Laboratório IPV6

IPV6 não faz fragmentação e deixa tudo a cargo da origem
Usa-se o protocolo, Path MTU Discovery (PMTUD) para descobrir a MTU do caminho.

PMTUD assume que o MTU de todo o caminho é igual ao do primeiro salto. Caso o tamanho dos pacotes enviados seja maior do que o suportado por algum enlace ao longo do caminho, o roteador irá descartá-lo e enviará uma mensagem ICMPv6 packet too big, contendo tanto a mensagem de erro quanto o valor do MTU do enlace seguinte.

Após o recebimento dessa mensagem, o nó de origem passa a limitar o tamanho dos pacotes de acordo com o MTU indicado. Isso é repetido até que o tamanho do pacote seja igual ou inferior ao menor MTU do caminho. Os dispositivos armazenam o MTU para cada destino em uma tabela chamada destination cache, não sendo necessário repetir a descoberta a cada pacote enviado. Caso o pacote seja enviado a um grupo multicast, o tamanho utilizado será o menor MTU de todo o conjunto de destinos. Implementações minimalistas de IPv6 podem não realizar a descoberta de MTU e utilizar 1280 bytes como tamanho máximo para os pacotes.

Roteiro experimental:

MTU Discover pag 99

1- Abrir o arquivo:

1-10-PMTU.imn

O objetivo dessa topologia de rede é representar o mínimo necessário para que o protocolo PMTUD seja percebido.

2 - Altere os valores de MTU nos dispositivos n1Router e n3HostB.

(a) Abra um terminal de n1Router, altere o MTU da interface eth1 e verifique a mudança. Para isso utilize os seguintes comandos:

```
# ip link set eth1 mtu 1400
# ip addr show
```

3- Abra um terminal de n3HostB com um duplo-clique, altere o MTU da interface eth0 e verifique a mudança por meio dos seguintes comandos:

```
# ip link set eth0 mtu 1400
# ip addr show
```

4 - Em paralelo, efetue:

(a) A coleta dos pacotes trafegados na interface eth0 de n2HostA. As instruções de coleta de pacotes utilizando tcpdump ou Wireshark:

(b) Abra outro terminal de n2HostA e verifique a conectividade IPv6 com n3HostB. Digite o comando:

```
# ping6 -s 1500 -M want -c 4 2001:db8:2::10
```

Verifique qual o resultado do comando. O enlace aceitou o ping com o tamanho de 1500 bytes.

Roteiro Experimental: Segurança – pag 177

Experiência 3.1. Ataque DoS ao Neighbor Discovery Protocol

1 - Para o presente exercício será utilizada a topologia descrita no arquivo:

3-01-DoS-NA.imn.

O protocolo de descoberta de vizinhança, o **NDP**, foi desenvolvido para automatizar configurações nos dispositivos de uma rede e para facilitar a comunicação entre eles. Entre suas funções está a detecção de dispositivos da rede, a determinação dos endereços físicos dos nós vizinhos, a localização dos roteadores na rede e a detecção do uso de endereços IP duplicados. Todas essas funções atuam baseadas na troca de mensagens ICMPv6.

A funcionalidade **DAD** pode ser utilizada por um usuário mau intencionado para gerar um ataque de negação de serviço a uma rede IPv6. A DAD ocorre quando um novo dispositivo conectado à rede envia uma mensagem NS para verificar se o endereço IPv6 atribuído a sua interface já está sendo utilizado por outro nó. Se o endereço já estiver em uso, o dispositivo que está utilizando esse IP envia uma mensagem NA contendo essa informação e o dispositivo que realizou a requisição fica impedido de utilizar esse endereço.

2- Faça este experimento (até a página 183) e explique com suas palavras como o ataque foi feito e como esse ataque poderia ter ser evitado.