Formação IPv6 – Maputo

Moçambique

26 Agosto – 29 Agosto '08

Segurança

Pedro Lorga (lorga@fccn.pt)

Carlos Friaças (cfriacas@fccn.pt)

Exercício Prático: *Segurança*

Objectivos

Neste exercício completará as seguintes tarefas:

- *Analisar os serviços IPv6 acessíveis num servidor*
- *Configurar filtros para o tráfego IPv6*
- *Efectuar o controle de acesso remoto (linhas VTY)*

Tarefa 1: *Identificar portos IPv6 acessíveis num sistema*

Passo 1: Entre no servidor Linux atribuído ao seu grupo através de SSH.

Passo 2: Verifique que todos os firewalls (IPv4 e IPv6) estão desactivados no servidor. Use «service iptables stop» e «service ip6tables stop».

Passo 3: Através do comando «ifconfig», verifique quais os endereços IPv4 e IPv6 do seu servidor.

Passo 4: Use a ferramenta NMAP em IPv4, com:
«nmap 10.0.6.**x**»

Passo 5: Use a ferramenta NMAP em IPv6, com:
«nmap -6 2001:690:258:1:**xxxx:yyyy:wwww:zzzz**»

Passo 6: Compare o resultado da execução dos 2 comandos, observando que serviços estão activos quer em IPv4, quer em IPv6.

Tarefa 2: *Filtros IPv6*

Tenha em atenção que os *routers* usados neste exercício têm suporte no seu IOS das funcionalidades mencionadas. É sempre necessário analisar se o IOS que estamos (ou viremos) a usar tem todas as funcionalidades necessárias.

Existem vários métodos de configuração de listas de controle de acesso (filtros), mas neste exercício vamos apenas abordar uma delas.

O método que vamos usar é o seguinte:

```
Router# conf t
Router#(config)# ipv6 access-list <name_access_list>
Router#( config-ipv6-acl)# <deny/permit> …
```

The **permit** clause is:

```
permit protocol {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address} [operator [port-number]] {destination-ipv6-
prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dest-option-type [doh-number | doh-
type]] [dscp value] [flow-label value] [fragments] [log] [log-
input] [mobility] [mobility-type [mh-number | mh-type]] [reflect
name [timeout value]] [routing] [routing-type routing-number]
[sequence value] [time-range name]
```

The **deny** clause is:

```
deny protocol {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address} [operator [port-number]] {destination-ipv6-
prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dest-option-type [doh-number | doh-
type]] [dscp value] [flow-label value] [fragments] [log] [log-
input] [mobility] [mobility-type [mh-number | mh-type]]
[routing] [routing-type routing-number] [sequence value] [time-
range name] [undetermined-transport]
```

Passo 1: Reconfiguração de cablagem

É necessário ligar o PC de um dos membros de cada grupo à porta do switch 30+número_grupo. Desta forma, este PC ficará ligado numa VLAN directamente com o router atribuído ao seu grupo. **É também necessário que os formadores assegurem que todos os routers tenham uma rota ::/0 devidamente configurada, e caminho para todas as redes 2001:db8:cafe.**

Passo 2: Abra uma janela de DOS no PC, e coloque um **ping –t** a correr indefinidamente, com o endereço de outro router **que não o seu** como destino. A tabela seguinte contém os endereços IPv6 dos routers:

Interface	Endereço IPv6
Router 1	2001:DB8:CAFE:***A***::1
Router 2	2001:DB8:CAFE:***B***::1
Router 3	2001:DB8:CAFE:***C***::1
Router 4	2001:DB8:CAFE:***D***::1
Router 5	2001:DB8:CAFE:***E***::1
Router 6	2001:DB8:CAFE:***F***::1

Tabela 1 Endereços dos interfaces dos Routers

Passo 3: Configure uma lista de acesso IPv6

Entre no router atribuído ao seu grupo e configure uma lista de acesso IPv6, para negar todo o tráfego:

(em modo de configuração, no router)

Router(config)#**ipv6 access-list stop-ping**

Router(config-ipv6-acl)#**deny ipv6 any any**

Passo 4: Aplique a lista de acesso IPv6 que acabou de criar.

Entre em modo de configuração no interface FastEthernet0/1.200+número_grupo, e aplique a lista recentemente criada.

Use o comando **ipv6 traffic-filter stop-ping in|out**

(Use **in**, ou em alternativa **out**, para especificar o sentido de aplicação da lista de acesso)

Observe se o **ping –t** deixou de ser bem sucedido, ou se continua a funcionar.

Passo 5: Controlar o acesso ao router (linhas VTY)

Como deve saber, é uma boa prática limitar o acesso aos seus routers, a partir de blocos de endereços bem determinados.

Crie uma nova lista de acesso IPv6, para permitir apenas acesso a partir do PC cujo endereço começa por **2001:db8:cafe**:

ipv6 access-list LOGIN

permit ipv6 2001:db8:cafe::/48 any

deny ipv6 any any

A aplicação desta lista é feita através dos commandos de configuração:

line vty 0 15

ipv6 access-class LOGIN in

Passo 6: Teste a última lista de acesso

Deverá sair e voltar a entrar no router através do endereço IPv6 (com sucesso), e outro elemento do grupo, cujo PC permanence noutra rede (não estando nas portas 31 a 36) deverá tentar entrar no mesmo router, através do mesmo endereço IPv6 (o que não deverá conseguir).

Sumário

Após completar estes exercícios, deverá ser capaz de:

- *Configurar e aplicar listas de acesso IPv6*
- *Limitar o acesso através de IPv6 a um equipamento*