EA080 - O — Roteamento Dinâmico BGP (Border Gateway Protocol)

Professor: Christian Esteve Rothenberg

Leonardo Rodrigues Marques `RA: 178610`

1 Introdução

No quinto relatório técnico de redes de computadores, aprendemos o funcionamento do protocolo BGP. Esse protocolo foi projetado para trocar informações de roteamento e alcançabilidade entre sistemas autônomos na Internet. Para isso, ele faz uso de atualizações **NLRI**, ou seja, Informações de Capacidade de Rede de vários roteadores vizinhos a fim de atualizar as tabelas de roteamento internas do roteador. Valendo-se dessa informação, configuramos uma rede com sistemas autônomos e simulamos um ataque do tipo BGP hijack a fim de compreender o funcionamento desse tipo de protocolo.

2 Metodologia

A metodologia proposta para desenvolver esse trabalho consistiu em duas etapas: configurar uma rede com sistemas autônomos e simular um ataque BGP hijack. Para a configuração dos sitemas autônomos, utilizamos os comandos especificados para entrar nos arquivos de configuração dos roteadores e setar os IPs de cada um. A medida que íamos adicionado as novas configurações, verificamos repetidamente as tabela de roteamento BGP dos roteadores para observar as possíveis alterações. Finalizado essa parte, executamos o script ./website.sh para verificar a conectividade entre os hosts.

Na segunda parte, simulamos um ataque hijack. Esse ataque basicamente é é a aquisição ilegítima de grupos de endereços IP por tabelas de roteamento corruptas da Internet. Ele faz com que requisições destinadas a sub-redes com IPs definidos sejam desviadas para outras sub-redes com mesmo IP.

Finalmente, lapidamos esses conceitos analisando um captura de pacotes no Wireshark. No pacote, pudemos observar as mensagens trocadas entre os roteadores para atualizar suas tabelas de roteamento BGP.

3 Resultado, Discussões e Conclusões

3.1 Questão 1

3.1.1

Ao executar o comando `sudo ps aux | grep quagga`, foram encontrado **6** processos relacionados ao *Quagga*. Dentre os 6 processos, 3 processos estão relacionados a daemon principal zebra e 3 a daemon auxiliar bgpd, responsável pela execução do algoritmo de roteamento do tipo BGP.

```
wifi@wifi-VirtualBox:~/lab5/conf$ sudo ps aux | grep quagga
[sudo] password for wifi:
quagga   17661  0.0  0.0  24500  2860 ?        Ss   14:26   0:00 /usr/lib/quagga/zebra -f co
quagga   17663  0.0  0.0  29320  3396 ?        Ss   14:26   0:00 /usr/lib/quagga/bgpd -f con
quagga   17665  0.0  0.0  24500  2632 ?        Ss   14:26   0:00 /usr/lib/quagga/zebra -f co
quagga   17667  0.0  0.0  29452  3328 ?        Ss   14:26   0:00 /usr/lib/quagga/bgpd -f con
quagga   17669  0.0  0.0  24500  2700 ?        Ss   14:26   0:00 /usr/lib/quagga/zebra -f co
quagga   17671  0.0  0.0  29320  3548 ?        Ss   14:26   0:00 /usr/lib/quagga/bgpd -f con
wifi     17702  0.0  0.0  14224   940 pts/36   S+   14:26   0:00 grep --color=auto quagga
wifi@wifi-VirtualBox:~/lab5/conf$
```

Figura 1: Processos relacionados ao Quagga.

3.1.2

Ao executarmos o comando `ping` entre os hosts h1-1 e h3-1, constatamos que não existe conectividade.

```
root@wifi-VirtualBox:~/lab5# ping -c10 13.0.1.1
PING 13.0.1.1 (13.0.1.1) 56(84) bytes of data.
From 11.0.1.254 icmp_seq=1 Destination Net Unreachable
From 11.0.1.254 icmp_seq=2 Destination Net Unreachable
From 11.0.1.254 icmp_seq=3 Destination Net Unreachable
From 11.0.1.254 icmp_seq=4 Destination Net Unreachable
^C
--- 13.0.1.1 ping statistics ---
10 packets transmitted, 0 received, +4 errors, 100% packet loss, time 9015ms
```

Figura 2: Teste de Ping entre os hosts h1-1 e h3-1.

3.2 Questão 2

3.2.1

A topologia experimental com protocolo BGP da figura possui 3 sub-redes definidas. Seus endereços são: 10.0.0.0/8(R1), 12.0.0.0/8(R2) e 13.0.0.0/8 (R3).

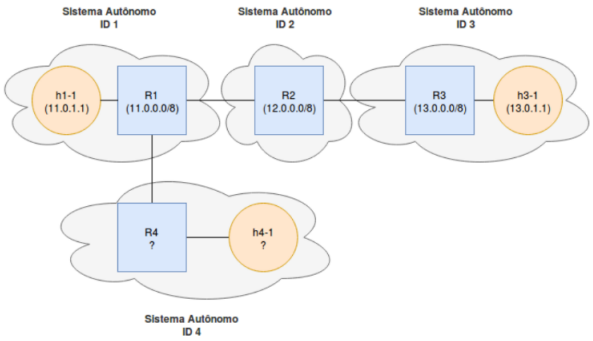

Figura 3:

3.2.2

Após seguir os passos para abrir o xterm do R1 e acessar o ambiente de configuração do BGPD, executamos o comando `sh ip bgp` e verificamos que não existe nenhuma tabela de roteamento BGP.

```
bgpd-R1# sh ip bgp
No BGP network exists
bgpd-R1#
```

Figura 4: Inexistência de tabela de roteamento BGP para R1.

3.2.3

Após a configuração dos roteadores, podemos observar que as redes BGP foram geradas. O vetor distância de R1 a 13.0.0.0/8 é [**0 2 3 i**].

```
bgpd-R1# sh ip bgp
BGP table version is 0, local router ID is 9.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 11.0.0.0         0.0.0.0                  0         32768 i
*> 12.0.0.0         9.0.0.2                  0             0 2 i
*> 13.0.0.0         9.0.4.2                  0             0 4 i
*                   9.0.0.2                                0 2 3 i

Total number of prefixes 3
bgpd-R1#
```

Figura 5: Tabela de roteamento do roteador R1.

3.2.4

Ao executar o comando `.\website.sh` noo xterm de h1-1, a mensagem recebida pelo servidor web foi `<h1>Default web server<\h1>`.

3.3 Questão 3

3.3.1

Após executar o script `.\go.sh`, a mensagem que passou a ser mostrada foi `<h1>***Attacker web server***<\h1>`.

Figura 6: Mensagem em h1-1 após execução do script no roteador R2.

3.3.2

O vetor de caminhos de R2 para a rede 13.0.0.0/8 é [**0 1 4 i**].

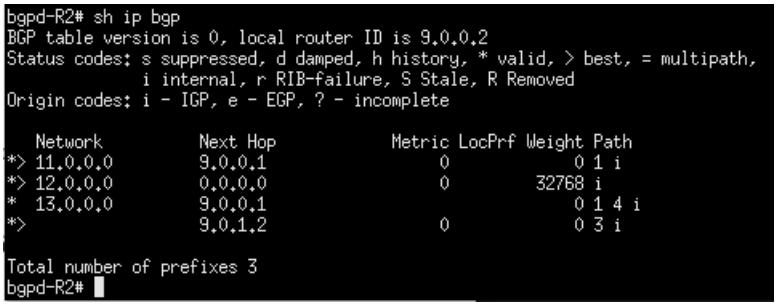

Figura 7: Vetor de caminhos na tabela de roteamento de R2.

3.3.3

Executamos o comando `curl 13.0.1.1(h3-1)` no xterm de R2, e a mesagem que obtivemos foi `<h1>Default web server<\h1>`, que é a mesma mensagem quando executamos o script `.\ website.sh`.

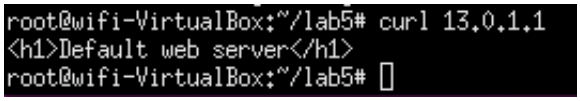

Figura 8:

3.3.4

Ao executar o script `.\go.sh`, uma sub-rede com endereço 13.0.0.0/8 é criada (onde o roteador R4 se localiza). Essa sub-rede possui mesmo endereço da sub-rede do roteador R3, onde está conectado o host

h3-1. O host h1-1 requisita a informação ao servidor. A requisição passa pelo roteador R1. Esse roteador, ao procurar a rede de destino, consulta a tabela de redes BGP e escolhe com menor distância, no caso a rede recém-criada. Essa alteração na escolha da rede reflete na mudança da mensagem.

3.4 Questão 4

3.4.1

A rede enunciada por R4 é 13.0.0.0/8.

```
bgpd-R4# sh ip bgp
BGP table version is 0, local router ID is 9.0.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 11.0.0.0         9.0.4.1                  0             0 1 i
*> 12.0.0.0         9.0.4.1                                0 1 2 i
*> 13.0.0.0         0.0.0.0                  0         32768 i

Total number of prefixes 3
bgpd-R4#
```

Figura 9: Tabela de roteamento BGP de R4.

3.4.2

As rotas para as sub-redes de R1 são: **11.0.0.0** com vetor de caminho [**i**]; **12.0.0.0** com vetor de caminho [**2 i**]; **13.0.0.0** com vetores de caminhos [**4 i**] e [**2 3 i**].

```
bgpd-R1# sh ip bgp
BGP table version is 0, local router ID is 9.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 11.0.0.0         0.0.0.0                  0         32768 i
*> 12.0.0.0         9.0.0.2                  0             0 2 i
*> 13.0.0.0         9.0.4.2                  0             0 4 i
*                   9.0.0.2                                0 2 3 i

Total number of prefixes 3
bgpd-R1#
```

Figura 10: Tabela de roteamento BGP de R1.

3.4.3

A principal mudança observável na nova verificação da tabela de roteamento de R1 é um novo vetor de caminhos adicionado a sub-rede 13.0.0.0/8.

```
*> 13.0.0.0         9.0.4.2                  0             0 4 i
*                   9.0.0.2                                0 2 3 i
```

Figura 11: Dois vetores de caminhos a sub-rede 13.0.0.0/8.

3.4.4

A mudança na mensagem no host h1-1 está relacionado ao seguinte fato: quando o script ./go.sh foi executado, uma nova sub-rede 13.0.0.0/8 mais próxima de R1 e h1-1 foi criada. Isso fez com que a requisição do host fosse encaminhada por R1 para a sub-rede recém-criada e lá encontrasse um servidor com mesmo endereço de h3-1, mas com uma mensagem diferente.

3.4.5

Ao executar o script `.\back.sh`, a sub-rede 13.0.0.0/8 recém-criada foi desligada. A tabela de roteamento BGP do roteador R1 foi atualizada e encaminhou a requisição para o caminho anterior [**2 3 i**], onde o host h3-1 está conectado.

3.4.6

O script **back.sh** mata os processos do roteador R4 relacionados ao quagga.

O script **go.sh** chama o script **back.sh**, e posteriormente cria os processos do roteador R4 no quagga.

3.4.7

O endereço IP do host **h4-1** é **13.0.1.1**, que é o mesmo do host **h3-1**.

3.4.8

Inicialmente, o protocolo BGP, através das mensagens "KEEPALIVE Message, UPDATE Message, UPDATE Message,...", verifica a alcançabilidade entre os hosts a partir do endereços de sub-rede dos roteadores.

3.4.9

Anteriormente, a tabela de roteamento BGP de R1, indicava rotas para o roteador R2 e R3. Após a execução do script `.\go.sh`, um roteador R4 foi adicionado com o mesmo número IP de sub-rede do roteador R3. Então, o R1, através das trocas de mensagens **UPDATE**, atualizou sua tabela de roteamento, incluindo esse caminho para o roteador R4. Como o algoritmo BGP é focado na otimização de rotas, ele não diferencia o roteador R4 de R3, mas apenas tenta chegar no endereço requisitado pelo caminho mais curto.

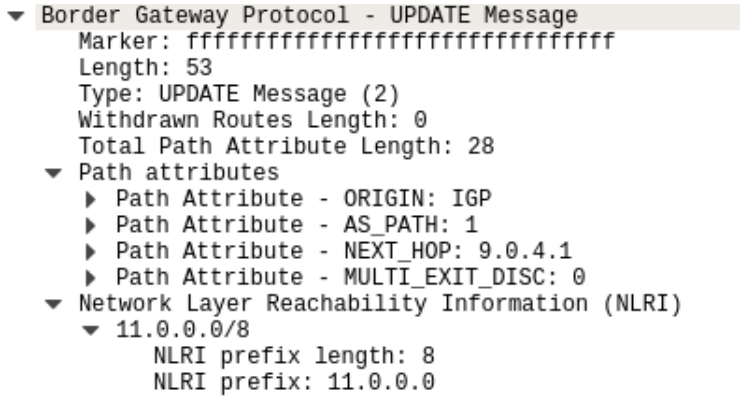

Figura 12: Pacote KEEP ALIVE UPDATE UPDATE ... BGP.

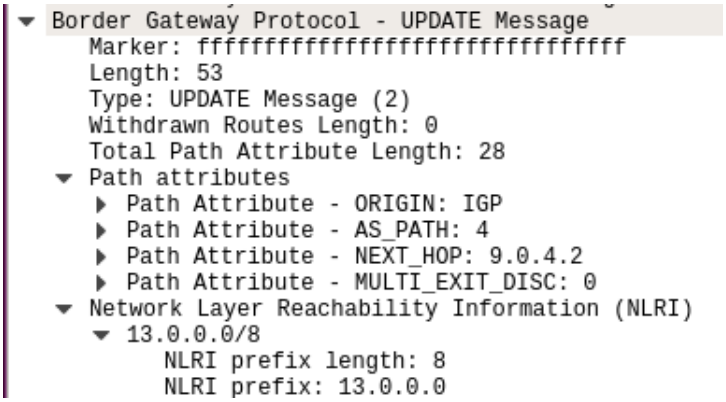

Figura 13: Pacote KEEP ALIVE UPDATE UPDATE BGP.

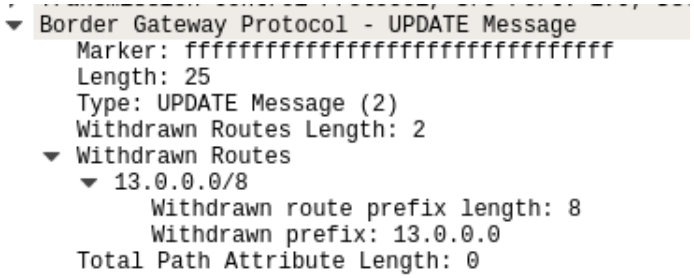

Figura 14: Pacote UPDATE Message BGP.