (2)

Funcionamento do sistema – Processador de fluxos



Modelo de rastreamento de fluxos (3)

Visão geral do sistema



ACME! Computer Security Research

Agenda

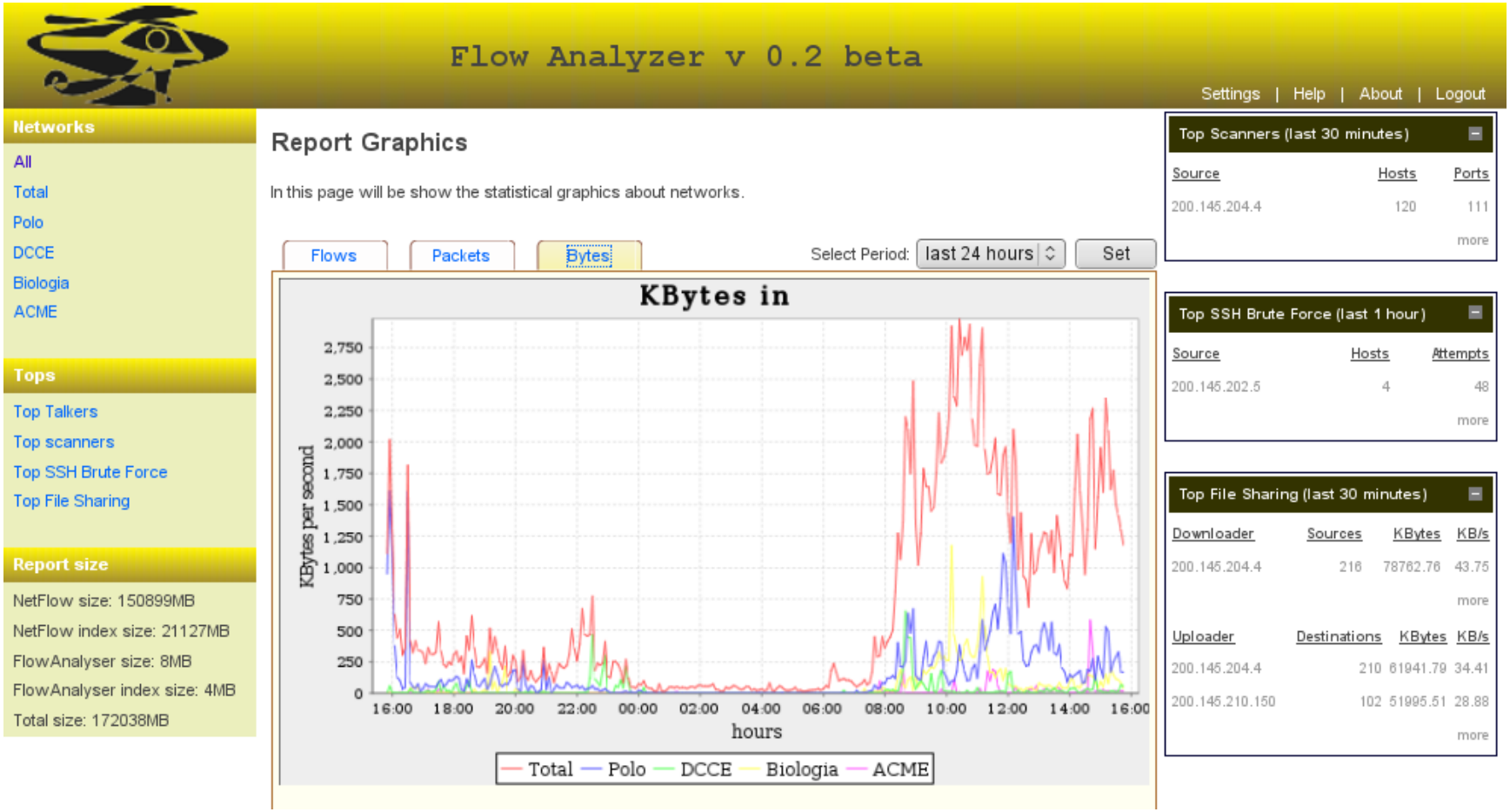
- Motivação e objetivos.
- Fluxos e exportação.
- Coleta: arquitetura de armazenamento.
- Assinaturas.
- Modelo de rastreamento de fluxos.
- **Resultados.**

Resultados

- **Disponíveis na versão atual**
  - Visualização gráfica de fluxos, pacotes e bytes;
  - Detecção de alguns eventos (*built-in*) com detalhamento:
    - Visualização dos fluxos que causaram o evento;
    - Consulta *whois* para hosts envolvidos.
  - Identificação dos hosts mais ativos na rede;
  - Possibilidade de visualização por rede;
    - Ainda sem suporte a VLSM (prioridade);
  - **Consulta dinâmica de fluxos.**

ACME! Computer Security Research

Resultados (2)



Resultados (3)

ACME! Computer Security Research

Networks
- All
- Total
- Polo
- DCCE
- Biologia
- ACME

Tops
- Top Talkers
- Top scanners
- Top SSH Brute Force
- Top File Sharing

Report size
- NetFlow size: 150907MB
- NetFlow index size: 21129MB
- FlowAnalyser size: 8MB
- FlowAnalyser index size: 4MB
- Total size: 172048MB

Top Talkers

Average samples of 5 minutes about 1 hour ago.

Flows | Packets | Bytes

Top 10 by Flows in

Host	flows/sec in	Pkts/sec in	Bytes/sec in
200.145.201.1 (11 samples)	12.84	19.45	2293.53
200.145.201.91 (11 samples)	10.33	214.17	245271.89
200.145.205.125 (11 samples)	7.60	20.11	16203.83
200.145.213.58 (4 samples)	4.70	36.00	40257.90
200.145.202.9 (5 samples)	3.64	30.92	31927.10
200.145.210.150 (11 samples)	3.63	84.32	73851.82
200.145.208.82 (7 samples)	3.04	8.97	5380.55
200.145.204.4 (10 samples)	2.57	91.32	71266.83
200.145.203.42 (11 samples)	2.17	52.13	39560.94
200.145.203.200 (8 samples)	2.16	30.55	10684.61

Top 10 by Flows out

Host	flows/sec out	Pkts/sec out	Bytes/sec out
200.145.205.125 (4 samples)	21.12	37.71	4917.60
200.145.201.1 (11 samples)	13.07	21.73	11575.53
200.145.201.91 (11 samples)	9.98	157.70	26344.72
200.145.213.58 (4 samples)	4.68	27.38	2750.04
200.145.210.150 (11 samples)	4.44	80.92	61197.23

Top Scanners (last 30 minutes)

Source	Hosts	Ports
62.217.53.210	562	1
200.145.204.4	132	120

more

Top SSH Brute Force (last 1 hour)

Source	Hosts	Attempts
200.145.202.5	4	48

more

Top File Sharing (last 30 minutes)

Downloader	Sources	KBytes	KB/s
200.145.204.4	236	76738.24	42.63

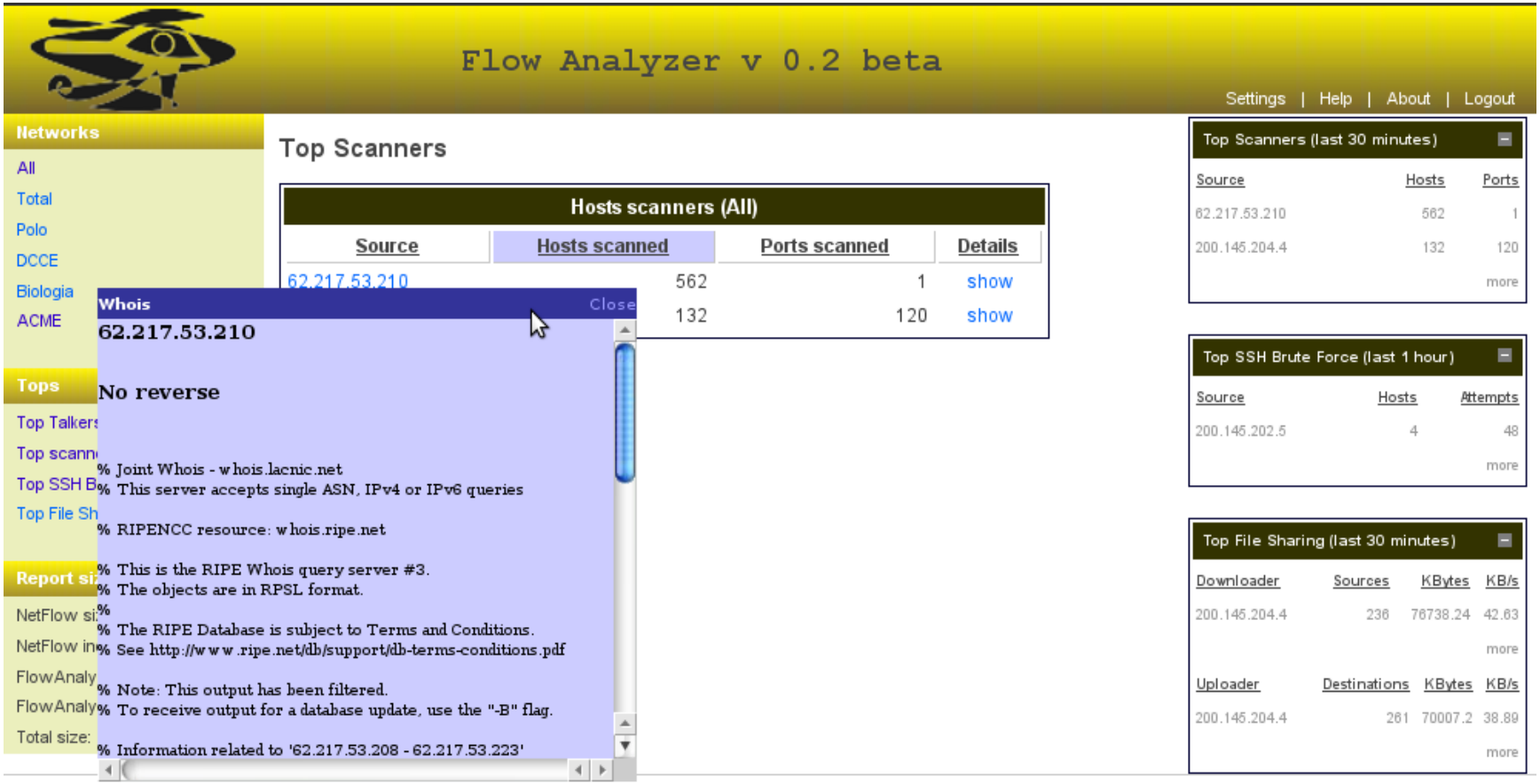
more

Uploader	Destinations	KBytes	KB/s
200.145.204.4	261	70007.2	38.89

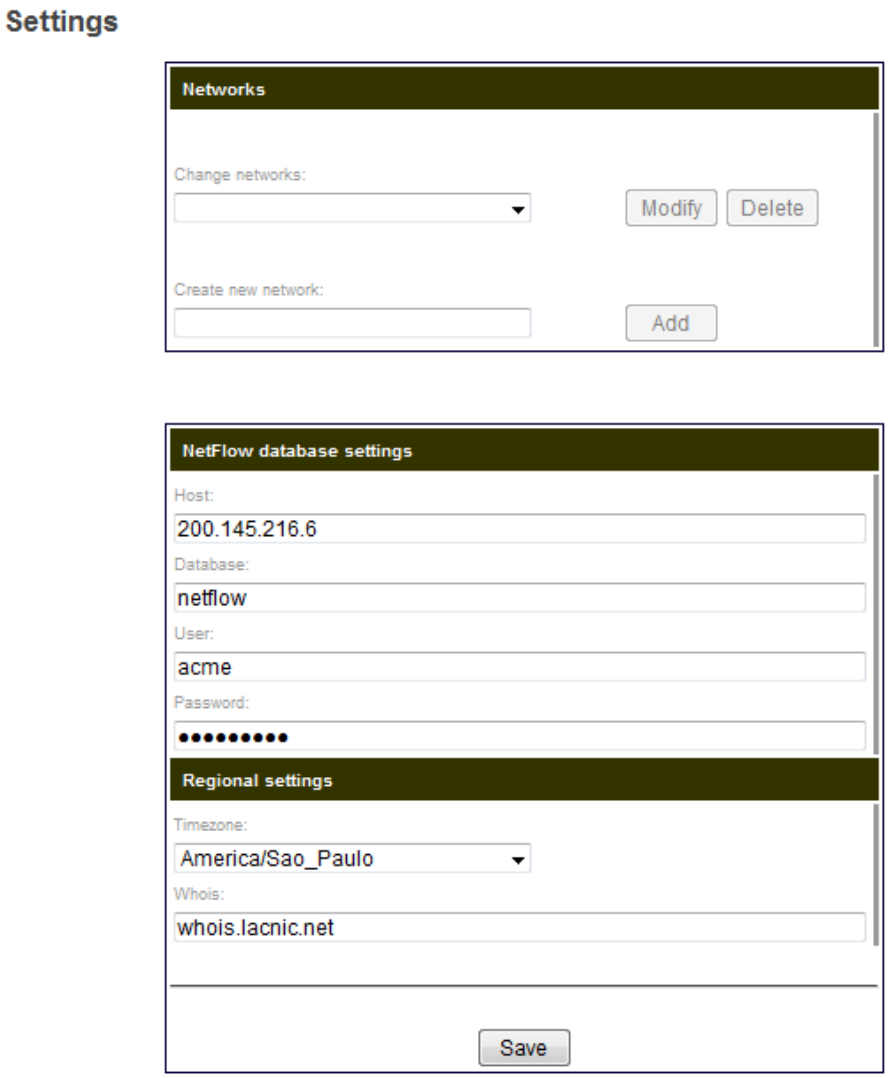
more

ACME!
Computer Security Research

Resultados (4)

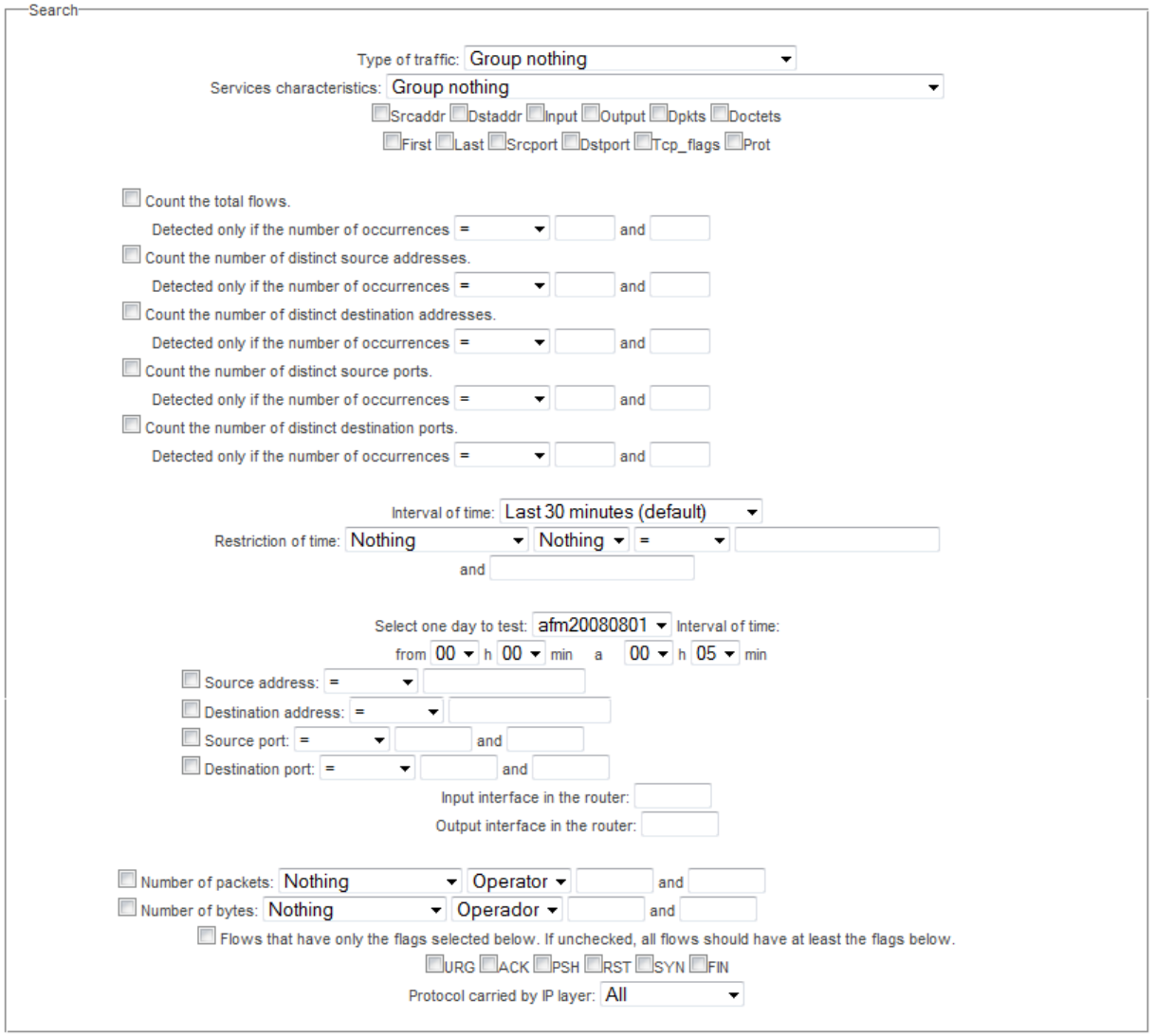


Resultados (5)



ACME! Computer Security Research

Resultados (6)



Resultados (7)

- **Próxima versão - eventos detectados com êxito**
  - Bittorrent;
  - P2P (*file-sharing* normal e filtrado por firewall);
  - Ataque de dicionário no SSH (sem restrição de porta);
  - Scans em um único host em busca de serviços;
  - Scans em uma rede em busca de hosts ativos;
  - Chamadas de voz Skype (quando há chamada);
  - Anomalia na quantidade de fluxos utilizando um mecanismo de médias acumuladas e mudança abrupta;
  - OBS.: qualquer evento que apresente características visíveis nos fluxos pode ser descrito, não apenas os ilícitos;
    - Ex.: para fazer *accounting*.

ACME! Computer Security Research

Resultados (8)

P2P

Id: 5
Descrição: Atividade de compartilhamento de arquivos com redes do tipo Kazaa, Emule, FastTrack, entre outras, também conhecidas como aplicações P2P
Como detectar (metodologia da assinatura): Uma aplicação P2P gera dois padrões de fluxos. O primeiro consiste do startup e mensagens de gerenciamento, todas UDP. O segundo são conexões TCP que representam a transferência de arquivos entre os hosts da rede distribuída. Primeiramente verifica-se se houve o padrão de startup e em seguida detecta-se as características da transferência de arquivos
Frequência: Comum (várias vezes ao dia).
Criada em: 2009-04-14 11:33:47
Última detecção em: 2009-05-31 07:25:00

Passo: 1 Código da operação: 0

Tipo de tráfego 1 para N.
Característica de serviço: Mesma porta de origem.
Campos selecionados: Srcaddr, Srcport.

Contar a quantidade de endereços destino distintos. Detectar apenas se a quantidade for >= 150.
Contar a quantidade de portas destino distintas. Detectar apenas se a quantidade for >= 150.
Executar a cada: 5 minutos.
Intevalo de tempo: Ultimos 5 minutos.
Restrição de tempo: last - first <= 6.
Srcaddr wildcard 200.145.%%%%%%%%.
Protocolo: UDP.

Passo: 2 Código da operação: 0

Tipo de tráfego 1 para N.
Característica de serviço: Mesma porta de origem.
Campos selecionados: Srcaddr, Srcport.

Contar a quantidade total de fluxos. Detectar apenas se a quantidade for >= 5.
Contar a quantidade de endereços destino distintos. Detectar apenas se a quantidade for >= 5.
Executar a cada: 5 minutos.
Intevalo de tempo: Ultimos 5 minutos.
Restrição de tempo: last - first >= 50.
Srcaddr = srcaddr do passo 1.
Srcport = srcport do passo 1.
Protocolo: TCP.

ACME! Computer Security Research

Resultados (9)

Scan em host

Id: 3
Descrição: Detecta uma varredura em um host, em busca de serviços abertos.
Como detectar (metodologia da assinatura): Procura por uma grande quantidade de fluxos para um único host, em várias portas diferentes, caracterizados pela flag SYN.
Frequência: Comum (várias vezes ao dia).
Criada em: 2009-05-12 10:57:17
Última detecção em: 2009-05-31 21:25:00

Passo: 1 **Código da operação:** 0

Tipo de tráfego: 1 para 1.
Nenhum agrupamento de portas.
Campos selecionados: Srcaddr, Dstaddr.

Contar a quantidade de portas destino distintas. Detectar apenas se a quantidade for >= 50.
Executar a cada: 5 minutos.
Intevalo de tempo: Ultimos 5 minutos.
Restrição de tempo: last - first = 0.
Dstaddr wildcard 200.145.%%%%%%%%.
Tcp_flags (fluxos que possuam APENAS as flags): SYN.
Protocolo: Todos.

ACME! Computer Security Research

Resultados (10)

Skype

Id: 4
Descrição: Detecção da aplicação Skype que tenha feito autenticação e tenha efetuado alguma chamada de voz
Como detectar (metodologia da assinatura): O primeiro passo consiste em detectar possíveis chamadas de voz em que a característica do tráfego é possuir portas altas e determinado padrão de bytes e pacotes. Para cada um destes possíveis hosts realizando uma chamada são procurados os fluxos correspondentes ao startup desta aplicação, em que ocorre uma repetição de portas origem e um padrão de bytes e pacotes
Frequência: Normal (poucas vezes ao dia).
Criada em: 2009-04-05 13:43:37
Última detecção em: 2009-05-29 21:30:00

Passo: 1 **Código da operação:** 0

Tipo de tráfego: 1 para 1.
Característica de serviço: Mesma porta de origem.
Campos selecionados: Srcaddr, Dstaddr, Srcport, Dstport.

Executar a cada: 5 minutos.
Intevalo de tempo: Ultimos 5 minutos.
Restrição de tempo: last - first >= 30.
Srcaddr wildcard 200.145.%%%%%%%%.
Srcport > 1023.
Dstport > 1023.
Bytes / Pacotes entre 130 e 320.
Protocolo: UDP.

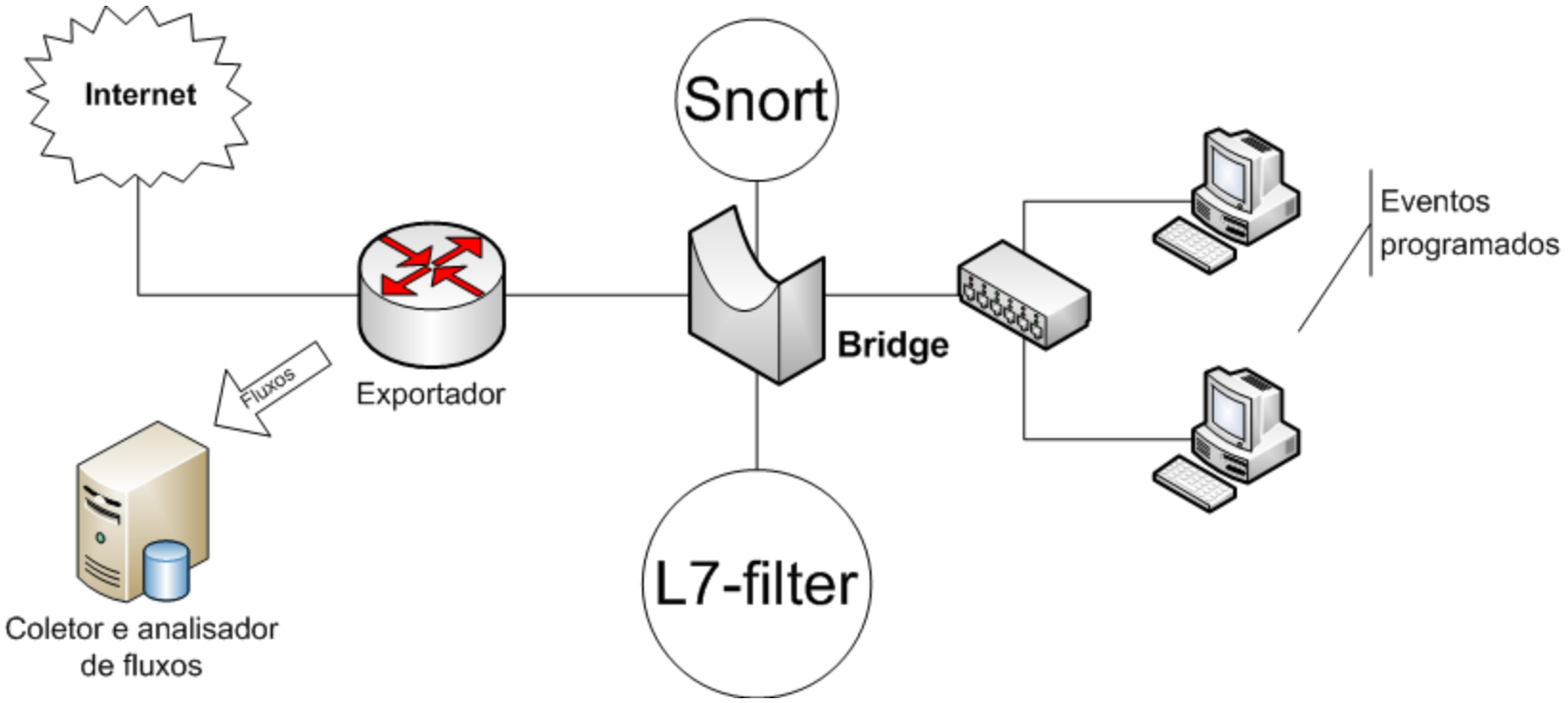
Passo: 2 **Código da operação:** 0

Tipo de tráfego 1 para N.
Característica de serviço: Mesma porta de origem.
Campos selecionados: Srcaddr, Srcport.

Contar a quantidade de endereços destino distintos. Detectar apenas se a quantidade estiver entre 50 e 500.
Contar a quantidade de portas destino distintas. Detectar apenas se a quantidade estiver entre 50 e 500.
Executar a cada: 5 minutos.
Intevalo de tempo: Ultimos 30 minutos (padrao).
Restrição de tempo: last - first <= 60.
Srcaddr = srcaddr do passo 1.
Srcport = srcport do passo 1.
Protocolo: UDP.

Resultados (11)

- Para coleta dos resultados quantitativos, foi utilizado o seguinte ambiente:



Resultados (12)

Comparação entre as taxas de detecção para os eventos P2P e Bittorrent

	Snort		L7-filter		Achow	
	P2P	Torrent	P2P	Torrent	P2P	Torrent
Taxa de acertos	-	0,98	0,91	0,98	0,90	0,66
Falso-positivos	-	0,17	0,38	0,88	0,00	0,06
Falso-negativos	-	0,02	0,09	0,10	0,10	0,34

Os dados analisados incluem períodos de inatividade de download. O cliente era ligado (suficiente para o Snort e o L7-Filter) mas nenhum arquivo era transferido.

OBS.: Snort e L7-filter analisando o tráfego apenas da bridge.
ACHoW procurando os eventos em meio aos fluxos de todo o campus.

ACME! Computer Security Research

Site e contatos

- **Site:**
  - www.acmesecurity.org/fluxos
    - Coletor
    - Sistema de monitoramento

- **Endereços para contato (dúvidas, sugestões, parcerias, etc):**
  - fluxos@acmesecurity.org
  - jorge@acmesecurity.org
  - andreproto@acmesecurity.org

- **Obrigado!**

ACME! Computer Security Research

Bibliografia

- http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
- http://tools.ietf.org/html/rfc3917
- http://www.ietf.org/rfc/rfc3954.txt
- http://tools.ietf.org/html/rfc3176
- http://www.sflow.org/about/index.php
- http://www.plixer.com/blog/general/cisco-netflow-v5-vs-netflow-v9-which-most-satisfies-your-hunger-pangs/
- http://www.plixer.com/blog/general/netflow-vs-sflow-it-may-matter-to-you/
- http://www.cert.org/flocon/
- http://fprobe.sourceforge.net/