Análise de Tráfego em Redes TCP/IP

Utilize tcpdump na análise de tráfegos em qualquer sistema operacional

João Eriberto Mota Filho

Novatec

Editor: Rubens Prates
Editora assistente: Ana Carolina Prates
Revisão gramatical: Patrizia Zagni
Editoração eletrônica: Carolina Kuwabata
Capa: Carolina Kuwabata

ISBN: 978-85-7522-375-8

Histórico de impressões:

Julho/2013 Primeira edição

Novatec Editora Ltda.
Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
Fax: +55 11 2950-8869
E-mail: novatec@novatec.com.br
Site: novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Mota Filho, João Eriberto
Análise de tráfego em redes TCP/IP : utilize tcpdump na análise de tráfegos em qualquer sistema operacional / João Eriberto Mota Filho. -- São Paulo : Novatec Editora, 2013.

Bibliografia.
ISBN 978-85-7522-375-8

1. Redes de computadores 2. TCP/IP (Protocolo de redes de computadores) I. Título.

13-07326 CDD-004.62

Índices para catálogo sistemático:

1. TCP/IP : Protocolo de redes de computador : Processamentos de dados 004.62

VC20130718

CAPÍTULO 1

O que é a análise de tráfego?

Este capítulo abordará a definição do objetivo principal deste livro, ou seja, a análise de tráfego em redes TCP/IP.

1.1 Desconhecimento sobre redes: um problema histórico

As redes modernas são compostas de diversos equipamentos, sistemas operacionais, recursos de segurança e recursos de monitoramento. Manter todos esses elementos funcionando corretamente é uma tarefa complexa que exige um bom conhecimento tanto prático quanto teórico.

Historicamente, no Brasil, a formação a respeito de redes de computadores, até meados da década de 2000, fazia parte dos cursos de graduação voltados para programação; assim, tínhamos as redes como sendo o "patinho feio" da informática, consistindo em uma disciplina com poucas horas de duração. A consequência mais relevante disso é que muitos profissionais antigos conheceram as redes apenas na prática e, até hoje, têm problemas indecifráveis com as mesmas. Sem falar que, na sua grande maioria, eram os únicos profissionais disponíveis para serem professores nos cursos de redes. Por outro lado, nas universidades mais conceituadas, o assunto ainda é abordado de forma extremamente teórica e com muita profundidade. Novamente, temos problemas de entendimento do assunto e, no fim, redes de computadores é tudo o que um aluno não quer ver na sua frente. Portanto, com poucas exceções, teremos duas situações finais: cursos de redes com muitos ensinamentos práticos, mas poucos embasamentos teóricos ou, ao contrário, cursos profundos em cima de teorias e conceitos abstratos para o aluno. O resultado disso é desastroso.

O perfeito domínio da teoria é indispensável para o entendimento de uma rede e sua correta administração. Note que os comentários deste item do livro não têm a intenção de ofender ou rebaixar ninguém. O objetivo é mostrar nossa

atual situação e sensibilizar para a extrema importância de estudar e conhecer a teoria e a prática de forma equilibrada. E tudo tem seu momento. Um exemplo disso é que, em vários cursos, tenta-se ensinar Modelo OSI na primeira aula. No entanto, é impossível entendermos o Modelo OSI sem conhecermos, com certa profundidade, protocolos básicos como IP, TCP, UDP e ICMP.

O objetivo deste livro é ensinar um pouco a respeito de protocolos de redes e sobre processos de análise que serão essenciais na localização de problemas. A partir disso, o leitor estará apto a enfrentar as redes TCP/IP sem receios e sem ter que contar com a sorte. Será abordado, inclusive o protocolo IPv6.

1.2 Análise de tráfego em redes TCP/IP

Mas o que seria esta análise de tráfego? Observe o diálogo a seguir:

O diálogo mostrado é algo comum em muitas redes. Contudo, ele não deveria ocorrer. Pessoas que trabalham em uma rede e realizam esse tipo de diálogo estão perdidas e "chutando" soluções. Na verdade, elas não têm a menor noção do que esteja ocorrendo. É nesse ponto que entra a análise de tráfego.

A análise de tráfego nos permite detectar, rapidamente, quais problemas estão ocorrendo em uma rede e onde eles estão. Um exemplo disso poderá ser visto na figura 1.1.

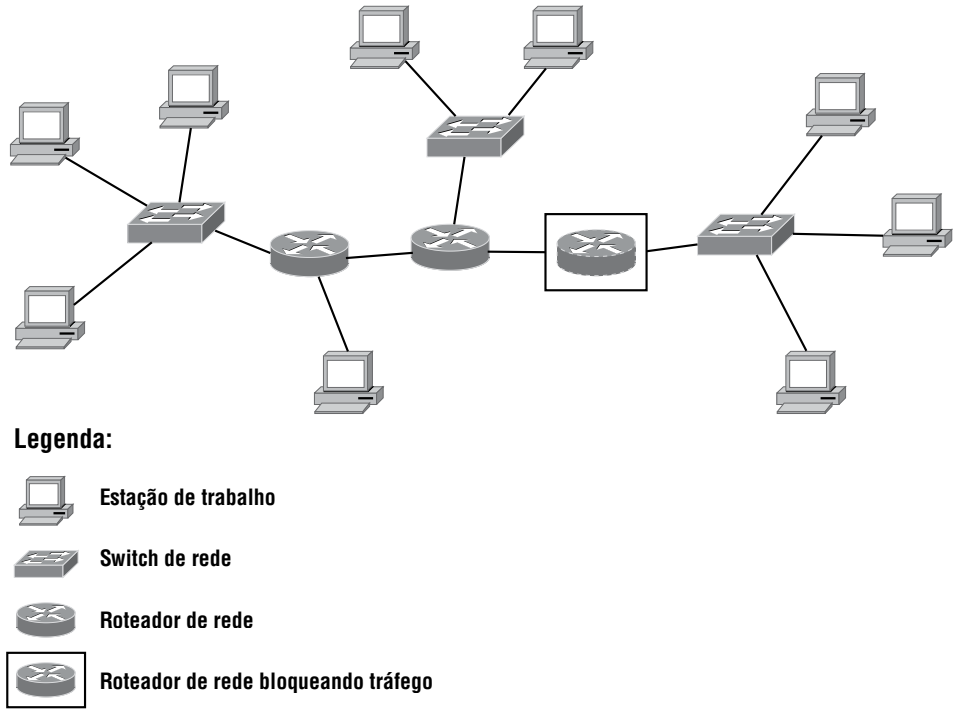

Figura 1.1 – Rede com bloqueio de tráfego.

Na figura 1.1 é possível notar uma rede com uma obstrução, uma vez que um dos roteadores está bloqueando todo o tráfego. Em consequência disso, não há comunicação entre as duas porções da rede interligadas por tal roteador. A questão está em como descobrir que o citado roteador é o problema. É nesse ponto que entra a análise de tráfego. Com ela, mesmo em uma rede com vários roteadores, será possível chegar ao problema em 2 minutos ou menos.

A análise de tráfego permite, entre outras possibilidades:

- detectar anomalias na rede;
- encontrar pontos de bloqueio na rede;
- descobrir equipamentos e cabeamento defeituosos;
- observar importantes mensagens de sistema não mostradas pelas aplicações;
- detectar falhas de segurança, instalação ou bugs em serviços disponíveis na rede;
- aprender sobre o funcionamento de protocolos e serviços pela observação;
- descobrir "tráfego pirata" dentro da rede.

1.3 Exemplos dos trabalhos a serem realizados neste livro

Este livro usará o famoso `tcpdump` como ferramenta principal. É lógico que vários outros comandos e aplicativos também serão empregados, como o `ping` e o `mtr`. Entretanto, como foi dito, a maior parte dos trabalhos estará baseada no `tcpdump`.

O `tcpdump` é um aplicativo que permite a visualização de todo o tráfego passante em uma rede. Teve seu desenvolvimento iniciado na década de 1980 e possui versões para ambientes Unix like (como o GNU/Linux, o Solaris e o OS X) e também para MS Windows, o `WinDump`.

Detalhes sobre o `tcpdump` e o `WinDump` serão mostrados no capítulo 4 e ao longo deste livro.

A listagem a seguir, produzida pelo `tcpdump` operando em uma rede, mostrará um típico cenário de análise de tráfego.

```
root@canopus:~# tcpdump -nS host www.darknet.com.br
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20:31:39.939213 IP 192.168.1.180.48961 > 203.0.113.112.80: Flags [S], seq 1160980399, win 14600, options [mss
      1460,sackOK,TS val 1083933 ecr 0,nop,wscale 7], length 0
20:31:40.398646 IP 203.0.113.112.80 > 192.168.1.180.48961: Flags [S.], seq 485093040, ack 1160980400, win 5840,
      options [mss 1460,nop,nop,sackOK,nop,wscale 9], length 0
20:31:40.398692 IP 192.168.1.180.48961 > 203.0.113.112.80: Flags [.], ack 485093041, win 115, length 0
20:31:40.398791 IP 192.168.1.180.48961 > 203.0.113.112.80: Flags [P.], seq 1160980400:1160980733, ack
      485093041, win 115, length 333
20:31:41.780977 IP 192.168.1.180.48961 > 203.0.113.112.80: Flags [P.], seq 1160980400:1160980733, ack
      485093041, win 115, length 333
20:31:42.270646 IP 203.0.113.112.80 > 192.168.1.180.48961: Flags [.], ack 1160980733, win 14, length 0
20:31:42.270815 IP 203.0.113.112.80 > 192.168.1.180.48961: Flags [P.], seq 485093041:485093521, ack 1160980733,
      win 14, length 480
20:31:42.270836 IP 192.168.1.180.48961 > 203.0.113.112.80: Flags [.], ack 485093521, win 123, length 0
20:31:44.268380 IP 192.168.1.180.48961 > 203.0.113.112.80: Flags [F.], seq 1160980733, ack 485093521, win 123,
      length 0
20:31:44.272200 IP 203.0.113.112.80 > 192.168.1.180.48961: Flags [F.], seq 485093521, ack 1160980733, win 14,
      length 0
20:31:44.272218 IP 192.168.1.180.48961 > 203.0.113.112.80: Flags [.], ack 485093522, win 123, length 0
20:31:44.791985 IP 203.0.113.112.80 > 192.168.1.180.48961: Flags [.], ack 1160980734, win 14, length 0
```

É possível ver um tráfego entre as máquinas 192.168.1.180 (cliente) e 203.0.113.112 (servidor). Trata-se de um tráfego TCP destinado à porta 80 do servidor e, tal tráfego, ocorreu de forma satisfatória e sem erros. Outro bom exemplo é o seguinte:

```
root@canopus:~# tcpdump -nS host 192.168.1.100
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

20:36:53.747869 IP 192.168.1.180.51204 > 192.168.1.100.90: Flags [S], seq 2501341939, win 14600, options [mss
    1460,sackOK,TS val 1162385 ecr 0,nop,wscale 7], length 0

20:36:53.748009 IP 192.168.1.100.90 > 192.168.1.180.51204: Flags [R.], seq 0, ack 2501341940, win 0, length 0
```

Nesse último exemplo, a máquina cliente tentou realizar uma conexão com a porta 90 da máquina servidora. No entanto, tal porta estava fechada.

Ao longo deste livro serão mostrados os detalhes sobre o funcionamento de cada protocolo de rede envolvido e como interpretar corretamente as listagens anteriores.

1.4 Este livro é só para quem usa GNU/Linux?

Não! Este livro se destina a qualquer pessoa e a qualquer sistema operacional, desde que se utilize TCP/IP. Como foi dito anteriormente, o `tcpdump` está disponível para, praticamente, todos os sistemas operacionais, incluindo o `WinDump` para MS Windows. Caso o tráfego a ser analisado esteja ocorrendo entre equipamentos que não permitam o emprego do `tcpdump`, bastará utilizar a técnica de análise por intermédio de bridge, como descrito no capítulo 14.

Resumindo, este livro:

- não é somente para quem usa GNU/Linux;
- objetiva o ensino da técnica de análise de tráfego;
- ao ensinar análise de tráfego, inevitavelmente, também ensinará muito sobre as redes TCP/IP. Esse ensino ocorrerá de forma prática, pois o leitor aprenderá vendo o tráfego e não imaginando como o mesmo seria.

Apenas como curiosidade, a maioria dos trabalhos foi desenvolvida em GNU/Linux e a distribuição utilizada foi a Debian, versão Wheezy 7.0.

1.5 Conclusão

A análise de tráfego é um assunto essencial para administradores de redes de computadores. Com tal análise, um administrador realmente dominará a sua rede. Muitas vezes, administradores não conhecem os conceitos básicos sobre protocolos de redes e terminam não resolvendo, conscientemente, os problemas técnicos encontrados. Isso sem mencionar os problemas que existem, mas nunca foram vistos ou notados.

De fato, a análise de tráfego é um assunto que interessa a todos os que trabalham em uma rede. Por exemplo, um desenvolvedor Java ou PHP poderá utilizar a análise de tráfego de uma forma bem básica para saber se há conectividade entre uma aplicação e um banco de dados. Isso não só facilitará sua vida e abrirá seus horizontes, como também o levará a contactar a equipe de redes somente em casos de real necessidade.