Gerência de Segurança Através do Uso de Netflow

Leandro Márcio Bertholdo, Andrey Vedana Andreoli, Liane M. R. Tarouco

POP-RS - Ponto de Presença da RNP no Rio Grande do Sul
Rua Ramiro Barcelos, 2574 CEP 90.035-003 – Porto Alegre – RS – Brasil

{berthold,andrey,liane}@penta.ufrgs.br

Resumo.

Esse artigo apresenta o Netflow como uma das ferramentas de gerência de segurança de redes utilizada no dia-a-dia do POP-RS[1] e CERT-RS para detecção de ataques DoS e outros. Aqui é apresentada sua utilização na detecção do verme Slammer, que assolou a Internet em janeiro desse ano.

1. Introdução

Como as redes se tornaram grandes e heterogêneas, os administradores necessitam de ferramentas eficientes para monitorar as atividades da rede a aplicar uma segurança global em seus backbones. Em ambientes abertos, como redes acadêmicas e de pesquisa, a restrição de acesso do usuário a aplicações nem sempre é uma opção, dessa forma o controle de uso dos recursos é imprescindível.

Ferramentas que sempre foram utilizadas para a análise da rede como: TCPDump, Trafshow, LANExplorer, Observer, Ethereal e outras, não tem capacidade para manipular satisfatoriamente as grandes quantidades de tráfego de uma rede gigabit ethernet a um custo viável.

Nesse artigo são descritas resumidamente as ferramentas utilizadas para analisar fluxos de dados (Flows) gerados por vários nodos da rede. Essas ferramentas são usadas a alguns anos pelo POP-RS/RNP e pelo CERT-RS para diagnosticar, contabilizar e tratar os incidendes detectados a partir do controle do próprio backbone. Hoje, o tráfego agregado no POP-RS supera a marca dos 70 Mbps, mas a solução é totalmente escalável e já utilizada na Internet2 [SHA 2001]. Essa abordagem nos permitiu rapidamente diagnosticar e controlar vários Denial of Services realizados contra e/ou utilizando instituições conectadas ao Ponto de Presença da RNP no Rio Grande do Sul, nos permitindo agir pró-ativamente.

2. Ferramentas utilizadas no experimento

As informações sobre fluxos de dados são obtidas a partir do Netflow [CIS 2002]. A sua ativação nos routers da rede permite o registro de um "flow"[2] em um host remoto na forma de um registro de dados contendo informações como: IP e porta origem do

[1] O Netflow foi incialmente implementado nos equipamentos do POP-RS em 2001, sendo posteriormente aprimorado. Desde então inúmeros problemas de segurança puderam ser facilmente resolvidos.

[2] Um registro NetFlow ou flow é uma seqüência unidirecional de pacotes entre dois pontos de comunicação.

pacote, IP e porta destino, tipo de protocolo, TOS (tipo do serviço), interface de entrada do fluxo, hora inicial e final do fluxo, número de pacotes e octetos que compõem o fluxo, além do sistema autônomo de origem e destino deste. Recentemente o IETF redigiu uma draft que discute o formato de exportação de dados para o NetFlow V9 [CLA 2002].

Uma vez os dados gerados no gateway e armazenado em um servidor[3], eles são processados por várias ferramentas como o Cflowd [CFL 2003], FlowTools [FLT 2003] e FlowScan [FLO 2003] gerando informações em modo gráfico e permitindo consultar os dados armazenados na base de dados de fluxos através de um conjunto de ferramentas adicionais providas pelo Flow-Tools.

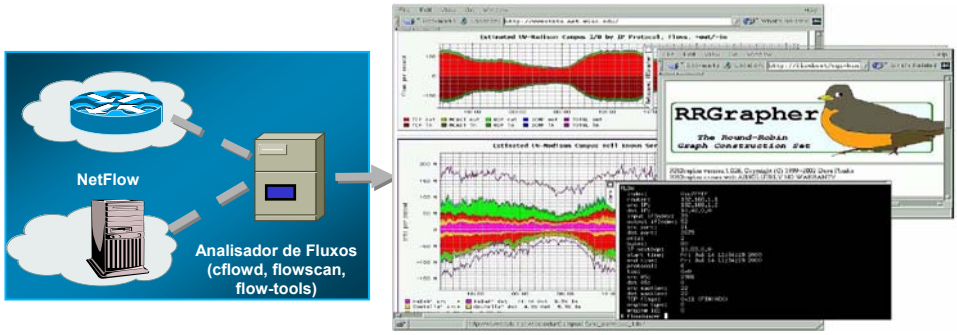

Figura 1: Fluxo de Informações no Netflow

Dentre as ferramentas que permitem extrair informações sobre os fluxos de dados existentes no Netflow, e que são utilizadas no POP-RS, podemos citar:

- Informações obtidas diretamente na console do equipamento (router): Através do comando *show ip cache flow* pode-se obter a distribuição atual dos fluxos de dados conforme o protocolo utilizado.
- Cflowd: Permite a análise e armazenamento dos dados gerados pelo NetFlow e, através de seus módulos CFlowdMux, Cflowd, CfdCollect e FlowDump, receber os fluxos de dados e armazená-los para posterior pesquisa. Através destes aplicativos e outros que compõem o pacote (cfdportmatrix, cfdprotos, etc) os fluxos armazenados podem ser consultados de forma semelhante ao TCPDump, ou seja, através de expressões regulares (ER´s).
- O FlowScan é outra ferramenta utilizada para gerar gráficos pré-definidos como os apresentados na Figura1. O RRGrapher.cgi permite gerar gráficos instantaneamente conforme os parâmetros solicitados.
- Outro conjunto de ferramentas utilizadas é o Flow-Tools que através de seus aplicativos (Flow-print, Flow-filter, Flow-dscan, etc.) permite detectar DoSs e scans realizados na rede, bem como detectar hosts que estejam utilizando grande número de portas TCP/UDP. Na figura 2 podemos verificar uma das listas de informações providas pelo Flow-Tools.

[3] No POP-RS os dados são armazenados em um Pentium IV 1.5Ghz e ocupam um total de 30Gb de espaço, o suficiente para manter 30 dias de fluxos de dados. O processamento gráfico desses dados é realizado neste mesmo equipamento.

Top 20 143.54.0.0/16 hosts by **bytes out**
for five minute flow sample ending Fri Feb 21 20:27:32 2003

rank	src Address	bits/sec in	bits/sec out	pkts/sec in	pkts/sec out	flows/sec in	flows/sec out
#1	143.54.28.105	37.0 k (0.5%)	2.1 M (54.1%)	103.5 (9.2%)	188.2 (14.2%)	473.3 m (1.1%)	713.3 m (0%)
#2	143.54.19.156	321.2 k (4.0%)	364.1 k (9.4%)	45.0 (4.0%)	51.0 (3.8%)	476.7 m (1.1%)	560.0 m (0%)
#3	143.54.47.240	10.3 (0.0%)	132.1 k (3.4%)	26.7 m (0.0%)	275.2 (20.8%)	26.7 m (0.1%)	93.8 (63%)
#4	143.54.1.3	7.2 k (0.1%)	126.6 k (3.3%)	11.7 (1.0%)	18.6 (1.4%)	700.0 m (1.6%)	866.7 m (1%)
#5	143.54.88.18	38.6 k (0.5%)	124.3 k (3.2%)	84.0 (7.5%)	49.0 (3.7%)	1.4 (3.1%)	1.4 (1%)

Figura2: Informações extraídas pelo Flow-Tools

3. Resultados Obtidos

Um bom momento que validou a estrutura implementada foi a ocorrência do verme Slammer ou Sapphire[CAI 2003]. O verme se propagou na madrugada de sábado, 25 de Janeiro de 2003, iniciando-se as 3:30h (BRDST) e infectando um grande número de servidores Windows com SQL Server. O verme utilizava a porta 1434/UDP. Alguns dos equipamentos de clientes do POP-RS começaram a gerar alerta de não alcançabilidade[4] próximo das 04:30h. Os dados coletados pelo NetFlow nesse instante foram fundamentais para detectar e isolar o problema até que este fosse confirmado nas várias listas de segurança, bem como os clientes contatados e os servidores atualizados[5].

Através da visualização do fluxo de dados por bloco IP (Figura 3) controlado pelo POP-RS, pôde-se facilmente visualizar quais os segmentos da rede estavam com tráfego anormal. Complementando-se com os fluxos de cada protocolo (Figura 4), conseguimos verificar que se restringia ao tráfego UDP.

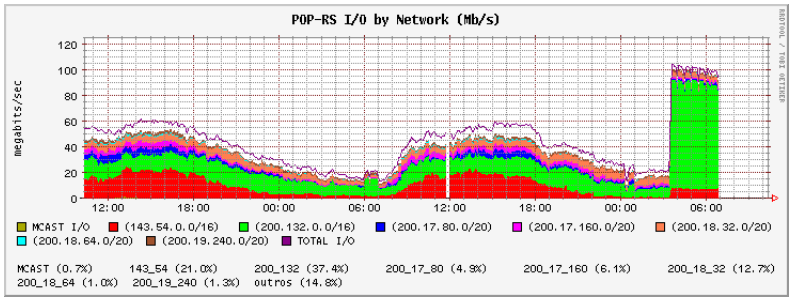

Figura 3: Identificando o tráfego de cada bloco do Backbone

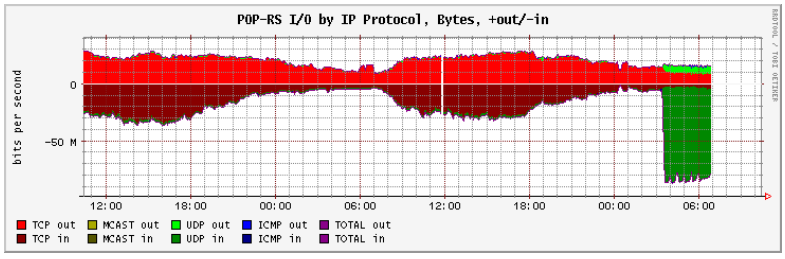

Figura 4: Identificando a anormalidade nos protocolos

[4]Alguns routers menores entraram em loop de inicialização, devido principalmente ao alto tráfego de retorno (ICMP Port e Host unreachable) gerado pelos portscans dos servidores contaminados pelos vírus.

[5]Como o problema se manifestou na madrugada de sábado, alguns administradores somente puderam ser contatados na segunda-feira, praticamente 30h depois do registro do problema.

4. Conclusões

A partir de informações como as aqui demonstradas, obtidas de ferramentas como o FlowDump e Flow-tools, foi possível rapidamente localizar os hosts que estavam contaminados e isolá-los através de ACLs nos seus respectivos gateways até realizar o contato com os administradores de servidores nas redes do clientes.

Caso não estivesse devidamente configurado esse conjunto de ferramentas, teria sido praticamente impossível, com os recursos de hardware que o POP-RS possui, identificar esse ataque e respondê-lo rapidamente. Cabe salientar que o tráfego total na interface do principal gateway de saída da rede chegou ao limite de 100Mbps durante o evento e que alguns gateways não conseguiam manusear tal demanda, deixando a rede local do POP em uma situação caótica.

5. Direções Futuras

Consoante com os projetos futuros da RNP, especificamente do GT-QoS, um dos próximos passos a serem realizados é a integração do mecanismo utilizado no POP-RS com uma estrutura maior e distribuída proposta pelo GT. Essa estrutura prevê a instalação de máquinas coletoras em vários POPs da RNP e a padronização dos dados em uma base de dados única, o que possibilita uma melhor visualização global.

Paralelo a isso, novos aplicativos estão sendo projetados visando detectar anomalias no tráfego do backbone através da análise do fluxo de dados gerado pelo NetFlow. Associado a um sub-agente SNMP, informações estatísticas sobre o número de ataques detectados pode prover uma visão mais realística do número de ataques que são lançados diariamente utilizando o backbone. Esse mesmo sub-agente pode também ser capacitado a gerar alerta, permitindo uma resposta pró-ativa dos grupos de segurança como o CAIS e o CERT-RS.

6. Referências

[CIS 2002] Cisco Systems Inc. **NetFlow Services and Applications – White Paper**. http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm.

[CFL 2003] **Cflowd: Traffic Flow Analysis Tool** http://www.caida.org/tools/measurement/cflowd/

[CAI 2003] **Analysis of the Sapphire Worm - A joint effort of CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego CSE**. http://www.caida.org/analysis/security/sapphire/.

[CLA 2002] Claise, B.; **Cisco Systems NetFlow Services Export Version 9.** http://www.ietf.org/internet-drafts/draft-bclaise-netflow-9-00.txt.

[FLO 2003] **FlowScan - Network Traffic Flow Visualization and Reporting Tool** http://www.caida.org/tools/utilities/flowscan/index.xml

[FLT 2003] **Flow-tools Information**. http://www.splintered.net/sw/flow-tools/

[I2 2003] **Internet 2 NetFlow Statistics**. http://netflow.internet2.edu/.

[SHA 2001] Shalunov, Stanislav; Teitelbaum, Benjamin. **Bulk TCP Use an Performance on Internet2.** http://abilene.internet2.edu/tcp/i2-tcp.pdf.