Utilizando o conjunto de ferramentas Flow-tools como mecanismo de Detecção de Intrusão

Almir Moreira Saúde
Arnaldo Candido Junior
Ronan Pedroso Nogueira Gaeti

Prof. Dr. Adriano Mauro Cansian
Coordenador

ACME! Computer Security Research Labs
UNESP - Universidade Estadual Paulista
Campus de São José do Rio Preto

Roteiro

- IPFIX e NetFlow
- Ferramentas
- Flow-tools
- ACME! Flow-Alert

Introdução

- Monitoramento clássico de tráfego:
  - MRTG
  - TCPDUMP
- Monitoramento por fluxo:
  - Uma forma mais interessante para caracterização de tráfego.
  - Detecta eventos interessantes na rede de forma mais eficiente.
- Definição para fluxo:
  - Um fluxo é uma seqüência unidirecional de pacotes com características comuns entre uma fonte e um destino.
- NeTraMet (RFC 2123): o próprio administrador define quais são estas características.
- NetFlow: define sete características.

IPFIX - IP Flow Information eXport

- RFC 3917 define alguns requisitos para o protocolo IPFIX. Deve atender a diferentes propósitos:
  - Contabilidade de uso
  - Caracterização de tráfego
  - Engenharia de tráfego
  - Detecção de Intrusão/Anomalias
  - Monitoramento de QoS
- RFC 3955 faz uma avaliação de cinco candidatos a protocolo IPFIX e recomenda que o NetFlow seja usado.

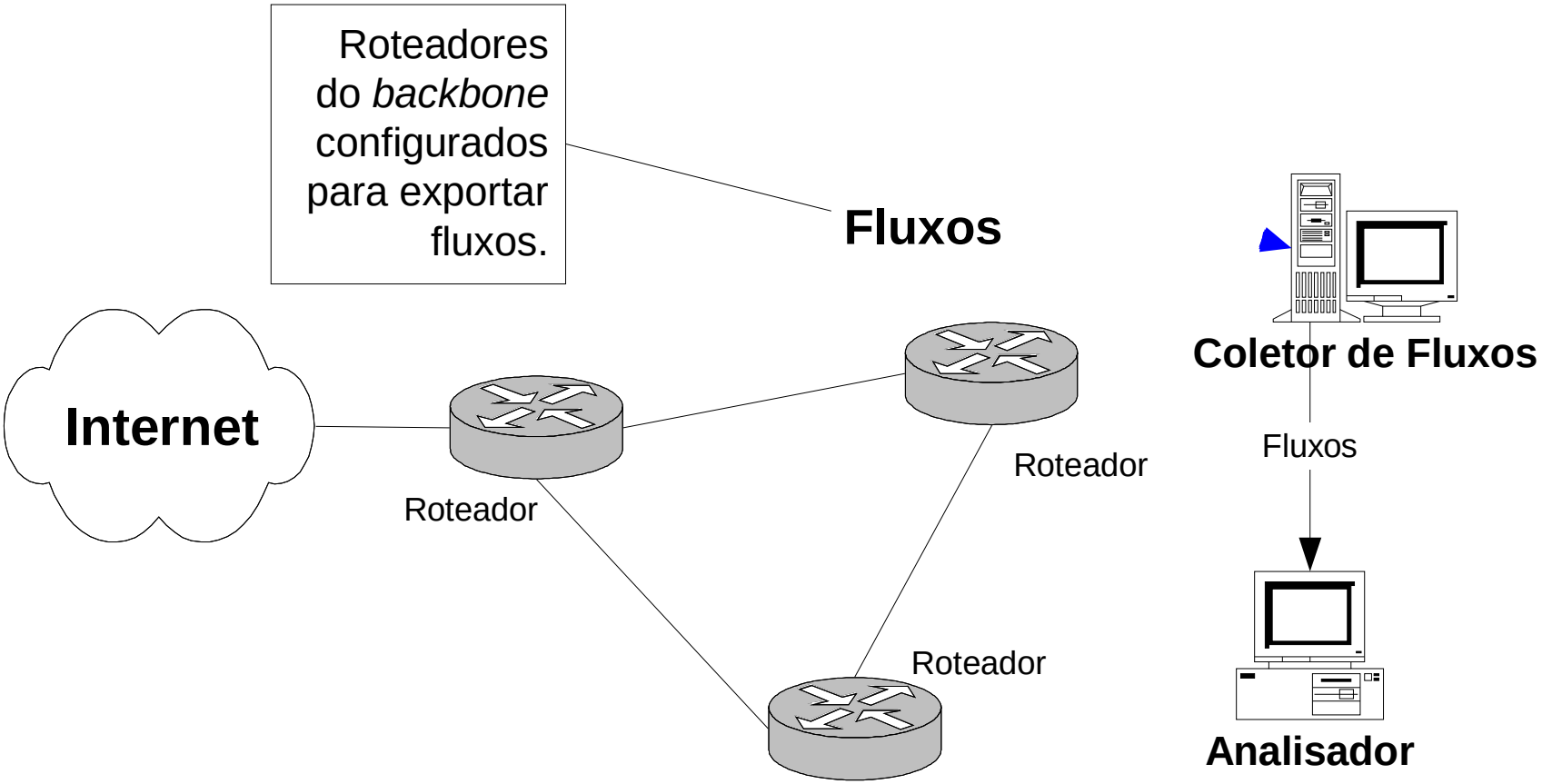
Detecção de Anomalias

- A análise a partir de fluxos NetFlow pode revelar a existência de:
  - Tentativas de intrusão realizadas por w*orms* (ex.: *Slammer*).
  - Varreduras de portas e de *hosts* em busca de serviços vulneráveis.
  - Ataques Distribuídos de Negativa de Serviço.
  - Violações de políticas de uso (ex.: P2P).
- *Worms* e varreduras totalizam 81% dos incidentes de segurança relatados ao Cert.br no primeiro trimestre de 2005.

NetFlow

- Padrão *de facto* para o gerenciamento de fluxos de redes.
- Proposto pela Cisco em 1996.
- Versão 9 documentada no RFC 3954.
- Define um fluxo por uma tupla:
  - IP de origem
  - IP de destino
  - Porta de origem
  - Porta de destino
  - Tipo de protocolo (do cabeçalho IP)
  - Bits de TOS
  - Interface de entrada

Topologia



Fluxos NetFlow

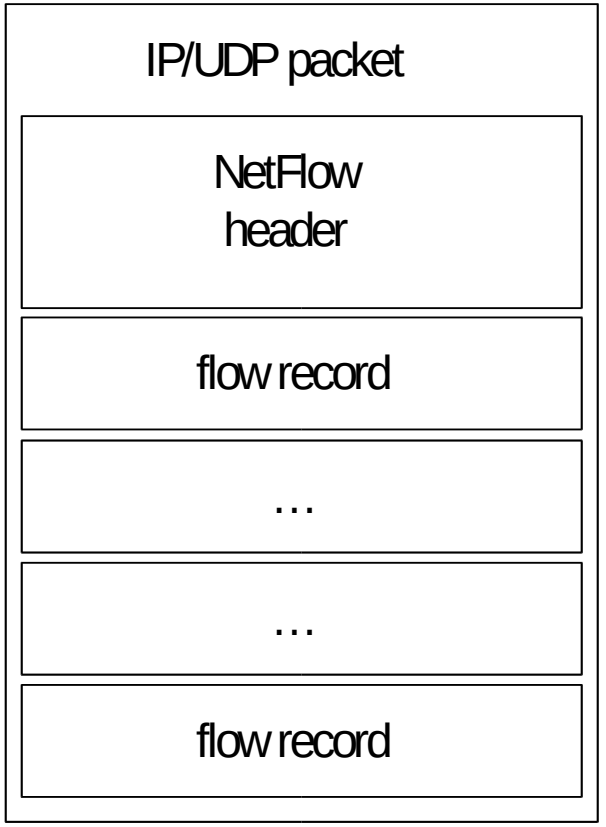
- Um novo fluxo é criado quando é recebido um pacote que não pertence a nenhum outro fluxo existente.
- Um fluxo expira quando:
  - Permanece inativo por mais de 15 segundos.
  - Sua duração excede 30 minutos.
  - Uma conexão TCP é encerrada por um FIN ou RST.
  - Tabela de fluxos está cheia ou usuário redefine configurações de fluxo.
- Amostragem:
  - Os pacotes usados na geração de novos fluxos podem ser amostrados como medida para diminuir o*verhead*.
- Agregação:
  - Fluxos podem ser agregados gerando um único fluxo. Isto é útil para diminuir o uso de banda.
  - Com agregação: v8.x, v9; sem agregação: v1, v5, v6, v7, v9.

Versões

- V1 – não possui números de seqüência (não detecta perda de fluxos).
- V5 – versão mais difundida atualmente. Cada pacote contém um cabeçalho e cerca de 30 registros de fluxo.
- V7 – traz alguns melhoramentos para *switchs* Cisco Catalist.
- V8.x – versões específicas para agregação.
- V9 – Utiliza *templates* para definir o formato de um registro de fluxos.
  - Versão definida no RFC 3954.
  - Os *templates* possibilitam a inserção de novos campos sem mudanças nos *softwares* já existentes.
- Versões 2, 3, 4 e 6 nunca foram oficialmente lançadas.

NetFlow - Formato típico de pacote

- Formato de pacote para as versões 1, 5, 7, 8.
- A versão 5 tem em média 30 registros de fluxo por pacote.
- Versão 9 pode conter registros com informações sobre o *template* e registros opcionais com informações extras.



Configuração Cisco IOS

- Configurando o *router*:

```
Router# configure terminal
Router(config)# ip flow-export destination a.b.c.d 7000
Router(config)# ip flow-export version 5 peer-as
Router(config)# ip flow-export source Ethernet 0/1
```

- Configurando as interfaces:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip route-cache flow
```

- Obtendo estatísticas:

```
Router(config)#show ip flow export
```

Configuração Cisco Catalist

- CatIOS:

```
Console> (enable) set mls flow full
Console> (enable) set mls nde version 7
Console> (enable) set mls nde a.b.c.d 7000
Console> (enable) set mls agingtime 32
```

- Native IOS:

```
Router(config)# mls flow ip destination-source
Router(config)# mls nde flow include
Router(config)# mls nde src_address a.b.c.d version 7
Router(config)# ip flow-export source Loopback0
Router(config)# ip flow-export version 5 peer-as
Router(config)# ip flow-export destination c.d.e.f 5555
```

Configuração Juniper (1)

- Configuração:

```
forwarding-options {
    sampling {
        input {
            family inet {
                rate 100;
            }
        }
        output {
            cflowd a.b.c.d {
                port 7000;
                version 5;
            }
        }
    }
```

- Obtendo amostragem de pacotes através do *firewall*:

```
firewall {
    filter all {
        term all {
            then {
                sample;
                accept;
            }
        }
    }
}
```

Configuração Juniper (2)

- Aplicando o filtro de *firewall* nas interfaces:

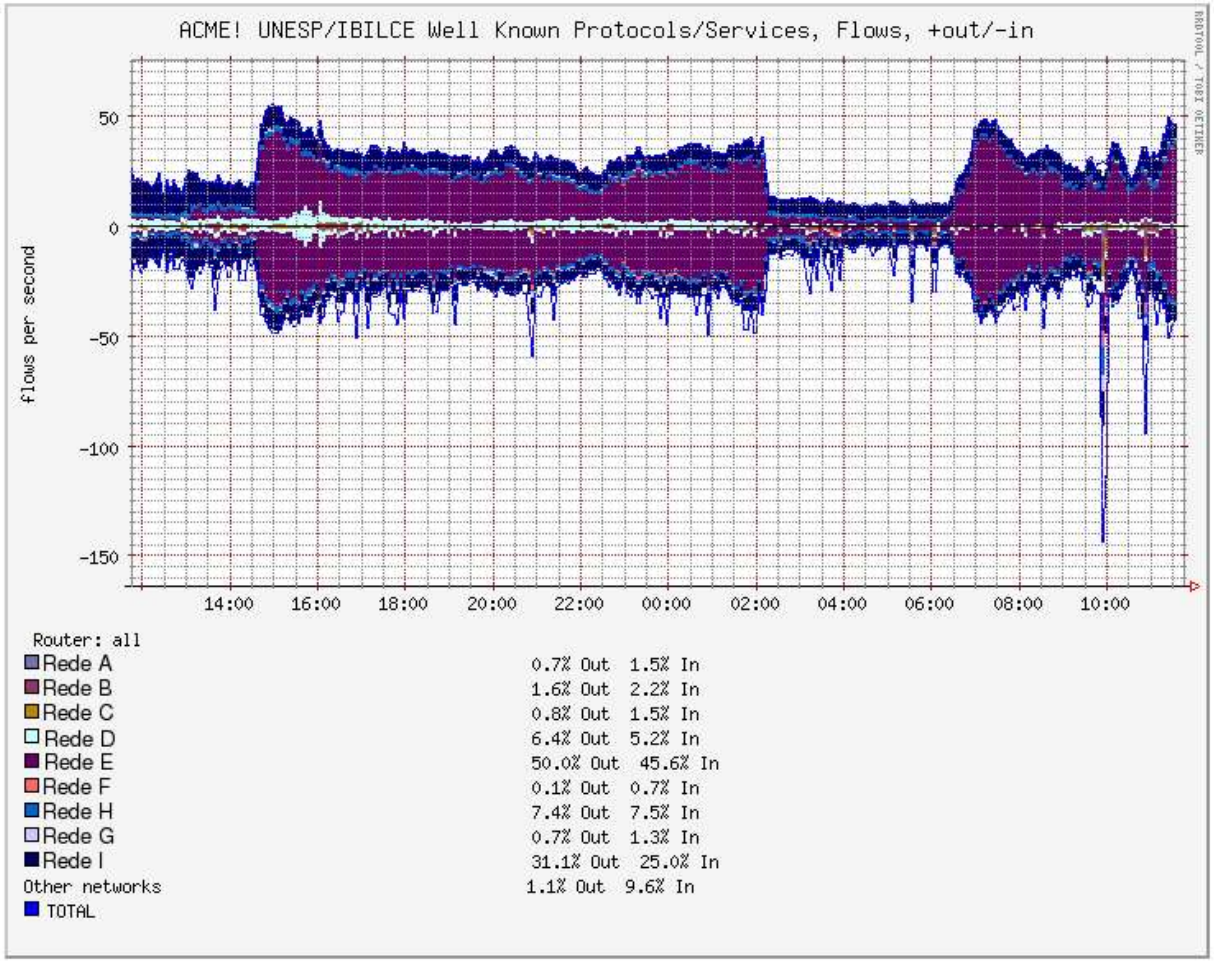
```
interfaces {
    ge-0/3/0 {
        unit 0 {
            family inet {
              filter {
                    input all;
                    output all;
                }
                address 192.148.244.1/24;
            }
        }
   }
```

Ferramentas

- *Flow-tools*: conjuntos de ferramentas para coleta e análise de fluxos.
  - http://www.splintered.net/sw/flow-tools/
- *FlowScan*: análise gráfica de fluxos NetFlow.
  - http://dave.plonka.us/FlowScan/
- *Cflowd*: semelhante ao Flow-tools, porém em desuso atualmente.
  - http://www.caida.org/tools/measurement/cflowd/
- *Ntop*: gerenciamento do tráfego de através de gráficos e relatórios. Pode utilizar os fluxos NetFlow.
  - http://www.ntop.org/
- *Nprobe*: permite que seja utilizado um servidor dedicado para exportar fluxos, deixando os roteadores menos sobrecarregados.
  - http://www.ntop.org/nFlow/
- *Argus*: ferramenta para exportar, coletar e analisar de fluxos.
  - http://www.qosient.com/argus/

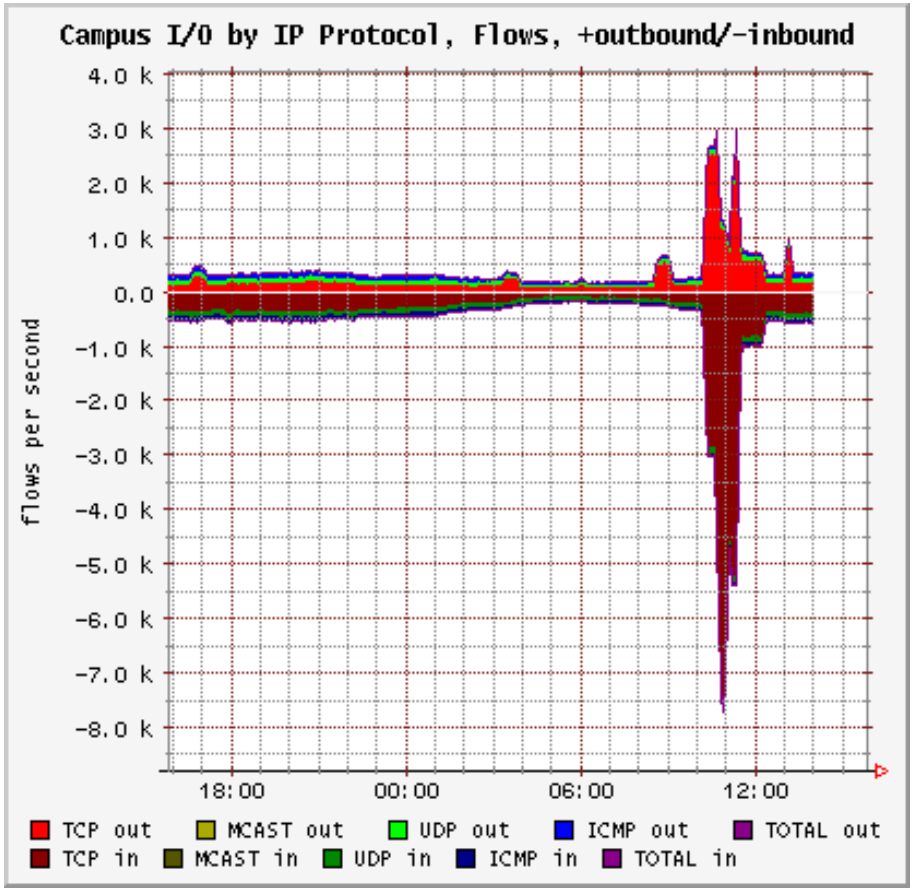
FlowScan (1)

- Exemplo de prospecção:



FlowScan (2)

- Exemplo de negativa de serviço (DDoS):



Flow-tools

- Conjunto de ferramentas utilizado para coletar, processar e gerar informações sobre dados do NetFlow.
- Algumas ferramentas:
  - *Flow-capture*: recebe, armazena e rotaciona arquivos de fluxos.
  - *Flow-cat*: concatena arquivos NetFlow. Utilizado para repassar informações para as outras ferramentas.
  - *Flow-print*: visualiza informações contidas em arquivos NetFlow.
  - *Flow-stat*, *flow-report*: geram relatórios e estatísticas sobre a rede.
  - *Flow-dscan*: dispara alertas para fluxos com muitos octetos e procura por varreduras de *hosts* e serviços.
  - *Flow-filter*, *flow-nfilter*: fornecem opções avançadas de filtragens.

Instalação e Configuração

- Instalação:

```
# ./configure
# make
# make install
```

- Iniciando flow-capture:
  - Receber fluxos do roteador 10.0.0.1 na porta 7200.
  - Utilizando o formato V5 com 50 GB armazenamento máximo de disco.

```
# flow-capture -w <flow_dir> 0/10.0.0.1/7200 -V5 -E50G -N 0
```

Alguns Exemplos (1)

- Visualizar todos os fluxos exportados do de primeiro de junho entre das 17:00 até as 18:00 do dia (supondo que os fluxos estejam no formato V5):

```
$ flow-cat ft-v05.2005-06-01.17* | flow-print
srcIP            dstIP            prot  srcPort  dstPort  octets      packets
a.a.a.a          b.b.b.b          6     3261     21       144         3
c.c.c.c          d.d.d.d          17    6346     6346     235         5
d.d.d.d          e.e.e.e          6     135      1076     120         3
f.f.f.f          g.g.g.g          6     80       2603     6088        7
h.h.h.h          i.i.i.i          6     80       3047     40          1
j.j.j.j          k.k.k.k          6     3046     80       80          2
l.l.l.l          m.m.m.m          6     1233     80       1424        13
...
```

Alguns Exemplos (2)

– Obter estatísticas gerais sobre o uso da rede:

```
$ flow-cat <flow_files> | flow-stat -f 0
Total Flows                      : 247530
Total Octets                     : 1963293045
Total Packets                    : 3642639
Total Time (1/1000 secs) (flows): 1319883688
Duration of data  (realtime)     : 3600
Duration of data (1/1000 secs)   : 3659416
Average flow time (1/1000 secs) : 5332.0000
Average packet size (octets)     : 538.0000
Average flow size (octets)       : 7931.0000
Average packets per flow         : 14.0000
Average flows / second (flow)    : 67.6496
Average flows / second (real)    : 68.7583
Average Kbits / second (flow)    : 4292.5238
Average Kbits / second (real)    : 4362.8735
...
```

Alguns Exemplos (3)

- Obter os *hosts Top-talkers*:

```
$ flow-cat <flow_files> | flow-stat -f11 -S3
# IPaddr          flows                   octets                  packets
#
a.a.a.a           54230                   406727082               769252
b.b.b.b           10204                   535210442               760396
c.c.c.c           17316                   128301234               229786
d.d.d.d           19041                   110948250               199408
...
```

- Informações sobre varreduras:

```
$ flow-cat <flow_files> | flow-dscan -b -l -s dscan.statefile -p -W -w
flow-dscan: host scan: ip=a.a.a.a ts=1100288268 start=1112.17:37:48.80
flow-dscan: host scan: ip=b.b.b.b ts=1100288511 start=1112.17:41:51.4
flow-dscan: host scan: ip=c.c.c.c ts=1100288595 start=1112.17:43:15.411
flow-dscan: port scan: src=d.d.d.d dst=80.117.91.22 ts=1100288718 start=
1112.17:45:18.125
flow-dscan: host scan: ip=e.e.e.e ts=1100288964 start=1112.17:49:24.90
...
```

ACME! Flow Alert

- *Script* Perl que utiliza o Flow-tools como *backend* para identificar eventos interessantes na rede.
  - Definição dos parâmetros aceitáveis da rede é feita através de um arquivo de configuração (*flow-alert.conf*).
  - Este arquivo também define quais testes serão realizados e outras informações gerais.
- Gera alertas e relatórios estatísticos.
  - Relatórios: informações gerais sobre o funcionamento da rede (ex.: varreduras de portas e *hosts*). *E-mail* diário enviado ao administrador.
  - Alertas: informações sobre potenciais problemas na rede (ex.: número de fluxos muito acima do normal). *E-mail* enviado ao administrador no momento em que o problema é detectado.

Eventos Detectáveis

- Através de análises de octetos:
  - Ataques de negativa de serviço.
  - Violações na política de tráfego.
- Através de análise de fluxos:
  - Ataques de negativa de serviço.
  - Tentativas de intrusão provenientes de w*orms*.
  - Varreduras em busca de serviços vulneráveis.

Relatório Estatístico

- Prospecções de *hosts* e portas geradas através do *flow-dscan*.
  - Os IPs dos servidores mais acessados devem ser armazenados nos arquivos *dscan.suppress.dst* e *dscan.suppress.src* para evitar falsos positivos.
- Tráfego de IPs suspeitos:
  - IPs não roteáveis (10.0.0.0/8, 127.0.0.0/8).
  - IPs de *multicast* (224-254.0.0.0/8).
  - IP *Spoofing* e ataques *Smurf*.
- *Top-talkers*.
  - Por fluxos.
  - Por octetos.
- Serviços mais populares (*top-services*).

Exemplo de Relatório

```
Report date: 2005-06-25

Port scans: 1
Host scans: 162

Top 10 destination ports by flow:
port        flows
a           410346
b           245921
c           223171
...

Top 10 Hosts by flow:
IP              flows
a.a.a.a         494981
b.b.b.b         347351
c.c.c.c         259700
...
```

```
Top 10 Hosts by octets:
IP              Octets
d.d.d.d         1126337522
e.e.e.e         1096880263
f.f.f.f         842165643


Uncommon IPs:
10.0.0.0/8: 1453
127.0.0.0/8: 0
172.16.0.0/12: 1470
192.168.0.0/16: 160
Multicast IPs: 39716

Report start: 01:00
Report finish: 01:01
```

Alertas

- Alertas por fluxos
  - Disparado quando o total de fluxos gerados excede o limite pré-definido.
  - Alerta para o administrador informando os *hosts* e serviços que estão consumindo mais fluxos.
- Alertas por octetos
  - Funciona de forma semelhante ao alerta por fluxos, informando ao administrador taxas muito elevadas de octetos por segundo e detalhando os serviços e *hosts* envolvidos.

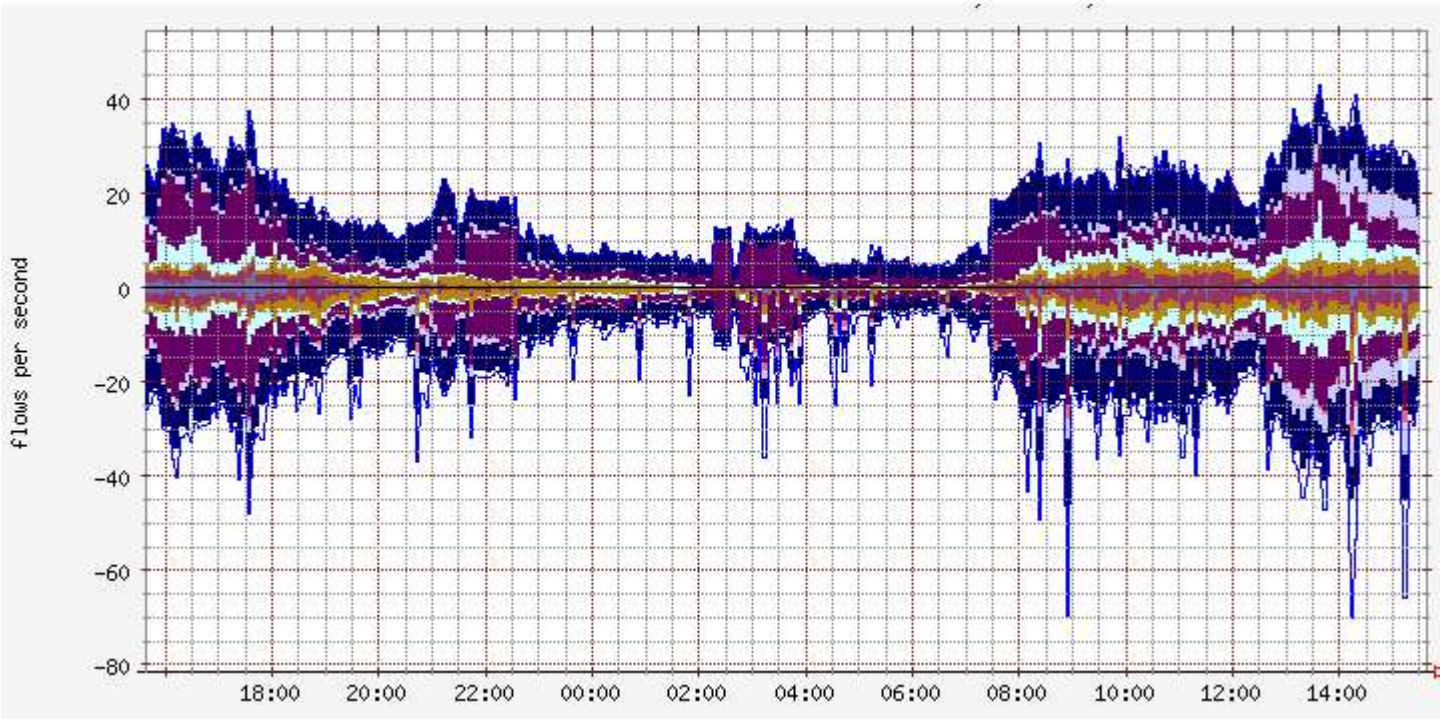
Exemplos de Alerta

```
Total flows / second:  89.2000

Top 10 Hosts by flow:
IP                flows
a.a.a.a           5581
b.b.b.b           3419
c.c.c.c           2487
...

Top 10 destination ports by flow:
port         flows
a            3688
b            2538
c            2170
...

In order to avoid false alarms keep
   flow_limit_alert high enough
```

```
Total kbits / second:  3450.2566

Top 10 Hosts by octets:
IP                Octets
d.d.d.d           27829564
e.e.e.e           23275696
f.f.f.f           9728153
...

Top 10 destination ports by octets:
port         octets
d            6334912
d            5167528
d            4959120
...

In order to avoid false alarms keep
   kbits_limit_alert high enough
```

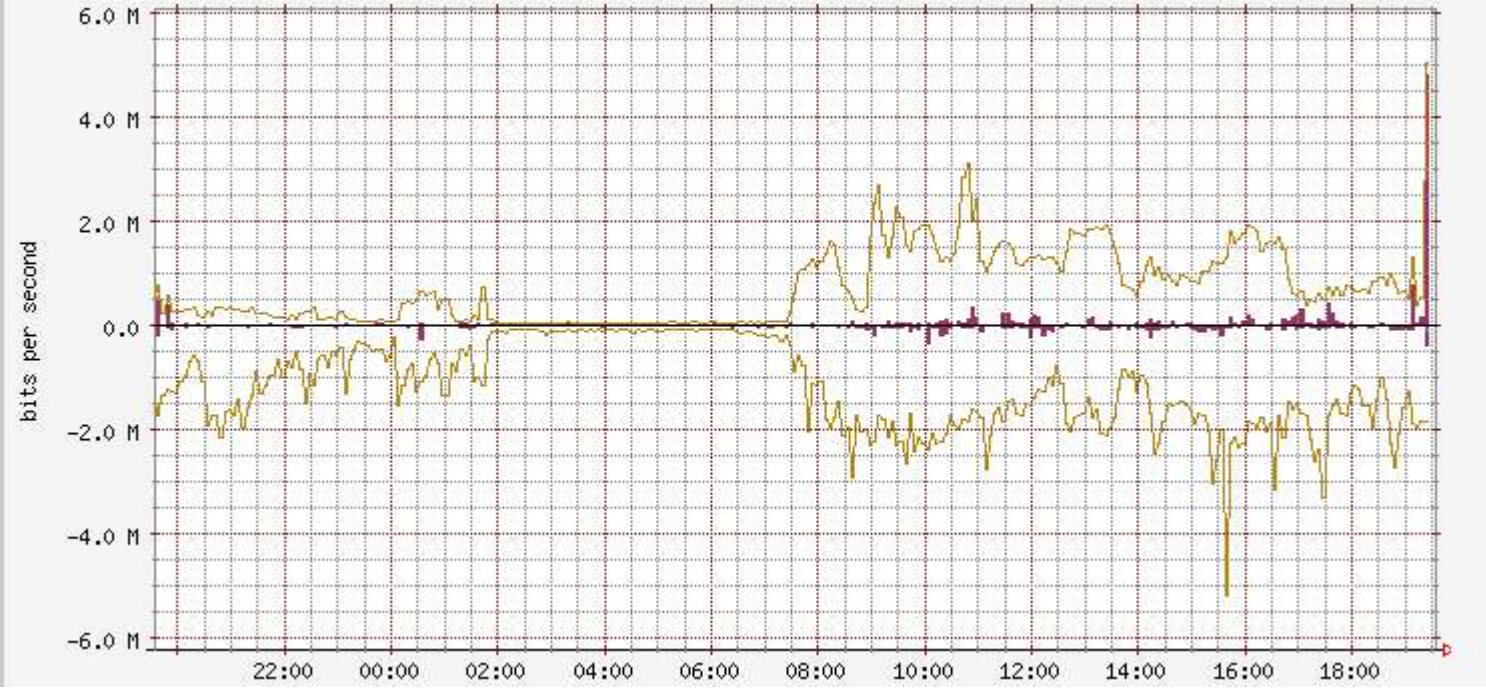
Prospecção Detectada

- Prospecções detectadas de máquinas infectadas pelo *worm Slammer* às 9:00, 14:00 e 15:00 horas.
- Gráfico correspondente:



Falso-Positivo

- Alto tráfego de octetos na porta 25. Aparentemente tráfego de *spam*.
- Gráfico correspondente:



- Posterior análise mostrou tratar-se de um usuário que envia correntes.

Instalação

- Requisitos mínimos de *hardware* considerando 1 GB de dados por dia:
  - Pentium IV 1.8 ou equivalente.
  - 512 megas de RAM.
- *Download*
  - www.acmesecurity.org/flow-alert
- Instalação
  - ./install.sh
  - Instalar biblioteca Perl NetAddr::IP
- Configuração
  - Revisar configurações em */etc/flow-alert/flow-alert.conf*.
  - *E-mail* do administrador.
  - Limites para fluxos e octetos (sugestão: usar o dobro da média da rede).
  - Análises que deverão ser habilitadas.

Observações

- É possível que algumas análises possam não ser efetuadas em configurações muito específicas ou diferentes do ambiente de desenvolvimento.
  - Roteador Cisco 7200.
  - *Exports* no formato V5.
  - Slackware GNU/Linux e Debian GNU/Linux.
- É recomendado que o *script* seja executado sem permissões de administrador.
- O tempo de criação dos fluxos deve ser um múltiplo de 5 minutos.
- *Bugs* encontrados podem ser encaminhados aos autores.

Conclusões

- A análise de fluxos é uma forma importante para detecção de algumas formas de anomalias na rede e de tentativas de intrusão.
- Dentre as opções disponíveis, o conjunto Flow-tools se mostrou uma ferramenta poderosa e flexível para a análise de fluxos.
- O s*cript* apresentado pode ser utilizado como ferramenta de apoio para detecção de anomalias. É possível obter informações sobre um ataque pouco tempo após seu início.
- O *script* fornece informações mais detalhadas sobre eventos anômalos, quando detectados, do que uma análise superficial do gráfico do FlowScan.

Referências

- Cert-br:
  - http://www.nbso.nic.br/stats/incidentes/2005-jan-mar/tipos-ataque.html
- Cisco NetFlow:
  - http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml
- FlowScan:
  - http://dave.plonka.us/FlowScan/
- Flow-tools:
  - http://www.splintered.net/sw/flow-tools/
- GTS 2003 - Andrey Verdana Andreoli
  - http://eng.registro.br/gter15/videos/experienciascomnetflow/
- Juniper Cflowd:
  - www.juniper.net/techpubs/software/junos/
- National Center for Network Engineering:
  - http://www.ncne.org/training/techs/2002/0127/presentations/
- Ntop:
  - http://www.ntop.org/
- RFCs 2123, 3917, 3954, 3955.
  - www.ietf.org

Obrigado!

Para entrar em contato e obter mais informações:

almir at acmesecurity dot org Key ID: 0x77F86990

arnaldo at acmesecurity dot org Key ID: 0x85A6CA01

ronan at acmesecurity dot org Key ID: 0x165130A6

adriano at acmesecurity dot org Key ID: 0x3893CD28

Agradecimentos a Gustavo Rodrigues Ramos pela ajuda na elaboração deste material

http://www.acmesecurity.org

ACME! Computer Security Reseach Labs

UNESP – IBILCE

São José do Rio Preto - Brasil